Navora

MANUAL DE SEGREGAÇÃO DE ATIVIDADES, CONFIDENCIALIDADE E SIGILO

Habilitação de Pessoa Jurídica CVM Nº 21. de 25 de fevereiro de 2021

30 de dezembro de 2025

NAVORA – GESTÃO DE RECURSOS S/A CNPJ60.579.514/0001-75

Londrina/PR, Avenida Ayrton Senna da Silva, nº.555

1. POLÍTICA DE SEGREGAÇÃO DAS ATIVIDADES

1.1. Segregação Física

Todas as áreas da Gestora são segregadas, especialmente a área de gestão de recursos, sendo o acesso limitado aos Colaboradores integrantes da área, por meio de controle de acesso em mesas separadas, ocorrendo segregação física e lógica desta em relação as demais áreas da Gestora, impedindo o compartilhamento de informações confidenciais e potenciais conflitos de interesse.

Não será permitida a circulação de Colaboradores em seções que não destinada ao respectivo Colaborador.

Reuniões com terceiros não colaboradores serão agendadas e ocorrerão em local específico. Será feito o controle e triagem prévia do terceiro não colaborador, inclusive clientes, sendo este encaminhado diretamente à devida sala.

A Gestora não medirá esforços para que ocorra a devida preservação de informações confidenciais por todos os seus administradores, diretores, colaboradores e funcionários, proibindo a transferência de tais informações a pessoas não habilitadas ou que possam vir a utilizá-las indevidamente. As respectivas informações confidenciais serão detidas apenas pelos colaboradores que atuem de forma essencial para os respectivos projetos, não podendo estas serem compartilhadas com demais colaboradores ou terceiros sem a aprovação prévia do Diretor de Compliance.

É de competência do Diretor de Compliance, ao longo do dia, fiscalizar a presença dos Colaboradores em suas devidas seções, sendo, ainda, informado imediatamente por e-mail se o acesso às áreas restritas for negado aos Colaboradores por mais de 5 (cinco) vezes.

O Diretor de Compliance elucidará as circunstâncias da ocorrência deste fato e aplicará as devidas sanções. Eventual infração à regra estabelecida será devidamente esclarecida e todos os responsáveis serão advertidos e passíveis de punições a serem definidas pelo Diretor de Compliance.

O Diretor de Compliance poderá a qualquer momento definir a implementação e manutenção de programas de treinamento de colaboradores e prestadores de serviço que tenham acesso a informações confidenciais e/ou participem de processo de decisão de investimento.

A propósito, as tarefas contábeis da empresa serão terceirizadas, de modo que sejam exercidas no local de atuação das empresas contratadas.

A Gestora possui equipe própria de Compliance, que atua de forma independente, se reportando apenas ao Diretor de Compliance indicado na Comissão de Valores Mobiliários, conforme o disposto no inciso IV, art. 4 º da Resolução CVM nº 21/21 e no art. 11 do Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros.

O Diretor de Compliance possui total autonomia e independência em suas decisões para questionar os riscos assumidos nas operações realizadas. O Comitê de Risco e Compliance, após recomendação do Diretor por Compliance, pode aplicar ações disciplinares cabíveis, independente de nível hierárquico, sem que seja necessária a validação prévia da Diretoria da Gestora.

1.2. Segregação Eletrônica

Adicionalmente, a Gestora segregará operacionalmente suas áreas a partir da adoção dos seguintes procedimentos: cada Colaborador possuirá computador de uso exclusivo, de modo a evitar o compartilhamento do mesmo equipamento e/ou a visualização de informações de outro Colaborador. Ademais, não haverá compartilhamento de equipamentos entre os Colaboradores da área de administração de recursos e os demais colaboradores, sendo que haverá impressora e fax destinados exclusivamente à utilização da área de administração de recursos.

Especificamente no que diz respeito à área de informática e de guarda, conservação, restrição de uso e acesso a informações técnicas/arquivos, dentre outros, informamos que o acesso aos arquivos/informações técnicas será restrito e controlado, sendo certo que tal restrição/segregação será feita em relação a: (i) cargo/nível hierárquico; e (ii) equipe.

Ademais, cada Colaborador possuirá um código de usuário e senha para acesso à rede, o qual é definido pelo responsável de cada área, sendo que somente os Colaboradores autorizados poderão ter acesso às informações da área de administração de recursos. Ainda, a rede de computadores da Gestora permitirá a criação de usuários com níveis de permissão diferentes, por meio de uma segregação lógica nos servidores que garantem que cada departamento conte com uma área de armazenamento de dados distinta no servidor com controle de acesso por usuário. Além disso, a rede de computadores manterá um registro de acesso e visualização dos documentos, o que permitirá identificar as pessoas que têm e tiveram acesso a determinado documento.

Ainda, cada Colaborador terá à disposição uma pasta de acesso exclusivo para digitalizar os respectivos arquivos, garantindo acesso exclusivo do usuário aos documentos de sua responsabilidade. Em caso de desligamento do Colaborador, todos os arquivos salvos na respectiva pasta serão transmitidos à pasta do seu superior direto, a fim de evitar a perda de informações.

Demais disposições encontram-se disponíveis na Política de Segurança da Informação e Cibernética da Gestora.

1.3. Segregação Funcional

A Gestora adota segregação funcional entre as atividades de Front-Office (Gestão/Investimentos/Comercial) e Backoffice (Risco, Compliance/Controles e Operações Internas), com o objetivo de evitar influência indevida, reduzir assimetria informacional e mitigar conflitos de interesse, especialmente considerando sua atuação preponderante em direitos creditórios.

Sem prejuízo das segregações física e eletrônica previstas nos itens 1.1 e 1.2, aplicam-se as seguintes regras mínimas de segregação funcional:

(i) Vedação de sobreposição crítica de funções: é vedado que o mesmo Colaborador acumule, simultaneamente, funções que comprometam a independência de controles, em especial: Gestão/Investimentos com Compliance/Controles Internos e/ou Risco.

(ii) Princípio dos "quatro olhos" (four-eyes): nenhuma etapa material do processo decisório e operacional deverá ser conduzida e concluída por uma única pessoa, devendo haver validação independente, registro e rastreabilidade.

(iii) Independência de Compliance/Risco: o Diretor e/ou a Equipe de Compliance e Risco possui autonomia para questionar, vetar, solicitar ajustes, impor condições de mitigação e determinar impedimentos/abstenções, inclusive quanto a decisões de investimento, credenciamento/seleção de cedentes/originadores, contratação de prestadores e tratamento de potenciais conflitos, sem necessidade de validação prévia da área de Gestão;

(iv) Registro e verificabilidade: as validações e manifestações de segunda linha Risco/Compliance e de Operações devem ser formalizadas (e-mail, ata, formulário interno ou ticket), com guarda e fácil recuperação.

1.3.1. Aplicação no fluxo de direitos creditórios

Para fundos sob gestão com foco em direitos creditórios, a segregação funcional se materializa, no mínimo, da seguinte forma:

(i) Originação/relacionamento com cedentes/originadores e prestadores: prospecção e relacionamento não substituem nem influenciam a análise técnica e a decisão de investimento;

(ii) Análise de crédito, elegibilidade e precificação: a área de Gestão/Investimentos elabora a proposta e racional; Risco (quando aplicável) e/ou Compliance/Controles Internos valida critérios, aderência a políticas, limites e conflitos;

(iii) Formalização e execução operacional: Operações/Backoffice valida documentação, fluxos, cadastros, trilhas e controles de execução (sem ingerência na decisão de investimento);

(iv) Monitoramento e cobrança: quando houver agente de cobrança e demais prestadores, a contratação e o monitoramento devem observar processo formal, critérios técnicos e controles de parte relacionada, com validação de Compliance quanto a conflitos e impedimentos.

1.3.2. Outras atividades profissionais dos Colaboradores

Todos os Colaboradores, especialmente aqueles em funções críticas e/ou elegíveis a certificação, devem declarar previamente e manter atualizadas junto ao Diretor de Compliance/Controles Internos todas as suas ocupações e atividades profissionais concomitantes, inclusive participações societárias relevantes, vínculos de prestação de serviços (PJ/MEI), cargos e assessoramentos.

A manutenção de atividade concomitante dependerá de avaliação e aprovação formal do Diretor de Compliance/Controles Internos, que considerará, no mínimo: (i) compatibilidade de dedicação e disponibilidade com o cargo exercido na Gestora; (ii) potencial conflito de interesses com clientes, cotistas, cedentes/originadores, sacados, garantidores, estruturadores, consultorias de crédito, SCDs, agentes de cobrança e demais prestadores usuais de FIDC; (iii) risco de acesso cruzado a informações sensíveis; e (iv) riscos reputacionais e regulatórios.

Identificada incompatibilidade por conflito ou por comprometimento de dedicação, o Colaborador deverá encerrar a atividade externa, ser realocado para função não conflitante ou, se aplicável, afastado de atividades elegíveis e decisórias, até saneamento, com registro formal da medida.

1.3.3. Integração com o Instrumento Formal de Segregação e Mitigação de Conflitos

Quando houver relação com partes relacionadas, vínculos cruzados, relações familiares relevantes ou relacionamento comercial com entidade potencialmente relacionada, a Gestora deverá aplicar, além deste Manual, o Instrumento Formal de Segregação, Reconhecimento e Mitigação de Conflitos de Interesse entre Partes Relacionadas, que estabelece barreiras de Chinese Wall e, incluindo: proibição de intercâmbio de pessoal e de compartilhamento de estrutura e acessos a sistemas, bem como vedações de participação em reuniões internas e deliberações sensíveis por pessoas vinculadas a partes relacionadas.

O referido Instrumento é considerado mecanismo central e verificável de mitigação e segregação quando aplicável, devendo permanecer arquivado, com controle de versões e disponibilidade para apresentação à CVM/ANBIMA quando solicitado.

1.4. Especificidades dos mecanismos de controles internos

A Gestora, por meio do Diretor de Compliance, mantém disponível, para todos os Colaboradores, quaisquer diretrizes internas, que devem ser sempre respeitadas, podendo atender, entre outros, os seguintes pontos:

(i) Definição de responsabilidades dentro da Gestora;
(ii) Meios de identificar e avaliar fatores internos e externos que possam afetar adversamente a realização dos objetivos da empresa;
(iii) Existência de canais de comunicação que assegurem aos Colaboradores, segundo o correspondente nível de atuação, o acesso a confiáveis, tempestivas e compreensíveis informações consideradas relevantes para suas tarefas e responsabilidades;
(iv) Contínua avaliação dos diversos riscos associados às atividades da empresa; e
(v) Acompanhamento sistemático das atividades desenvolvidas, de forma que se possa avaliar se os objetivos da Gestora estão sendo alcançados, se os limites estabelecidos e as leis e regulamentos aplicáveis estão sendo cumpridos, bem como assegurar que quaisquer desvios identificados possam ser prontamente corrigidos.

Caso qualquer Colaborador identificar situações que possam configurar como passíveis de conflito de interesse, deverá submeter imediatamente sua ocorrência para análise do Diretor de Compliance.

Adicionalmente, serão disponibilizados a todos os Colaboradores equipamentos e softwares sobre os quais a Gestora possua licença de uso, acesso à internet, bem como correio eletrônico interno e externo com o exclusivo objetivo de possibilitar a execução de todas as atividades inerentes aos negócios da Gestora. A esse respeito, o Diretor de Compliance poderá disponibilizar a diretriz para utilização de recursos de tecnologia, detalhando todas as regras que devem ser seguidas por todo e qualquer Colaborador, independentemente do grau hierárquico dentro da Gestora.

São realizados testes mensais de segurança para os sistemas de informações utilizados pela Gestora para garantir a efetividade dos controles internos mencionados neste documento, especialmente as informações mantidas em meio eletrônico.

2. POLÍTICAS DE CONFIDENCIALIDADE

2.1. Sigilo e Conduta

Todos os Colaboradores deverão ler atentamente e entender o disposto neste documento, bem como deverão firmar o termo de confidencialidade, conforme modelo constante no Anexo II ("Termo de Confidencialidade").

Conforme disposto no Termo de Confidencialidade, nenhuma Informação Confidencial, conforme abaixo definido, deve, em qualquer hipótese, ser divulgada fora da Gestora. Fica vedada qualquer divulgação, no âmbito pessoal ou profissional, que não esteja em acordo com as normas legais e regulatórias aplicáveis (incluindo, sem limitação, a Resolução CVM nº 21/21, a regulamentação vigente da CVM e as normas e códigos de autorregulação aplicáveis da ANBIMA) e de compliance da Gestora.

São consideradas informações confidenciais, reservadas ou privilegiadas ("Informações Confidenciais"), para os fins deste documento, independente destas informações estarem contidas em discos, pen-drives, fitas, e-mails, outros tipos de mídia ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre a Gestora, sobre as empresas pertencentes ao seu conglomerado, seus sócios e clientes, aqui também contemplados os próprios fundos sob gestão da Gestora, incluindo:

i. Know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador;
ii. Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e dos fundos geridos pela gestora;
iii. Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento e carteiras geridas pela Gestora;
iv. Estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;
v. Informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Gestora e a seus sócios e clientes, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (IPO), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da Gestora e que ainda não foi devidamente levado à público;
vi. Informações a respeito de resultados financeiros antes da publicação dos balanços, balancetes e/ou demonstrações financeiras dos fundos de investimento;
vii. Transações realizadas e que ainda não tenham sido divulgadas publicamente; e
viii. Outras informações obtidas junto a sócios, diretores, funcionários, trainees, estagiários ou jovens aprendizes da Gestora ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

A Informação Confidencial não pode ser divulgada, em hipótese alguma, a terceiros não-Colaboradores ou a Colaboradores não autorizados, não só durante a vigência de seu relacionamento profissional com a Gestora, mas também após o seu término.

Os Colaboradores deverão guardar sigilo sobre qualquer Informação Confidencial à qual tenham acesso, até sua divulgação ao mercado, bem como zelar para que subordinados e terceiros de sua confiança também o façam, respondendo pelos danos causados na hipótese de descumprimento.

Sem prejuízo da colaboração da Gestora com as autoridades fiscalizadoras de suas atividades, a revelação de Informações Confidenciais a autoridades governamentais ou em virtude de decisões judiciais, arbitrais e/ou administrativas, deverá ser prévia e tempestivamente informada ao respectivo Diretor de Compliance e Risco da Gestora titular da Informação Confidencial, para que este decida sobre a forma mais adequada para tal revelação, após exaurirem todas as medidas jurídicas apropriadas para evitar a supramencionada revelação.

Caso os Colaboradores tenham acesso, por qualquer meio, a Informação Confidencial, deverão levar tal circunstância ao imediato conhecimento do respectivo Diretor de Compliance e Risco da Gestora titular da Informação Confidencial, indicando, além disso, a fonte da Informação Confidencial assim obtida. Tal dever de comunicação também será aplicável nos casos em que a Informação Confidencial seja conhecida de forma acidental, em virtude de comentários casuais ou por negligência ou indiscrição das pessoas obrigadas a guardar segredo. Os Colaboradores que, desta forma, acessarem a Informação Confidencial, deverão abster-se de fazer qualquer uso dela ou comunicá-la a terceiros, exceto quanto à comunicação ao Diretor de Compliance e Risco, conforme acima.

2.2. Insider Trading, "Dicas" e Front-running

Em nenhuma hipótese as Informações Confidenciais poderão ser utilizadas para a prática de atos que configurem: (a) Insider Trading, ou seja, a compra e venda de títulos ou valores mobiliários com base no uso de Informação Confidencial, com o objetivo de conseguir benefício próprio ou de terceiros (compreendendo os Colaboradores); (b) "Dica", ou seja, a transmissão, a qualquer terceiro, estranho às atividades da Gestora, de Informação Confidencial que possa ser usada com benefício na compra e venda de títulos ou valores mobiliários; e/ou (c) Front-running, ou seja, a prática que envolve aproveitar alguma Informação Confidencial para realizar ou concluir uma operação antes de outros.

É expressamente proibido valer-se das práticas aqui descritas para obter, para si ou para outrem, vantagem indevida mediante negociação, em nome próprio ou de terceiros, de títulos e valores mobiliários, sujeitando-se o Colaborador às penalidades descritas neste documento e na legislação aplicável, incluindo eventual demissão por justa causa.

3. POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

As medidas de segurança da informação têm por finalidade minimizar as ameaças aos negócios da Gestora e às disposições deste documento, buscando, principal, mas não exclusivamente, a proteção de Informações Confidenciais.

As instalações da Gestora são protegidas por controles de entrada apropriados para assegurar a segurança dos Colaboradores e proteger o sigilo, a integridade e a disponibilidade da informação.

Todos os equipamentos da rede deverão ter acesso restrito. Os computadores que serão utilizados pelos Colaboradores deverão estar seguros e as sessões abertas deverão ser trancadas quando deixadas sem supervisão do Colaborador responsável por seu computador.

A política de segurança da informação e segurança cibernética leva em consideração diversos riscos e possibilidades considerando o porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvida pela Gestora.

A execução direta das atividades relacionadas à política de segurança da informação e segurança cibernética ficará a cargo da Equipe de Compliance, responsável inclusive por sua revisão, realização de testes e treinamento dos Colaboradores, conforme descrito neste documento.

Os Diretores de Compliance realizarão a revisão e atualização desta Política de Segurança da Informação e de Segurança Cibernética a cada 24 (vinte e quatro) meses, ou em prazo inferior sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão dos Diretores de Compliance.

3.1. Identificação de Riscos (risk assessment)

No âmbito de suas atividades, a Gestora identificou os seguintes principais riscos internos e externos que precisam de proteção:

i. Dados e Informações: Informações Confidenciais, incluindo informações a respeito de investidores, clientes, Colaboradores e da própria Gestora, operações e ativos investidos pelas carteiras de valores mobiliários sob sua gestão, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);
ii. Sistemas: Informações sobre os sistemas utilizados pela Gestora e as tecnologias desenvolvidas internamente e por terceiros, suas ameaças possíveis e sua vulnerabilidade;

iii. Processos e Controles: Processos e controles internos que sejam parte da rotina das áreas de negócio da Gestora; e
iv. Governança da Gestão de Risco: Eficácia da gestão de risco pela Gestora quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

Ademais, no que se refere especificamente à segurança cibernética, a Gestora identifica as seguintes principais ameaças, nos termos inclusive do Guia de Cibersegurança da Anbima:

i. Malware – softwares desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, Spyware e Ransomware);
ii. Engenharia social – métodos de manipulação para obter informações confidenciais (Pharming, Phishing, Vishing, Smishing, e Acesso Pessoal);
iii. Ataques de DDoS (distributed denial of services) e botnets: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; e
iv. Invasões (advanced persistent threats): ataques realizados por invasores sofisticados utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Com base no acima, a Gestora avalia e define o plano estratégico de prevenção e acompanhamento para a mitigação ou eliminação do risco, assim como as eventuais modificações necessárias e o plano de retomada das atividades normais e reestabelecimento da segurança devida.

3.2. Ações de Prevenção e Proteção

Após a identificação dos riscos, a Gestora adota as medidas a seguir descritas para proteger Informações Confidenciais e sistemas.

- Regra Geral de Conduta

A Gestora realiza efetivo controle do acesso a arquivos que contemplem Informações Confidenciais em meio físico, disponibilizando-os somente aos Colaboradores que efetivamente estejam envolvidos no projeto que demanda o seu conhecimento e análise.

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da Gestora e circulem em ambientes externos à Gestora com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas confidenciais.

A proibição acima referida não se aplica quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Gestora.

Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a Informação Confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

A troca de informações entre os Colaboradores da Gestora deve sempre se pautar no conceito de que o receptor deve ser alguém que necessita receber tais informações para o desempenho de suas atividades e que não está sujeito a nenhuma barreira que impeça o recebimento daquela informação. Em caso de dúvida a Equipe de Compliance deve ser acionada previamente à revelação.

Neste sentido, os Colaboradores não deverão, em qualquer hipótese, deixar em suas respectivas estações de trabalho ou em outro espaço físico da Gestora qualquer documento que contenha Informação Confidencial durante a ausência do respectivo usuário, principalmente após o encerramento do expediente.

Qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois pode conter informações restritas e confidenciais mesmo no ambiente interno da Gestora.

Cada Colaborador é responsável direto pela boa conservação, integridade e segurança de quaisquer Informações Confidenciais que estejam em meio físico sob a sua guarda.

O descarte de Informações Confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Os documentos físicos que contenham Informações Confidenciais ou de suas cópias deverão ser triturados e descartados imediatamente após seu uso de maneira a evitar sua recuperação ou leitura.

Em consonância com as normas internas acima, os Colaboradores devem se abster de utilizar pen-drives, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Gestora. É proibida a conexão de equipamentos na rede da Gestora que não estejam previamente autorizados pela área de informática e pela Equipe de Compliance da Gestora.

O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam difamar a imagem e afetar a reputação da Gestora.

O recebimento de e-mails muitas vezes não depende do próprio Colaborador, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente. Neste caso, o Colaborador deve apagá-las imediatamente, de modo que estas permaneçam o menor tempo possível nos computadores da Gestora.

A visualização de sites, blogs, fotologs, webmails, entre outros, que contenham conteúdo discriminatório, preconceituoso (sobre origem, etnia, religião, classe social, opinião política, idade, sexo ou deficiência física), obsceno, pornográfico ou ofensivo é terminantemente proibida.

Em nenhuma hipótese um Colaborador pode emitir opinião por e-mail em nome da Gestora, ou utilizar material, marca e logotipos da Gestora para assuntos não corporativos ou após o rompimento do seu vínculo com este, salvo se expressamente autorizado para tanto.

Programas instalados nos computadores, principalmente via internet (downloads), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia do responsável pela área de informática na Gestora. Não é permitida a instalação de nenhum software ilegal ou que possua direitos autorais protegidos. A instalação de novos softwares, com a respectiva licença, deve também ser comunicada previamente ao responsável pela informática. Este deverá aprovar ou vetar a instalação e utilização dos softwares dos Colaboradores para aspectos profissionais e pessoais.

AÇÕES DE PREVENÇÃO E PROTEÇÃO DE INFORMAÇÕES CONFIDENCIAIS E SEGURANÇA CIBERNÉTICA
Acesso Escalonado do Sistema O acesso como "administrador" de área de desktop é limitado aos usuários aprovados pelo respectivo Diretor de Compliance da Gestora e, com isso, serão determinados privilégios/credenciais e níveis de acesso de usuários apropriados para os Colaboradores. A Gestora mantém diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções e senioridade dos Colaboradores. As combinações de login e senha são utilizadas para autenticar as pessoas autorizadas e conferir acesso à parte da rede da Gestora necessária ao exercício de suas atividades. A Gestora implementa criação de logs e trilhas de auditoria sempre que permitido pelos sistemas. A implantação destes controles é projetada para limitar a vulnerabilidade dos sistemas da Gestora em caso de violação.
Senha e Login
A senha e login para acesso aos dados contidos em todos os computadores, bem como nos e-mails que também possam ser acessados via webmail, devem ser conhecidas somente pelo respectivo usuário do computador e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros. Dessa forma, o Colaborador pode ser responsabilizado inclusive caso disponibilize a terceiros a senha e login acima referidos, para quaisquer fins.

É estabelecido regras mínimas (complexidade, periodicidade e autenticação de múltiplos fatores) na definição de senhas de acesso a dispositivos corporativos, sistemas e rede em função da relevância do ativo acessado. Além disso, os eventos de login e alteração de senha são auditáveis e rastreáveis.
Uso de Equipamentos e Sistemas
Cada Colaborador é responsável ainda por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade. A utilização dos ativos e sistemas da Gestora, incluindo computadores, telefones, internet, e-mail e demais aparelhos se destina prioritariamente a fins profissionais. O uso indiscriminado destes para fins pessoais deve ser evitado e nunca deve ser prioridade em relação a qualquer utilização profissional. Tendo em vista que a utilização de computadores, telefones, internet, e-mail e demais aparelhos se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos Colaboradores, a Gestora monitoram a utilização de tais meios. Todo Colaborador deve ser cuidadoso na utilização do seu próprio equipamento e sistemas e zelar pela boa utilização dos demais. Caso algum Colaborador identifique a má conservação, uso indevido ou inadequado de qualquer ativo ou sistemas deve comunicar ao respectivo Diretor de Compliance responsável.
Acesso Remoto
A Gestora permite o acesso remoto pelos Colaboradores ao e-mail, rede e diretório. Os Colaboradores que se utilizarem do acesso remoto serão instruídos a (i) manter a utilização apenas em dispositivos que requeiram a inclusão de login e senha previamente ao acesso, (ii) manter softwares de proteção contra malware/antivírus nos dispositivos remotos, (iii) relatar ao Diretor de Compliance da Gestora para o qual atua qualquer violação ou ameaça de segurança cibernética ou outro incidente que possa afetar informações da Gestora e que ocorram durante o trabalho remoto, e (iv) não armazenar Informações Confidenciais ou sensíveis em dispositivos pessoais.
Acesso por Terceiros

Reuniões com terceiros não colaboradores serão agendadas e ocorrerão em local específico. Será feito o controle e triagem prévia do terceiro não Colaborador, inclusive Clientes, sendo este encaminhado diretamente à devida sala.
Firewall, Software, Varreduras e Backup
A Gestora utiliza um hardware de firewall projetado para evitar e detectar conexões não autorizadas e incursões maliciosas. A Gestora mantém proteção atualizada contra malware nos seus dispositivos e software antivírus projetado para detectar, evitar e, quando possível, limpar programas conhecidos que afetem de forma maliciosa os sistemas da empresa (por exemplo, vírus, worms, spyware). O sistema de antivírus é gerenciado através de uma console única por prestador de serviços especializado, onde existem alertas e procedimentos de automação para proteção quando se registra uma ameaça de infeção. Todos os servidores e estações de trabalho têm antivírus instalados e monitorados. A Gestora mantém e testa regularmente medidas de backup consideradas apropriadas pelos Diretores de Compliance. As informações da Gestora são atualmente objeto de backup online executado diariamente. Esse backup cópia tudo o que é modificado ou criado, possui fácil recuperação e visualização das informações copiadas.

3.3. Monitoramento e Testes

A Gestora possui mecanismos de monitoramento das ações de proteção implementadas, para garantir seu bom funcionamento e efetividade.

Nesse sentido, a Gestora mantém inventários atualizados de hardware e software bem como realiza verificações periódicas no intuito de identificar elementos estranhos à Gestora, como computadores não autorizados ou softwares não licenciados.

Além disso, a Gestora mantém os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas. As rotinas de backup são monitoradas diariamente, com a execução de testes regulares de restauração dos dados.

São realizados, periodicamente, testes de invasão externa e phishing, bem como análises de vulnerabilidades na estrutura tecnológica, sempre que houver mudança significativa em tal estrutura.

Ainda, a Gestora analisa regularmente os logs e as trilhas de auditorias, de forma a permitir a rápida identificação de ataques, sejam eles internos ou externos.

Serão realizados testes de segurança para os sistemas de informações utilizados pela Gestora, em periodicidade, no mínimo, anual, para garantir a efetividade dos controles internos mencionados neste documento, especialmente as informações mantidas em meio eletrônico.

3.4. Plano de Identificação e Resposta

• Identificação de Suspeitas

Qualquer suspeita de infecção, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da Gestora (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer Informações Confidenciais, mesmo que de forma involuntária, deverá ser informada ao respectivo Diretor de Compliance responsável prontamente. O Diretor de Compliance se reunirá com os demais diretores da respectiva Gestora para compreender o evento ocorrido, os motivos e consequências imediatas, bem como a gravidade da situação.

• Procedimentos de Resposta

O Diretor de Compliance, juntamente com os demais diretores da Gestora, correspondente responderá a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da respectiva Gestora de acordo com os critérios abaixo:

i. Avaliação do tipo de incidente ocorrido (por exemplo, infecção de malware, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;
ii. Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;
iii. Determinação dos papéis e responsabilidades do pessoal apropriado;
iv. Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;
v. Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, segurança pública, órgãos reguladores e autorreguladores);
vi. Avaliação da pertinência da adoção de medidas como registro de boletim de ocorrência ou queixa crime e/ou consulta com advogado para avaliação dos riscos jurídicos e medidas judiciais cabíveis para assegurar os direitos da Gestora.

vii. Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, (por exemplo: em sendo Informações Confidenciais de fundo de investimento sob gestão da respectiva Gestora, a fim de garantir a ampla disseminação e tratamento equânime da Informação Confidencial);

viii. Determinação do responsável (ou seja, a Gestora ou o cliente ou investidor afetado) que arcará com as perdas decorrentes do incidente. A definição ocorrerá após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

3.5. Arquivamento de Informações

Os Colaboradores deverão manter arquivada, pelo prazo regulamentar aplicável, toda e qualquer informação, bem como documentos e extratos que venham a ser necessários para a efetivação satisfatória de possível auditoria ou investigação em torno de possíveis investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro, bem como todos os documentos e informações exigidos pela Resolução CVM 21, correspondência, interna e externa, papéis de trabalho, relatórios e pareceres relacionados com o exercício de suas funções em conformidade com o inciso IV do Artigo 18 e com o Artigo 34 da Resolução CVM 21.

4. APROVAÇÕES E REVISÕES

O presente documento deverá ser revisto, no mínimo, anualmente, levando-se em consideração, dentre outras questões, mudanças regulatórias ou eventuais deficiências encontradas. Este Manual poderá ser também revista a qualquer momento, sempre que o Diretor de Gestão de Risco e Compliance, Operações e Controles Internos deliberar necessária.

Versão	Motivo da Revisão	Data Publicação
01	Documento Inicial	30/12/2025

ANEXO I

DECLARAÇÃO DE DISPONIBILIZAÇÃO DE DOCUMENTOS E CESSÃO DE DIREITOS

Por meio deste instrumento eu, _____, inscrito no CPF/MF sob o no _____, na qualidade de Colaborador da NAVORA – GESTÃO DE RECURSOS S/A ("Gestora"), declaro, para todos os fins, que, ao disponibilizar à Gestora documentos, planilhas, arquivos, fórmulas, modelos de avaliação, análise e gestão ou quaisquer ferramentas similares ("Materiais") observo o quanto segue:

i. a utilização ou disponibilização de tais documentos e arquivos não infringe quaisquer contratos, acordos ou compromissos de confidencialidade que o Colaborador tenha firmado, bem como não viola quaisquer direitos de propriedade intelectual de terceiros; e

ii. quaisquer alterações, adaptações, atualizações ou modificações, de qualquer forma ou espécie, em tais documentos e arquivos, serão de propriedade exclusiva da Gestora, sendo que, eu, o Colaborador, não poderei apropriar-me ou fazer uso de tais documentos e arquivos alterados, adaptados, atualizados ou modificados após um potencial desligamento da Gestora, exceto se aprovado expressamente pela Gestora.

[local], [data].

_____

[COLABORADOR]

ANEXO II

TERMO DE CONFIDENCIALIDADE

Por meio deste instrumento eu, _____, inscrito no CPF/MF sob o nº _____, doravante denominado Colaborador, e NAVORA – GESTÃO DE RECURSOS S/A inscrita no CNPJ sob o nº 60.579.514/0001-75 ("Gestora").

Resolvem as partes, para fim de preservação de informações pessoais e profissionais dos clientes e da Gestora, celebrar o presente termo de confidencialidade ("Termo"), que deve ser regido de acordo com as cláusulas que seguem:

1. São consideradas informações confidenciais, reservadas ou privilegiadas ("Informações Confidenciais"), para os fins deste Termo, independente destas informações estarem contidas em discos, disquetes, pen-drives, fitas, outros tipos de mídia ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre a Gestora, seus sócios e clientes, aqui também contemplados os próprios fundos, incluindo:

a) Know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador;

b) Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes, dos clubes, fundos de investimento e carteiras geridas pela Gestora;

c) Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os clubes, fundos de investimento e carteiras geridas pela Gestora;

d) Informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, trainees ou estagiários da Gestora ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (IPO), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da Gestora e que ainda não foi devidamente levado à público;

e) Informações a respeito de resultados financeiros antes da publicação dos balanços e balancetes dos fundos;

f) Transações realizadas e que ainda não tenham sido divulgadas publicamente; e

g) Outras informações obtidas junto a sócios, diretores, funcionários, trainees ou estagiários da Gestora ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

2. O Colaborador compromete-se a utilizar as Informações Confidenciais a que venha a ter acesso estrita e exclusivamente para desempenho de suas atividades na Gestora, comprometendo-se, portanto, a não divulgar tais Informações Confidenciais para quaisquer fins, Colaboradores não autorizados, mídia, ou pessoas estranhas à Gestora, inclusive, nesse último caso, cônjuge, companheiro(a), ascendente, descendente, qualquer pessoa de relacionamento próximo ou dependente financeiro do Colaborador.

2.1. O Colaborador se obriga a, durante a vigência deste Termo e por prazo indeterminado após sua rescisão, manter absoluto sigilo pessoal e profissional das Informações Confidenciais a que teve acesso durante o seu período em qualquer da Gestora, se comprometendo, ainda a não utilizar, praticar ou divulgar Informações Confidenciais, "Insider Trading", "Dicas" e "Front Running", seja atuando em benefício próprio, da Gestora ou de terceiros.

2.2. A não observância da confidencialidade e do sigilo, mesmo após o término da vigência deste Termo, estará sujeita à responsabilização nas esferas cível e criminal.

3. O Colaborador entende que a revelação não autorizada de qualquer Informação Confidencial pode acarretar prejuízos irreparáveis, ficando deste já o Colaborador obrigado a indenizar a Gestora, seus sócios e terceiros prejudicados, nos termos estabelecidos a seguir.

3.1. O descumprimento acima estabelecido será considerado ilícito civil e criminal, ensejando inclusive sua classificação como justa causa para efeitos de rescisão de contrato de trabalho, quando aplicável, nos termos do artigo 482 da Consolidação das Leis de Trabalho.

3.2. O Colaborador tem ciência de que terá a responsabilidade de provar que a informação divulgada indevidamente não se trata de Informação Confidencial.

4. O Colaborador reconhece e toma ciência que:

(i) Todos os documentos relacionados direta ou indiretamente com as Informações Confidenciais, inclusive contratos, minutas de contrato, cartas, fac-símiles, apresentações a clientes, e-mails e todo tipo de correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, planos de ação, modelos de avaliação, análise, gestão e memorandos por este elaborados ou obtidos em decorrência do desempenho de suas atividades na Gestora são e permanecerão sendo propriedade exclusiva da

Gestora e de seus sócios, razão pela qual compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na Gestora, devendo todos os documentos permanecer em poder e sob a custódia da Gestora, salvo se em virtude de interesses da Gestora for necessário que o Colaborador mantenha guarda de tais documentos ou de suas cópias fora das instalações da Gestora;

(ii) Em caso de rescisão do contrato individual de trabalho, desligamento ou exclusão do Colaborador, o Colaborador deverá restituir imediatamente à Gestora todos os documentos e cópias que contenham Informações Confidenciais que estejam em seu poder; e

(iii) Nos termos da Lei 9.609/98, a base de dados, sistemas computadorizados desenvolvidos internamente, modelos computadorizados de análise, avaliação e gestão de qualquer natureza, bem como arquivos eletrônicos, são de propriedade exclusiva da Gestora, sendo terminantemente proibida sua reprodução total ou parcial, por qualquer meio ou processo; sua tradução, adaptação, reordenação ou qualquer outra modificação; a distribuição do original ou cópias da base de dados ou a sua comunicação ao público; a reprodução, a distribuição ou comunicação ao público de informações parciais, dos resultados das operações relacionadas à base de dados ou, ainda, a disseminação de boatos, ficando sujeito, em caso de infração, às penalidades dispostas na referida lei.

5. Ocorrendo a hipótese do Colaborador ser requisitado por autoridades brasileiras ou estrangeiras (em perguntas orais, interrogatórios, pedidos de informação ou documentos, notificações, citações ou intimações, e investigações de qualquer natureza) a divulgar qualquer Informação Confidencial a que teve acesso, o Colaborador deverá notificar imediatamente a Gestora, permitindo que a Gestora procure a medida judicial cabível para atender ou evitar a revelação.

5.1. Caso a Gestora não consiga a ordem judicial para impedir a revelação das informações em tempo hábil, o Colaborador poderá fornecer a Informação Confidencial solicitada pela autoridade. Nesse caso, o fornecimento da Informação Confidencial solicitada deverá restringir-se exclusivamente àquela que o Colaborador esteja obrigado a divulgar.

5.2. A obrigação de notificar a Gestora subsiste mesmo depois de rescindido o contrato individual de trabalho, ao desligamento ou exclusão do Colaborador, por prazo indeterminado.

6. Tenho ciência dos direitos, obrigações e penalidades aplicáveis constantes da Lei n.º 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - "LGPD") e me comprometo a adotar todas as medidas necessárias para utilização dos dados e informações aos quais tiver acesso em decorrência das atividades desempenhadas em conformidade com o estabelecido pela LGPD e com as orientações acerca da privacidade e do tratamento de informações fornecidas pela Gestora.

6.1. Estou ciente, ainda, de meu compromisso de comunicar ao Encarregado, conforme definido pela Gestora, qualquer situação que chegue ao meu conhecimento que esteja em desacordo com as orientações acerca da privacidade e do tratamento de informações fornecidas pela Gestora.

6.2. Na qualidade de pessoa física titular de Dados Pessoais ("Titular de Dados Pessoais"), estou ciente e de acordo que cada uma da Gestora, na qualidade de "Controladora" para fins de atendimento às disposições da LGPD, tome decisões relativas ao Tratamento de meus Dados Pessoais , incluindo operações como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração ("Tratamento") durante todo o período em que eles forem pertinentes, observados os princípios e as garantias ora estabelecidas pela referida lei.

6.3. Também na qualidade de Titular de Dados Pessoais, estou ciente de que, a qualquer tempo, mediante requisição às Controladoras, tenho o direito de (i) confirmar a existência de Tratamento e acessar meus Dados Pessoais, (ii) corrigir dados incompletos, inexatos ou desatualizados, (iii) solicitar a anonimização, bloqueio ou eliminação de Dados Pessoais desnecessários, excessivos ou tratados em desconformidade com a LGPD, (iv) solicitar a portabilidade de meus Dados Pessoais a outro fornecedor de serviço, (v) solicitar a eliminação dos Dados Pessoais tratados com o meu consentimento, (vi) solicitar informações sobre o compartilhamento dos meus dados pelas Controladoras e sobre a possibilidade de não fornecer o consentimento e as consequências dessa negativa, e (vii) me opor ao Tratamento de meus Dados Pessoais em caso de descumprimento da LGPD. "Encarregado" é a pessoa indicada pela Gestora para atuar como canal de comunicação entre os Titulares dos Dados Pessoais e a Autoridade Nacional de Proteção de Dados. Para os fins do presente Termo de Compromisso são considerados Dados Pessoais toda informação relacionada a uma pessoa física que a torne diretamente identificada ou identificável.

6.4. Reconheço que as Controladoras poderão compartilhar os Dados Pessoais com outros agentes de Tratamento de dados, tais como escritórios de contabilidade, agências de turismo, planos de saúde e instituições financeiras, caso seja necessário, bem como que poderá compartilhar em seu website os Dados Pessoais, incluindo minha identificação como Colaborador da Gestora e meu histórico profissional, observados os princípios e as garantias ora estabelecidas pela LGPD, com o que, desde já, estou de acordo.

6.5. Estou ciente de que as Controladoras poderão manter armazenados os Dados Pessoais necessários após o término da relação contratual, por prazo determinado em lei, para fins de cumprimento de obrigações legais e/ou regulatórias, bem como para exercer seus direitos em processos administrativos e/ou judiciais.

6.6. Comprometo-me, enfim, a observar em tudo às instruções fornecidas pela Gestora, na qualidade de Controladoras, acerca do Tratamento que deverá ser concedido aos Dados Pessoais aos quais tiver acesso em razão de minhas atividades, bem como a sempre agir de acordo com as disposições da LGPD e das normas internas da Gestora quanto à privacidade e proteção de Dados Pessoais.

7. Este Termo é parte integrante das regras que regem a relação contratual e/ou societária do Colaborador com a Gestora, que ao assiná-lo está aceitando expressamente os termos e condições aqui estabelecidos.

8. A transgressão a qualquer das regras descritas neste Termo, sem prejuízo do disposto no item 3 e seguintes acima, será considerada infração contratual, sujeitando o Colaborador às sanções que lhe forem atribuídas pelos sócios da Gestora.

Assim, estando de acordo com as condições acima mencionadas, assinam o presente em 02 (duas) vias de igual teor e forma, para um só efeito produzirem, na presença das testemunhas abaixo assinadas.

[Cidade], [---] de [---] de [---].

Parte	Nome	CPF/MF	Endereço Eletrônico
Colaborador			
Contratante			
Testemunha 1			
Testemunha 2			

A Lei nº 14.620/2023 passou a conferir força executiva aos documentos constituídos ou atestados por meio eletrônico, que tenham sido assinados mediante o uso de qualquer modalidade de assinatura eletrônica prevista em lei, dispensando as assinaturas de testemunhas nos casos em que a integridade das assinaturas apostas pelas partes for conferida pelo provedor de assinatura (i.e. tal como já como ocorre quando há a assinatura com certificado digital emitido no âmbito da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil.).

ANEXO III

DECLARAÇÃO DE AFASTAMENTO POR NÃO CERTIFICAÇÃO

Por meio deste instrumento eu, _____, inscrito no CPF/MF sob o no _____, na qualidade de Colaborador da NAVORA – GESTÃO DE RECURSOS S/A ("Gestora"), declaro, para todos os fins, que:

(i) estou ciente de que, por não possuir atualmente a certificação exigível para o desempenho das minhas atividades conforme previsto no Manual Interno da Gestora, encontrarei-me imediatamente afastado de todas as atividades elegíveis até que regularize minha situação junto ao Conselho de Certificação;

(ii) comprometo-me a não exercer, direta ou indiretamente, quaisquer das atividades elegíveis da Gestora enquanto não obtiver a certificação correspondente ou não seja formalmente dispensado pelo Conselho de Certificação;

(iii) reconheço que meu afastamento perdurará até a apresentação de comprovante de certificação válida ou até a notificação oficial de isenção pelo Conselho de Certificação, data a partir da qual poderei retomar minhas funções;

(iv) declaro, finalmente, que recebi e compreendi todas as condições estipuladas neste Anexo III, estando ciente das implicações do não cumprimento destes requisitos.

[local], [data].

_____

[COLABORADOR]

A Lei nº 14.620/2023 passou a conferir força executiva aos documentos constituídos ou atestados por meio eletrônico, que tenham sido assinados mediante o uso de qualquer modalidade de assinatura eletrônica prevista em lei, dispensando as assinaturas de testemunhas nos casos em que a integridade das assinaturas apostas pelas partes for conferida pelo provedor de assinatura (i.e. tal como já como ocorre quando há a assinatura com certificado digital emitido no âmbito da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil.