MANUAL DE COMPLIANCE
(CONFORMIDADE e CONTROLES INTERNOS)

CORE CAPITAL

MANUAL DE COMPLIANCE
(CONFORMIDADE E CONTROLES INTERNOS)

Manual de Compliance (Conformidade e Controles Internos) ("Manual") da **Core Capital Gestora de Recursos Ltda.**, sociedade empresária limitada, inscrita no CNPJ sob o nº 45.695.771/0001-89, com sede na cidade e Estado de São Paulo, na Avenida Dr. Cardoso de Melo 878, sala 72, Vila Olimpia, CEP 04548-003 ("Gestora" ou "Core Capital").

INDEX

VERSÃO 02:
NOVEMBRO DE 2024

---

1. INTRODUÇÃO

Este Manual estabelece as diretrizes e normas que são mandatórias para todos os "Colaboradores" da Gestora, assim denominados os: (i) sócios; (ii) colaboradores; e (iii) quaisquer pessoas que possuam cargos, funções ou posições na Gestora.

O propósito deste Manual é definir os procedimentos, as normas de Compliance e os controles internos da Gestora, incluindo aspectos como confidencialidade, segurança da informação e segregação de atividades. Este Manual foi elaborado de acordo com os requisitos estabelecidos pela Comissão de Valores Mobiliários ("CVM") e pela Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("ANBIMA").

A Gestora atuará, exclusivamente, na administração de recursos de terceiros, através da gestão de fundos de investimento constituídos no Brasil ("Fundos") e de carteiras administradas ("Carteiras").

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

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

Cabe ressaltar que algumas políticas contidas neste Manual também se aplicam a familiares diretos, Fundos, Carteiras ou clubes de investimento e/ou entidades que são controladas direta ou indiretamente, ou administradas de forma discricionária, pelos Colaboradores. As especificidades estarão detalhadas nas respectivas políticas neste Manual.

2. ESTRUTURA ORGANIZACIONAL

A Alta Administração da Gestora

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

Os membros da Alta Administração são profissionais com profunda expertise e competência técnica, responsáveis pela eleição dos integrantes do Comitê de Risco e Compliance e pela indicação do Diretor de PLD/FTP. Este último assume adicionalmente as funções do Diretor de Risco e Compliance, e tem a responsabilidade de estabelecer diretrizes para prevenir a Lavagem

de Dinheiro, o Financiamento ao Terrorismo e a Proliferação de Armas de Destruição em Massa ("LD/FTP") na Gestora.

A Alta Administração é formada pelos Srs. (i) **PEDRO AUGUSTO MIRANDA NUNES**, sócio da Gestora e Diretor responsável pela administração de carteira de valores mobiliários, (ii) **THIAGO DE ANDRADE NEVES,** Diretor de Risco e Compliance; (iii) **CARLOS WALD REISSMANN,** sócio administração da Sociedade Controladora.

Diretor de Risco e Compliance

O diretor encarregado pelas políticas, regras, procedimentos e controles da Core Capital ("**Diretor de Risco e Compliance**") deverá conduzir suas atividades de forma independente, não podendo exercer quaisquer funções relacionadas à administração de carteiras de valores mobiliários, intermediação e distribuição e consultoria de valores mobiliários.

O diretor indicado pela Gestora para ocupar, cumulativamente, o cargo de Diretor de Compliance e Risco, Diretor de Prevenção a Lavagem de Dinheiro e ao Financiamento ao Terrorismo e membro do Comitê de Risco e Compliance, é o Sr. **THIAGO DE ANDRADE NEVES**.

São atribuições do Diretor de Risco e Compliance:

a. Monitorar e auditar o programa de Compliance da Gestora de forma periódica, bem como preservar registros e evidências dessas auditorias;

b. Manter e revisar o presente Manual, o Código de Ética, a Política de Compra e Venda de Valores Mobiliários, Investimentos Pessoais, além das demais políticas internas da Gestora;

c. Disponibilizar uma cópia atualizada deste Manual no site da Gestora e fornecer uma cópia para cada Colaborador anualmente e sempre que houver atualizações;

d. Garantir a obtenção do Formulário 'Conheça seu Colaborador' da Gestora, seja diretamente ou por meio de terceiro competente;

e. Coordenar a formação interna em Compliance, assegurando que esteja sempre atualizada de acordo com as leis e regulamentações pertinentes;

f. Coordenar e acompanhar quaisquer inspeções regulatórias;

g. Convocar, presidir e coordenar as reuniões do Comitê de Risco e Compliance;

h. Receber e responder prontamente a todas as perguntas e dúvidas dos Colaboradores sobre Compliance;

i. Registrar a conformidade de cada Colaborador com as políticas internas da Gestora, bem

como com as leis e regulamentações aplicáveis;

j. Comunicar quaisquer irregularidades à Alta Administração da Gestora e aos órgãos reguladores competentes, quando pertinente;

k. Assegurar a correta guarda das atas de reunião do Comitê de Risco e Compliance e das evidências de análises de Compliance, que possam ser pertinentes para futuras auditorias e inspeções regulatórias;

l. Elaborar o Relatório Anual de Compliance ("Relatório"), conforme a Resolução CVM 21, de 25/02/2021 e suas alterações. O Relatório, uma vez concluído, será apresentado à Alta Administração da Gestora, contendo as seguintes considerações;

- conclusões dos exames efetuados;

- propostas de correções para eventuais falhas identificadas, com o respectivo cronograma para solução destas, se for o caso; e

- obter a opinião do diretor responsável pela administração de carteiras de valores mobiliários ou, quando pertinente, do diretor responsável pela gestão de risco, sobre as deficiências constatadas nas verificações e as ações planejadas de acordo com cronograma específico ou as medidas já adotadas para resolvê-las.

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

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

Comitê de Risco e Compliance

O Comitê de Risco e Compliance da Gestora é órgão responsável pelo monitoramento e controle de risco da Gestora e é composto por pessoas naturais que reúnem a *expertise* e a capacidade técnica para exercer suas respectivas funções, inclusive (i) manter adequados e em funcionamento todos os sistemas de coleta, atualização e guarda de informações de políticas de "Conheça seus Cliente", "Conheça seu Colaborador" e "Conheça seu Prestador de Serviço"; (ii) manter os sistemas de monitoramento das operações e de situações atípicas alinhados com o nível de risco da Gestora; e (iii) fazer com que a Gestora aloque os recursos humanos e financeiros necessários suficientes para cumprimentos das leis, normas e regulamentações de PLD/FTP vigentes.

O Comitê de Risco e Compliance da Gestora também conduzirá uma revisão anual para assegurar a eficácia da Política de PLD/FTP e da aplicação do programa de treinamento de PLD/FTP contínuo para todos os Colaboradores da Gestora ("Programa"),assim como deliberar, sempre quando necessário, sobre qualquer ocorrência de atividade atípica ou suspeita, bem como quaisquer outras matérias sobre o assunto.

O Comitê de Risco e Compliance é formado pelo Sr. **THIAGO DE ANDRADE NEVES,** Diretor de Risco e Compliance; e (ii) por Lutfala Wadhy Neto (Analista de Risco e Compliance). As reuniões do Comitê de Risco e Compliance são presididas pelo Diretor de Risco e Compliance.

O Comitê de *Compliance* deverá se reunir, no mínimo, uma vez por mês, mediante convocação do Diretor de Risco e *Compliance* e, extraordinariamente, sempre que necessário.

O Comitê de *Compliance* é o órgão responsável por (i) deliberar sobre as políticas e procedimentos da Gestora; (ii) supervisionar sua aderência e implementação; (iii) analisar o impacto e cumprimento das leis e regulamentações vigentes e aplicáveis; (iv) deliberar sobre eventual descumprimento do presente Manual, do Código de Ética e demais políticas e suas consequências; (v) apurar e tomar as medidas relativas ao gerenciamento de risco, inclusive sobre risco de liquidez dos ativos e carteiras, definição de cenários de teste de estresse e limites de risco, além das demais situações que não estejam previstas nas políticas internas.

Além da Alta Administração e do Comitê de Compliance, o Anexo I deste Manual reflete ao organograma funcional da Gestora em vigor na data que este Manual foi elaborado.

3. CONFLITOS DE INTERESSE E POLÍTICA DE PRESENTES

Política de Conflitos de Interesse

Este Manual estabelece a Política de Conflitos de Interesse, cujo objetivo é gerenciar, mitigar e, quando possível, eliminar todos os conflitos de interesse reais ou potenciais que possam surgir das atividades da Gestora e de seus Colaboradores.

Os conflitos de interesse podem surgir quando um ou mais Colaboradores estão envolvidos em atividades ou relações que possam ser incompatíveis, em algum grau, com esta Política. Nestas situações, as condutas dos Colaboradores e as decisões de investimento podem entrar em conflito com suas funções na Gestora, comprometendo sua capacidade de julgamento ou a eficácia de suas atividades profissionais. Portanto, o Colaborador deve exercer discernimento antes de se envolver em qualquer atividade ou transação que possa causar um conflito de interesse.

Na execução de suas atividades, a Gestora e seus Colaboradores se comprometem a permanecer vigilantes e evitar situações em que seus interesses pessoais ou de terceiros possam entrar em conflito ou parecer contrários aos interesses da Gestora ou de seus clientes.

Se um conflito de interesse se tornar inevitável, cabe ao Diretor de Risco e Compliance (ou, na sua ausência, aos membros do Comitê de Risco e Compliance) avaliar o conflito de interesse em questão e tomar as medidas necessárias para minimizar seus riscos. Qualquer conflito que não possa ser prevenido ou evitado deve ser imediatamente comunicado ao Diretor de Risco e Compliance por qualquer Colaborador que o identifique.

Em último caso, Diretor de Risco e Compliance convocará uma reunião com a Alta Administração da Gestora para deliberar sobre os conflitos de interesse.

São exemplos de possíveis conflitos de interesse:

- ser proprietário ou administrador de uma empresa que negocia diretamente com a Gestora;

- ter um emprego ou interesses comerciais externos que possam interferir em sua capacidade de desempenhar seu trabalho na Gestora;

- ter influência significativa como acionista, diretor, funcionário, consultor ou agente de uma empresa, organização ou entidade concorrente da Gestora ou que tenha negócios atuais ou futuros, seja como cliente, fornecedor ou contratado da Gestora.

Os Colaboradores estão proibidos de exercer atividades externas, remuneradas ou não, que possam representar um conflito de interesses com os negócios da Gestora ou que impliquem na utilização indevida de informações, conhecimentos ou quaisquer outros recursos que sejam de propriedade da Gestora. Se um Colaborador desejar exercer atividades externas, remuneradas ou não, deve comunicar previamente o Diretor de Risco e Compliance para obter sua aprovação, a fim de evitar possíveis conflitos de interesse e comprometimento de sua dedicação ao trabalho na Gestora.

Presentes, Brindes e Entretenimento

Os Colaboradores da Gestora estão expressamente proibidos de receber qualquer forma de vantagem (como presentes, doações e brindes) de clientes, potenciais clientes, fornecedores e quaisquer terceiros que possam influenciar suas decisões ou ações dentro da Gestora.

Em geral, os Colaboradores são proibidos de solicitar e desencorajados a aceitar presentes de clientes, potenciais clientes ou parceiros que não sejam membros de suas famílias, a menos que o valor desses presentes não exceda R$ 500,00 (quinhentos reais). Caso o valor seja maior, a situação deve ser analisada e decidida pelo Diretor de Risco e Compliance.

Está expressamente proibido para os Colaboradores oferecer, prometer dar, receber ou prometer receber, em nome da Gestora, qualquer objeto de valor a qualquer colaborador de empresa atuante no mercado financeiro e de capitais ou órgãos reguladores, com a intenção de corrupção pública ou privada.

Ressaltamos que qualquer exceção a esta política, especialmente em relação à regra de R$ 500,00, deve ser claramente documentada e aprovada pelo Diretor de Risco e Compliance. A violação destas diretrizes poderá resultar em sanções disciplinares, incluindo a possibilidade de demissão e/ou desligamento do Colaborador.

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

Para esclarecer, as refeições realizadas durante uma reunião, seja na sede da Gestora ou em outro local, não serão consideradas presentes, mas despesas de representação.

4. POLÍTICA DE TREINAMENTO

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

O Diretor de Risco e Compliance da Gestora é encarregada de organizar, ou garantir a organização, de treinamentos, anuais e obrigatórios, de Compliance, observados os seguintes temas:

- Prevenção à Lavagem de Dinheiro;
- Anticorrupção e Confidencialidade;
- Práticas de mercado, produtos disponíveis e regulamentação aplicável; e
- Insider Trading.

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

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

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

5. POLÍTICA DE CONFIDENCIALIDADE

O presente Manual dispõe sobre a política de confidencialidade ("**Política de Confidencialidade**"), que tem como objetivo estabelecer os termos da confidencialidade das informações da Gestora e seus clientes.

A confidencialidade é um dos princípios norteadores das atividades desenvolvidas dentro do mercado financeiro e de capitais. O princípio da confidencialidade deverá reger e será aplicável a todas e quaisquer informações (i) não públicas da Gestora, (ii) obtidas pela Gestora no curso de suas atividades, e (iii) recebidas de clientes, ex-clientes ou potenciais clientes ("**Informações Confidenciais**").

Inclui-se na definição de Informações Confidenciais todas as comunicações orais e escritas, informais ou não, independentemente do meio enviado, seja presencialmente, por carta, impressão, correio eletrônico, assim como a informações geradas no computador ou aplicativo de comunicação.

Os Colaboradores da Gestora deverão proteger a confidencialidade das Informações Confidenciais que não sejam de domínio público, informações essas que tenham obtido ou criado em função das atividades que desempenham ou desempenharam junto à Gestora.

Nenhum Colaborador poderá revelar qualquer Informação Confidencial ou informação proprietária referentes à Gestora, seus Colaboradores, clientes, ex-clientes, clientes em potencial ou parceiros, a terceiros que não estejam autorizados a recebê-las ou sobre as quais não tenham necessidade de tomar conhecimento.

A única exceção é a revelação autorizada pelo cliente ou parceiro, ou requerida por lei ou autoridade competente, como por exemplo, os órgãos fiscalizadores de supervisão, em processo legal cabível.

Proteção das Informações de Clientes.
A Gestora e os seus Colaboradores reconhecem a sua obrigação de resguardar as informações recebidas ou que se refiram aos seus clientes e investidores de forma segura e confidencial.

É um compromisso da Gestora manter seguras as informações e usá-las de modo adequado, que preza pela confiança de seus clientes e Colaboradores.

Os Colaboradores também devem garantir que as informações recebidas sejam utilizadas apenas para as finalidades para as quais foram colhidas, salvo se outro tipo de utilização for permitido por lei ou normas internas.

Informações pessoais confidenciais somente poderão ser compartilhadas: (i) dentro da Gestora e quando seja necessária para a condução de seus negócios; (ii) com as afiliadas da Gestora e outras empresas, quando necessário para atender o cliente; e (iii) com os reguladores e/ou quando exigido por lei, norma, regulamentos ou ordem judicial emitida por

um tribunal de jurisdição competente, ou por um órgão, judiciário, administrativo ou legislativo; desde que, no entanto, o Comitê de Risco e Compliance seja consultado previamente para aprovação.

Quaisquer outras exceções para o compartilhamento de Informações Confidenciais, com pessoas não autorizadas, deverão ser revisadas e previamente aprovadas pelo Comitê de Risco e Compliance.

Informações sobre a Gestora deverão ser disponibilizadas apenas se tiverem um propósito legítimo da Core Capital. O compartilhamento de informações deve ser restrito e deverá ser feito com o entendimento de que as mesmas são confidenciais e devem ser utilizadas exclusivamente para o objeto restrito para o qual foram recebidas ou concedidas.

A Informação Confidencial só pode ser usada para fins profissionais e sob nenhuma hipótese deve ser utilizada para obtenção de quaisquer vantagens pessoais. É estritamente proibida a divulgação de informação para terceiros não envolvidos ou não autorizados a recebê-la.

O serviço de e-mail da Sociedade se encontra na nuvem, através da solução Office 365 Business da Microsoft e seu ambiente interno é garantido por dispositivo de segurança que executa funções de firewall e antivírus no nível do roteador. Além disso, uma proteção contra vírus é ativada em cada computador individual na rede de escritório. Com seus procedimentos de backup externo e acesso remoto a e-mails, a mesma pode continuar a funcionar mesmo que não possa ter acesso físico ao escritório. O backup externo é realizado por soluções da Microsoft.

6. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Este Manual estabelece a Política de Segurança da Informação ("**Política de Segurança da Informação**"), que orienta todos os colaboradores da Gestora. Seu principal objetivo é garantir a proteção de todas as informações significativas acessadas pelos colaboradores devido às suas funções ou cargos na Core Capital. Além disso, zela pela segurança das informações, incluindo aquelas armazenadas ou acessíveis nos equipamentos fornecidos pela Gestora para desempenho de suas funções. Cada colaborador é responsável pela preservação, integridade e confidencialidade dessas informações.

As informações são um recurso valioso para a operação das atividades da Gestora. Por essa razão, tal como qualquer outro ativo da Core Capital, devem ser tratadas com diligência, ética e profissionalismo. Todos os colaboradores são responsáveis por proteger as informações, independentemente da forma de armazenamento ou transmissão.

Além disso, a Gestora implementa um programa de segurança cibernética que inclui:

Identificação/Avaliação de riscos
A Gestora realiza uma avaliação de riscos regular e abrangente para identificar os riscos internos e externos. Esta avaliação inclui a identificação de todos os ativos relevantes da

Gestora, sejam equipamentos, sistemas, processos ou dados, usados para seu correto funcionamento. Além disso, a Gestora avalia as vulnerabilidades dos ativos em questão, identificando as possíveis ameaças e o grau de exposição dos ativos a elas. Vários cenários são considerados nessa avaliação, incluindo os possíveis impactos financeiros, operacionais e reputacionais, em caso de evento de segurança, assim como a expectativa de tal evento ocorrer.

Segue abaixo uma lista não exaustiva de alguns riscos de segurança cibernética identificados, na avaliação inicial:

a) Invasão sistêmica que prejudique dados internos, incluindo vírus ou ataque de hackers;

b) Comunicações falsas utilizando os dados coletados para ter credibilidade e enganar vítimas e comprometimento de estações de trabalho decorrente de cliques em link malicioso;

c) Exposição do ambiente devido a uma brecha de segurança, por diversos motivos como a instalação de software em contrariedade com as aprovações e condições estabelecidas nesta Política;

d) Vazamento de informações durante tráfego de dados não criptografados; ou

Medidas Preventivas.
A Gestora estabelece um conjunto de medidas cujo objetivo é mitigar e minimizar a concretização dos riscos identificados na avaliação de riscos. Isso inclui o controle do acesso adequado aos ativos da Gestora, a implementação de regras mínimas na definição de acesso a dispositivos corporativos, a disponibilização de autenticação de múltiplos fatores, a limitação do acesso a apenas recursos relevantes para o desempenho das atividades e a implementação de serviço de backup dos diversos ativos da Gestora.

Monitoramento e Testes.
A Gestora implementa um programa de monitoramento e testes para detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico. Isso inclui a criação de mecanismos de monitoramento de todas as ações de proteção implementadas, a manutenção de inventários atualizados de hardware e software, a realização de testes de invasão externa e phishing, e a análise regular dos logs e as trilhas de auditoria criados.

O ambiente de TI da Gestora será monitorado, por meio de indicadores e geração de históricos: (i) do uso da capacidade instalada da rede e dos equipamentos; (ii) tempo de resposta no acesso à Internet e aos sistemas críticos da Gestora; (iii) de períodos de indisponibilidade no acesso à Internet e aos sistemas críticos da Gestora; (iv) de incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante); e (v) das atividade de todos os Colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

Para garantir as regras mencionadas nesta Política, a Gestora deverá (a) para os riscos associados a Phishing, conduzir treinamentos e campanhas periódicas, bem como testes de Phishing, (b) realizar, a qualquer tempo, inspeção física nas máquinas de hardware;(c) instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso; (d) testar a vulnerabilidade e penetração do Website da Gestora, bem como de todo e qualquer sistema eletrônico desenvolvido internamente pela Gestora, ao menos anualmente.

Plano de Resposta

A Gestora mantém um plano de resposta a incidentes de segurança cibernética, que inclui a comunicação interna e externa necessária em caso de incidente. Este plano é revisado e atualizado regularmente para garantir que permaneça eficaz e relevante para as necessidades da Gestora. O plano de ação conta com mecanismos que asseguram a comunicação imediata para todos os colaboradores relevantes com relação a incidentes que possam gerar riscos à Core Capital, e prevê o acionamento dos colaboradores-chaves e contatos externos relevantes, inclusive de reguladores, considerando critérios e prazos vigentes, quando aplicável.

- Procedimento em caso de incidente - Uma vez que o Diretor de Risco e Compliance tenha sido acionado devido a um potencial incidente, este deverá atuar em conjunto com a área de TI para solução imediata do problema.

- Avaliação Inicial - Na etapa inicial, aspectos e decisões fundamentais deverão ser analisadas e tomadas após o incidente. Deverá ser realizada uma análise do que aconteceu, compreendendo motivos e consequências imediatas, bem como a gravidade da situação, devendo ser decidido a formalização ou não do incidente.

- Incidente Caracterizado - Se for caracterizado um incidente, devem ser tomar as medidas imediatas, que poderão abranger (i) se será registrado um boletim de ocorrência ou queixa crime, (ii) se há necessidade de informar à CVM, ANBIMA ou mais alguma autoridade, (iii) se é necessário envolver consultor ou advogado externo; (iv) se haverá comunicação interna ou externa, em especial a Investidor que eventualmente tenha sido afetado; e (v) se houve prejuízo para a Gestora, algum veículo de investimento ou investidor específico. Além disso, caso seja necessário, deverão ser definidos os passos a serem tomados sob o aspecto de cibersegurança, tais como iniciar a redundância de TI, redirecionar as linhas de telefone para os celulares, instruir o provedor de Telecom a desviar linhas de dados/e-mail.

- Recuperação - Essa fase começa após o incidente inicial ter sido contornado, já tendo sido a redundância de TI acionada e terceiros-chave notificados, caso necessário. Será realizado um acompanhamento, com um sumário elaborado pelo Responsável pela Segurança Cibernética contendo as medidas a serem tomadas, responsabilidades e prazos

Quaisquer dados faltando ou corrompidos, ou problemas identificados por Colaboradores da Gestora, devem ser comunicados. Colaboradores externos relevantes deverão ser mantidos atualizados, caso seja necessário.

- Retomada - Por fim, essa fase é a de transição ao modo normal de operação e pode incluir a análise de projetos, reconstrução de eventuais sistemas e eventuais mudanças e medidas de prevenção. Ademais, após eventual evento de contingência, o Diretor de Risco e Compliance deverá avaliar os prejuízos decorrentes da ocorrência e propor melhorias e investimentos para a redução dos riscos.

- Testes de Contingência - Os Testes de Contingência serão realizados com periodicidade mínima anual ou em virtude das mudanças ocorridas na Gestora que assim o justifiquem, de modo a permitir que a Gestora esteja sempre aprimorando sua infraestrutura para a continuação de suas atividades.

O objetivo do teste incluirá a avaliação se o Plano desenvolvido é capaz de suportar, de modo satisfatório, os processos operacionais críticos para a continuidade dos negócios da Gestora e manter a integridade, a segurança e a consistência dos bancos de dados criados pela alternativa adotada, e se o Plano pode ser ativado tempestivamente.

Os testes abrangerão os seguintes eventos, apenas de forma amostral, a saber:

- Testes dos nobreaks, verificando o status de funcionamento e do tempo de suporte das baterias com carga;
- Acesso aos sistemas e aos e-mails remotamente, de endereço externo;
- Acesso aos dados armazenados externamente; e
- Outros necessários à continuidade das atividades.
- O resultado de cada teste será registrado no documento de Teste de Contingência.

Governança
A Gestora mantém o programa de segurança cibernética continuamente atualizado garantindo que ações, processos e indicadores sejam regularmente executados, retroalimentando a estratégia definida. O Comitê de Risco e Compliance tem como uma de suas funções tratar de segurança cibernética dentro da Gestora, a revisão periódica do programa de segurança cibernética, a promoção e disseminação da cultura de segurança com a criação de canais de comunicação internos eficientes, e a definição e manutenção de indicadores de desempenho (key performance indicators).

Caso algum Colaborador identifique a conservação inadequada, utilização indevida de qualquer ativo (físico ou eletrônico) ou sistemas, deverá comunicar a ocorrência ao Diretor de Risco e Compliance.

O Diretor de Risco e Compliance será a responsável pela revisão da política cibernética e suas revisões, bem como para tratar e responder questões de segurança cibernética dentro da Gestora.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente ao Diretor de Risco e Compliance, devendo ser observado o procedimento previsto nesta Política

em caso de vazamento de informação confidencial.

O Diretor de Risco e Compliance irá se consultar com setor de tecnologia de informação, tendo como objetivo a supervisão e monitoramento das regras de Segurança Cibernética, conforme aqui previsto.

Um plano de contingência e a continuidade dos sistemas e processos operacionais críticos deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Todos os requisitos de segurança da informação e segurança cibernética, incluindo a necessidade de planos de contingência, serão previamente identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

A Gestora exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus Colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

As informações podem existir em diversos formatos, incluindo sistemas de informação, diretórios de rede, bancos de dados, arquivos físicos, dispositivos eletrônicos, equipamentos portáteis e até mesmo por meio da comunicação oral. Se algum colaborador identificar a má conservação ou uso indevido de qualquer recurso (físico ou eletrônico) ou sistemas, ele deverá comunicar o incidente ao Diretor de Risco e Compliance.

Descrições e Características

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

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

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

Todos os logs de sistemas são mantidos pela Gestora por um período de 5 anos. A Core Capital

verifica regularmente os padrões de todos os computadores, arquivos em rede, softwares, hardwares ou acessos não autorizados. Dessa forma, por meio dos logs, a Gestora consegue garantir a integridade, autenticidade e capacidade de auditoria das informações e sistemas.

Todas as declarações de imprensa (envolvendo ou não a Gestora) devem ser aprovadas previamente pelo Diretor de Risco e Compliance. Este poderá, a qualquer momento e sem aviso prévio, verificar o conteúdo das ligações telefônicas gravadas, os arquivos disponíveis no diretório interno e os e-mails enviados e recebidos. Isso não configura quebra de sigilo e tem como objetivo monitorar o cumprimento das normas de Compliance e regulamentações legais pertinentes à gestão de Fundos e Carteiras.

O descarte de informações confidenciais armazenadas digitalmente deve ser realizado de maneira a impossibilitar sua recuperação. Documentos físicos contendo informações confidenciais que não precisam ser arquivados devem ser descartados imediatamente após seu uso, impedindo sua recuperação ou leitura.

Em determinadas situações, para evitar a comunicação entre certos colaboradores ou departamentos, as áreas de Compliance e Tecnologia podem implementar barreiras de informação. Isso preserva a confidencialidade de certas informações confidenciais e impede sua comunicação entre diferentes áreas da Gestora. Os colaboradores não devem compartilhar informações confidenciais sujeitas a barreiras de informação com outras áreas sem a aprovação prévia do Diretor de Risco e Compliance.

A Gestora deverá proteger continuamente todos os ativos de informação da Gestora contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso ou indesejado.

7. PROCEDIMENTO DE TESTES PERIÓDICOS

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

Para cada teste de Compliance realizado, ao Diretor de Risco e Compliance deve emitir um relatório contendo recomendações sobre possíveis deficiências identificadas, bem como estabelecer um cronograma de correção, quando aplicável. Esses relatórios devem ser incluídos no Relatório.

O Relatório deve observar e conter os seguintes elementos:

a. Análise e verificação da reputação ilibada dos Diretores e controladores da Gestora;

b. Análise e verificação de possíveis ajustes realizados em políticas e documentos da Gestora, originados de mudanças regulatórias, exigências das autoridades reguladoras ou como consequência de mudanças internas, decisões gerenciais ou observações recebidas durante processos de due diligence;

c. Análise e verificação do descumprimento dos Códigos e demais políticas internas da Gestora por parte dos Colaboradores. Deve ser relatado como foram resolvidas as ocorrências de desvios profissionais mais graves, se estes resultaram em sanções e/ou consequências para a Gestora e o Colaborador em questão, e quais medidas foram tomadas para prevenção futura;

d. Confirmação de que o programa de treinamento dos Colaboradores, estabelecido previamente, foi devidamente cumprido, conforme indicado no item 4 deste Manual;

e. Confirmação de que a Política de Conflitos de Interesse está sendo eficazmente cumprida, conforme indicado no item 3 deste Manual;

f. Confirmação de que a Política de Confidencialidade é eficaz, juntamente com a existência de testes periódicos de segurança dos sistemas;

g. Confirmação de que a Política de Gestão de Risco foi cumprida, e se está de acordo com as normas e regulamentos;

h. Relato de possíveis desvios e desenquadramentos ocorridos no cumprimento do mandato pelo respectivo administrador de carteiras de valores mobiliários de terceiros, e quais medidas foram adotadas;

i. Indicação de que a atuação de terceiros contratados para a prestação de serviços está adequada, inclusive em relação à sua qualificação. Caso aplicável, devem ser apontadas eventuais rupturas de contratos motivadas por situações que possivelmente representavam riscos aos Fundos ou Carteiras da Gestora e aos investidores/clientes da Core Capital; e

j. Apresentação de estatísticas dos eventos ocorridos ao longo do ano, seu diagnóstico e aprimoramentos, no que se refere aos riscos operacionais.

A Gestora tem um sistema de processos internos para incluir todas as rotinas e procedimentos relacionados ao cumprimento da regulamentação em vigor e da sua Política de Gestão de Risco.

Todas as rotinas e procedimentos da área de Gestão de Risco devem variar de acordo com o tipo de risco envolvido, levando em conta a operação objeto do controle. A área de risco trabalhará de maneira preventiva e constante para alertar, informar e solicitar providências ao gestor em relação a eventuais desenquadramentos de limites normativos e daqueles estabelecidos internamente pela Gestora.

A Gestora contratará a utilização do sistema para gestão de Risco chamado Bloomberg Terminal. Este sistema fornece informações sincronizadas sobre as carteiras geridas, como marcação a mercado de ativos, posição e rentabilidade na forma percentual. Além disso, fornece dados dos ativos e passivos, associados a métricas de risco para acompanhamento das posições.

8. PROCEDIMENTO INTERNO DE REPORTE DE VIOLAÇÕES À CVM

O presente Manual dispõe sobre o procedimento interno de reporte de violações à CVM ("**Procedimento**"), que estabelece normas e procedimentos, a serem utilizados por todos os Colaboradores que tenham acesso a informações relevantes sobre a Gestora ou sobre suas estratégias de investimento com a finalidade de assegurar a comunicação à CVM de quaisquer violações às regulamentações emitidas por esta Autarquia.

Todos os Colaboradores deverão comunicar imediatamente ao Diretor de Risco e Compliance a identificação ou suspeita de quaisquer violações.

Em caso de violações relativas à legislação expedida pela CVM, ao Diretor de Risco e Compliance, deverá analisar o cadastro, as operações ou transações pertinentes. Após o prazo para regularização de eventuais situações de não conformidade, ou caso a suspeita se confirme após todas as análises, o Diretor deve apresentar um relatório sobre o caso. Este relatório deve incluir uma recomendação sobre se o caso deve ou não ser comunicado ao Conselho de Controle de Atividades Financeiras (COAF), a unidade de inteligência financeira do Brasil, ao Comitê de Risco e Compliance para deliberação.

A constatação de ilicitude não é condição para que o Comitê de Risco e Compliance determine a comunicação de uma operação suspeita ao COAF. Basta que o Comitê estabeleça, de maneira consistente e fundamentada, que a operação é atípica.

Após a deliberação do Comitê de Risco, ao Diretor de Risco e Compliance deve comunicar ao COAF, dentro do prazo regulatório, quaisquer transações ou propostas de transação que possam ser consideradas indícios sérios de infração.

Cada comunicação deve ser feita individualmente e fundamentada de maneira detalhada, contendo, quando aplicável, as seguintes informações:

a. data de início e natureza do relacionamento com a Gestora;

b. explicação fundamentada dos sinais de alerta identificados;

c. descrição e o detalhamento das características das operações realizadas;

d. apresentação das informações obtidas por meio das diligências previstas Resolução CVM nº 50 de 31 de agosto de 2021, que qualifiquem os envolvidos, inclusive informando tratar-se, ou não, de PPE, e que detalhem o comportamento da pessoa comunicada; e

e. conclusão da análise, incluindo o relato fundamentado que caracterize os sinais de alerta identificados como uma situação suspeita a ser comunicada ao COAF.

As conclusões de suas análises sobre operações ou propostas que fundamentaram a decisão de fazer ou não as comunicações mencionadas devem ser mantidas por um período de 5 (cinco) anos, ou por um prazo maior se expressamente determinado pela CVM, em caso de processo administrativo.

Se a Gestora não comunicar ao COAF durante um determinado ano civil, deve informar à CVM, até o último dia útil de janeiro do ano subsequente, por meio de sistema eletrônico disponível no site da CVM, que não ocorreram transações ou propostas de transações que necessitassem ser comunicadas no ano civil anterior.

9. SEGREGAÇÃO DE ATIVIDADES

Inicialmente, cumpre esclarecer que a Gestora atua exclusivamente como administradora de carteiras de valores mobiliários, na categoria de gestão de recursos de terceiros, não prestando, portanto, quaisquer outros serviços no mercado de capitais.

Em razão disso, não é suscitada qualquer hipótese de conflito no nível da Gestora. Não obstante, a Gestora manterá a devida segregação entre as suas áreas e implementará controles que monitorem a execução das atividades, a fim de garantir a segurança das informações e impedir a ocorrência de fraudes e erros.

A segregação de atividades é um requisito essencial para que seja dado o efetivo cumprimento às suas estratégias de administração de recursos de terceiros.

O Diretor de Risco e Compliance possui total autonomia e independência em suas decisões para questionar os riscos assumidos nas operações realizadas, sendo possível a aplicação das ações disciplinares cabíveis, independente de nível hierárquico, sem que seja necessária a validação prévia dos Diretores ou demais sócios da Gestora.

A Área de Compliance atua de forma autônoma e independente, se reportando ao Diretor de Risco e Compliance.

A Gestora adota um conjunto de procedimentos estabelecidos pelo Diretor de Risco e Compliance, com o objetivo de proibir e impedir o fluxo de informações privilegiadas e/ou sigilosas para outros departamentos, ou Colaboradores, da instituição que não estejam diretamente envolvidos na atividade de administração de recursos de terceiros.

A Gestora realizará os melhores esforços para que a segregação das informações e suas atividades sejam sempre preservadas. Com o intuito de assegurar a completa segregação, os seguintes procedimentos operacionais serão adotados:

- **Instalação Física com limitação de acesso de terceiros**. Serão adotadas medidas adicionais para garantir a devida segregação física das operações da Gestora,

delimitando, também, as áreas para discussões confidenciais e a aplicação de políticas rígidas que proíbem tais discussões em espaços compartilhados;

- **Segregação Informacional**. Todos os Colaboradores devem observar e respeitar as Políticas da Gestora e a segregação informacional absoluta e inviolável entre a Gestora e qualquer sociedade com a qual os Colaboradores tenham relacionamento. Os equipamentos da Gestora devem ser utilizados apenas por aqueles autorizados e em circunstâncias específicas. Adicionalmente, a gestão e proteção das informações comuns serão reforçadas através do uso de tecnologia segura e práticas de gerenciamento de dados;

- **Informações Confidenciais**. É imperativa a preservação de informações confidenciais por todos os seus Colaboradores, proibindo a transferência de tais informações a pessoas não habilitadas ou que possam vir a utilizá-las indevidamente, em processo de decisão de investimento, próprio ou de terceiros;

- **Treinamento de Compliance**. Idealização, implantação e manutenção de programa de treinamento de Colaboradores que tenham acesso a informações confidenciais e/ou participem de processo de decisão de investimento. O programa incluirá orientações claras sobre as políticas de confidencialidade, expectativas de comportamento e as consequências para o não cumprimento dessas políticas. A participação de todos os Colaboradores relevantes será obrigatória e registrada para garantir a conformidade; e

- **Acesso Restrito**. Acesso restrito a arquivos, bem como à adoção de controles que restrinjam e permitam identificar as pessoas que tenham acesso às informações confidenciais.

Dessa forma, a Gestora acredita que as medidas acima relacionadas são eficazes para cumprir os requisitos mínimos de segregação de atividades aplicados a sua realidade, buscando servir adequadamente seus clientes e cumprir com suas obrigações.

10. CONSIDERAÇÕES FINAIS

Este Manual não substitui a obrigação que cada Colaborador tem de usar o bom senso, discernimento e de, sempre que necessário, em caso de dúvidas, contatar o Diretor de Risco e Compliance diretamente ou através do e-mail compliance@corecapital.com.br.

Quaisquer solicitações de exceções às regras descritas neste Manual devem ser encaminhadas ao Diretor de Risco e Compliance, que verificará a solicitação e determinará a necessidade (ou não) de encaminhá-la ao Comitê de Risco e Compliance. O Comitê de Risco e Compliance por sua vez possui amplos poderes para aprovar exceções a este Manual, desde que a razão, natureza, prazo, e outras informações importantes sobre a decisão sejam devidamente formalizadas, sempre respeitando as leis e regulamentações aplicáveis.

Mediante a contratação/início do relacionamento profissional, e anualmente, todos os Colaboradores deverão aderir a este Manual através do preenchimento e assinatura do Formulário 'Conheça seu Colaborador' que será disponibilizado pelo Diretor de Risco e Compliance.

O Diretor de Risco e Compliance atualizará este Manual dentro de um período de tempo razoável depois que ocorrerem mudanças nas leis e normas aplicáveis, ou sempre que considerar apropriado. A versão atualizada do Manual deverá ser aprovada pelo Comitê de Risco

e Compliance e, subsequentemente, divulgada a todos os Colaboradores e no website da Gestora www.corecapital.com.br