



REGRAS DE *COMPLIANCE*,
PROCEDIMENTOS E CONTROLES INTERNOS

HECTARE CAPITAL GESTORA DE RECURSOS LTDA.

APRESENTAÇÃO DA GESTORA

(i) Perfil

A Hectare Capital Gestora de Recursos Ltda. (“Hectare” ou “Gestora”) tem como principal foco a atividade de gestão de fundos de investimentos, com expertise na gestão tanto de ativos líquidos como de ativos ilíquidos (caso dos FIDCs e FIIs).

(ii) Filosofia de Investimento

A filosofia de investimento da Hectare Capital é baseada em profunda análise fundamentalista e controle de riscos rigorosos. Acreditamos na importância de entender detalhadamente cada um dos mercados alvos, com o objetivo de identificar assimetrias positivas de risco x retorno. Com isso, buscamos construir um portfólio balanceado, privilegiando empresas e projetos que se enquadrem em nossos 3 pilares de gestão: (i) modelo de negócios com diferencial competitivo; (ii) governança sólida e transparente (iii) retorno atrativo.

Diferencial Competitivo – Projetos com vantagens competitivas estruturais: potencial de crescimento acima de seu custo de capital, modelo de negócios estruturado e alto potencial de geração de caixa.

Governança – Acreditamos que governança, controle e transparência são fatores essenciais para o sucesso dos projetos. Para tanto, é indispensável que os líderes dos projetos e suas equipes sejam competentes e tenham interesses alinhados para entregar os resultados esperados.

Retorno – Buscamos projetos que apresentem assimetrias relevantes de risco x retorno, proporcionando margem de segurança para o investimento. Acreditamos que a disciplina na análise é essencial para maximizar retornos e para gerir os riscos associados, reduzindo assim a ocorrência de investimentos que resultem em perda permanente de capital.

(iii) Vigência e Atualização

A presente Política de Regras de *Compliance*, Procedimentos e Descrição dos Controles Internos entra em vigor na data de sua aprovação e fica disponível no site da Gestora. Cabe ao Diretor de *Compliance* da Gestora rever e atualizar tal documento anualmente, ou sempre que constatado a necessidade de atualização de seu conteúdo, ainda que não decorrido o prazo de 1 (um) ano.

POLÍTICA DE COMPLIANCE

SEÇÃO I – REGRAS DE COMPLIANCE, PROCEDIMENTOS E DESCRIÇÃO DOS CONTROLES INTERNOS

(i) *Estrutura de Governança do Compliance*

A Gestora mantém uma política de *compliance* abrangente e integrada que é alicerçada num sistema interno de controle de práticas de negócio apoiado por normas vigentes e aplicáveis à Gestora, recursos humanos e infraestrutura técnico/tecnológica, e governança alinhada com os objetivos da empresa.

Nesse sentido, procura-se assegurar:

- a) a aderência da Gestora e seus Colaboradores às regulamentações em vigor da CVM, ANBIMA e demais reguladores aplicáveis;
- b) que todos os seus profissionais atuem com imparcialidade e conheçam o Código de Ética e Conduta, as normas aplicáveis e as demais Políticas Internas da Gestora;
- c) a eliminar conflitos de interesses, identificando, administrando e coibindo eventuais situações que possam afetar a imparcialidade das pessoas no desempenho de suas funções;
- d) a confidencialidade de informações que a Gestora e seus Colaboradores têm acesso no exercício de suas atividades;
- e) a condução e continuidade dos negócios; e
- f) o funcionamento do programa de treinamentos sobre as Políticas Internas da Gestora para todo o quadro de Colaboradores, com reciclagem anual.

Responsável: Sr. Andre Catrocchio, Diretor de *Compliance* da Hectare.

(ii) *Atribuições e Responsabilidades da Diretoria de Compliance*

É de responsabilidade da Diretoria e da área de *Compliance* da Gestora:

- a) Assegurar a conformidade com a legislação, as normas, os regulamentos, as políticas internas e suas atualizações;
- b) Auxiliar na informação e na capacitação de todos os Colaboradores e dos prestadores de serviços terceirizados relevantes, em assuntos relativos à conformidade;
- c) Assegurar o funcionamento do programa de *compliance* na Gestora;
- d) Assegurar o funcionamento do programa de prevenção à lavagem de dinheiro na Gestora (sistemas, processos, procedimentos e treinamentos);
- e) Monitorar e prevenir riscos de vazamento de informações;

- f) Adotar procedimentos para coibir o conflito de interesses;
- g) Assegurar o funcionamento o processo de *due diligence* para avaliação de novos parceiros, intermediários, fornecedores e terceiros relevantes;
- h) Instaurar e executar testes de controles internos, compliance e prevenção à lavagem de dinheiro para assim, identificar eventuais riscos e elaborar planos de mitigação;
- i) Elaborar relatório, com periodicidade mínima anual, contendo o sumário dos resultados das atividades relacionadas ao *compliance*, suas principais conclusões e planos de ações a tomar pela administração da Gestora;
- j) Revisar, aprimorar e aprovar as regras e diretrizes do programa de *compliance*;
- k) Deliberar penalidades para os Colaboradores que descumprirem o Código de Ética e demais políticas internas da Gestora;
- l) Garantir que todos os processos de *compliance* estejam em conformidade através da realização de monitoramento contínuo; e
- m) Adequar seu programa conforme o mapeamento de atividades de todas as áreas e legislação vigente, e com autonomia para realizar testes esporádicos, sempre que necessário.

(iii) Garantia de Independência

A Diretoria de *Compliance* é independente das demais áreas da Gestora e poderá exercer seus poderes em relação a qualquer Colaborador, independentemente de sua posição hierárquica.

Apurado o descumprimento das regras inerentes à atividade da Gestora, bem como outras disposições deste documento, o infrator estará sujeito a ação disciplinar, e conforme a gravidade do caso, também estará sujeito a outras penalidades, dentre as quais: (i) advertência; (ii) demissão por justa causa; (iii) destituição do cargo de administrador; ou (iv) exclusão do quadro societário.

(iv) Relatórios

A Diretoria de *Compliance*, também responsável pela implementação e cumprimento de regras, políticas, procedimentos e controles internos, disponibiliza à Diretoria da Gestora e à Administradora Fiduciária dos fundos sob gestão, até o último dia útil do mês de abril de cada ano, os Relatórios Anuais de Controles Internos e PLDFT relativo ao ano civil imediatamente anterior à data de entrega (conforme Resoluções CVM nº 21/21 e nº 50/21), contendo: (a) as conclusões dos exames efetuados; (b) as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e (c) a manifestação do diretor responsável pela administração de carteiras de valores mobiliários ou, quando for o caso, pelo diretor responsável pela gestão de risco a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las.

(v) Violações ao Código de Ética e Conduta, às Regras de Compliance e Outras Políticas Internas da Gestora

Denúncias e manifestações por parte de Colaboradores ou de terceiros que tenham conhecimento de violações a esta Política de *Compliance* ou outras políticas internas da Gestora, bem como quaisquer informações acerca de eventual descumprimento de dispositivos legais e normativos aplicáveis deverão ser feitas diretamente para a Diretoria de Compliance, para o [Canal de Ética](https://app.compliasset.com/hectarecapital) (<https://app.compliasset.com/hectarecapital>), ou para o e-mail canaldeetica@hectarecapital.com.br.

O teor das denúncias deve ser sempre o mais completo possível, a fim de possibilitar o início de eventual processo de investigação, sendo imprescindíveis as informações: (i) época em que ocorreu a infração; (ii) infratores envolvidos; (iii) área/ departamento da ocorrência; (iv) detalhes do conteúdo da infração; (v) evidências e/ou testemunha da infração; (vi) se houve valor financeiro envolvido; e, mas não se limitando a (vii) sugestão para solução e prevenção de novas infrações semelhantes.

Uma violação passível de punições da Gestora poderá ocorrer mediante a qualquer ação, participação ou omissão que esteja em desacordo com a legislação vigente e normas internas da Gestora.

Será assegurado a não retaliação para o denunciante de boa-fé e qualquer outro terceiro (que não seja o infrator ou o que facilitou a infração) que contribuir com informações ou der assistência no decurso da investigação. A confidencialidade das informações e do(s) denunciante(s) também será preservada e o mínimo de pessoas será envolvido no processo da investigação.

Classificação do documento:

Confidencial Interno Público

SEÇÃO II – OUTROS CONTROLES OPERACIONAIS

PLANO DE CONTINUIDADE DE NEGÓCIOS

(i) Objetivo

O objetivo deste Plano de Continuidade de Negócios (“PCN”) é assegurar a continuidade dos negócios na ocorrência de eventos que impliquem na impossibilidade da condução da operação normal da gestora em suas instalações principais. Nesse sentido, a Gestora adota uma série de medidas e procedimentos, incluindo as atribuições e responsabilidades de cada Colaborador, no sentido de executar este PCN.

O PCN possui o escopo precípua de dar continuidade às atividades consideradas críticas para a prestação de serviços pela Gestora, de modo que os interesses dos cotistas não sejam prejudicados.

O PCN é responsabilidade da área de *Compliance*, a quem cumprirá garantir que o referido plano esteja em conformidade com as leis e normas dos órgãos reguladores aplicáveis, bem como zelar por sua atualização e seu pleno funcionamento.

Na ocorrência de qualquer evento que impossibilite seu acesso ou permanência nas dependências principais da Gestora, os Colaboradores devem imediatamente contatar o departamento de *Compliance* que avaliará as atividades em andamento e orientará os Colaboradores quanto à continuidade das atividades fora das dependências principais, assim como se devem permanecer em suas residências ou se dirigir a um local previamente determinado durante sua jornada de trabalho.

(ii) Arquitetura do Ambiente Computacional

A Gestora utiliza o sistema de nuvem para *backup* de seus dados, possibilitando o fácil acesso às últimas versões de cada arquivo para restauração. O ambiente operacional da Gestora é pensado para utilizar o máximo de recursos computacionais na nuvem, garantindo contingência contra incidentes e desastres originados por fatores sistêmicos, físicos ou sociais.

Os Colaboradores da Gestora possuem acesso remoto aos seus e-mails e à nuvem de arquivos da empresa, de modo que podem acessá-los de fora do escritório, se necessário. Os registros contábeis da Gestora ficam com o contador responsável e as informações sobre os fundos de investimento geridos, com a respectiva instituição administradora.

(iii) Principais contingências mapeadas e respostas do PCN

Com isso, diante dos riscos de continuidade de negócios que a Gestora poderia enfrentar, foram estabelecidos os seguintes controles:

Classificação do documento:

Confidencial Interno Público

- Backup das planilhas e bancos de dados operacionais diariamente;
- Manutenção de uma lista virtual (na Intranet da Gestora) em local de fácil acesso com o telefone dos fornecedores de sistemas e pessoas responsáveis para solucionarem problemas no menor tempo possível;
- Plano alternativo de comunicação (pelo telefone 011 3849-7766 ou diretamente pelo endereço: Rua Fidêncio Ramos, 195, cj. 71);
- Espaço operacional alternativo (sede do Grupo RTSC, além da possibilidade de realizar *home office*) caso ocorra uma prolongada impossibilidade de se utilizar as facilidades do escritório durante um longo período;
- Plano para substituição de pessoal em caso de saída: documentação de atividades, redistribuição de tarefas, contratação de novo funcionário ou realocação interna.

Também foram adotadas outras ações pela Gestora que visam garantir a continuidade de suas operações em caso de incidentes/ desastres, dentre os quais podem ser destacados:

1. Queda de energia

Há *No-break* para até 1 (uma) hora. Em caso de falta de energia para períodos maiores que 1 (uma) hora, o acesso dos dados e arquivos será feito remotamente.

2. Queda do link para acesso à internet

Utilização de conexão de redundância com links de diferentes operadoras, ou seja, quando o acesso à Internet de uma operadora cai, imediatamente o serviço de outra operadora é acionado. Caso nenhuma das contingências funcione, é possível ainda fazer o acesso remoto aos arquivos hospedados na nuvem através de outros provedores e localizações.

3. Falha na disponibilização do e-mail

Serviço de e-mail é hospedado em nuvem, com acordo de nível de serviço elevado, garantindo a continuidade do acesso remoto. Além disso, há meios alternativos de comunicação como pelo telefone (011 3849-7766) ou diretamente pelo endereço (Rua Fidêncio Ramos, 195, cj. 71).

4. Falha na comunicação entre os Colaboradores

Todos os Colaboradores dispõem de acesso a e-mails e chat virtual interno, de forma remota, bem como o contato uns dos outros, para a eventualidade dos serviços de telefonia encontrarem-se indisponíveis.

5. Contingências com Computadores

Caso haja alguma falha em algum computador, a Gestora possui equipamentos reservas para serem utilizados pelo(s) Colaborador(es) afetado(s). Uma vez que todos os arquivos são armazenados na nuvem, no momento que um computador de contingência entra em uso, ele já terá acesso a todos os recursos necessários para continuidade do trabalho.

6. Invasão da intranet por hackers

A rede local da Gestora conta com firewall, com monitoramento e alertas de segurança. Além disso, contribui para um baixo risco deste tipo de invasão a ausência de servidores na rede local, uma vez que todos os serviços estão hospedados na nuvem.

Classificação do documento:

Confidencial Interno Público

CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO

(i) Introdução

A obrigação de confidencialidade é um princípio fundamental nas funções de todos os Colaboradores da Gestora, considerando quaisquer informações não-públicas referentes aos negócios da Gestora, como também informações recebidas de seus clientes, contrapartes ou fornecedores da Gestora durante o processo natural de condução dos negócios.

Os Colaboradores estão obrigados a manterem sigilo de qualquer informação relevante a que tenha acesso privilegiado até sua divulgação ao público em geral. Além disso, os Colaboradores devem zelar para que subordinados e terceiros de sua confiança também o façam.

Os Colaboradores devem preservar a confidencialidade de informações relativas a operações em andamento, bem como informações recebidas de entidades/pessoas cuja publicidade ou publicação possa influenciar o mercado.

As regras de confidencialidade aqui dispostas devem ser observadas durante a vigência do relacionamento profissional do Colaborador com a Gestora e após o seu término. Os Colaboradores, para tanto, assinam o Termo de Confidencialidade, quando de seu ingresso na Gestora.

(ii) Confidencialidade

Todas as informações concernentes a sistemas, negócios, estratégias, posições ou clientes da Gestora são confidenciais e devem ser assim tratadas, sendo utilizadas tão somente para possibilitar o desempenho das atribuições na Gestora e sempre em benefício dos interesses desta e de seus clientes.

Toda e qualquer informação que os Colaboradores tiverem com relação aos clientes da Gestora deve ser mantida na mais estrita confidencialidade, não podendo ser divulgada sem o prévio e expresso consentimento do cliente, salvo na hipótese de decisão judicial específica que determine à Gestora a prestação de informações ou, extrajudicialmente, em razão de procedimento fiscalizatório de autoridade competente, especialmente da Comissão de Valores Mobiliários ("CVM").

Todo Parceiro, Fornecedor e demais Terceiros que tiverem acesso a informações estratégicas ou confidenciais da Gestora são submetidos à devida diligência sobre o programa de segurança da informação, assinatura de "NDA" ("Non-disclosure Agreement" ou "Acordo de Não divulgação") e, se oficializar um contrato, o documento preverá cláusulas de confidencialidade e de segurança da informação.

Os Colaboradores devem se esforçar para garantir que os prestadores de serviços que porventura

venham a trabalhar junto à Gestora, tais como, instituições administradoras de fundos de investimento, distribuidores de títulos e valores mobiliários, escritórios de advocacia, corretores, agentes autônomos, entre outros, mantenham a confidencialidade das informações apresentadas, sejam tais informações dos clientes ou das operações realizadas pela Gestora. Neste sentido, qualquer conduta suspeita deve ser informada imediatamente e por escrito à Diretoria de *Compliance* ou ao [Canal de Ética](#) da Gestora, para que sejam tomadas as medidas cabíveis.

A Gestora exige que seus Colaboradores atuem buscando a garantia da confidencialidade das informações às quais tiverem acesso. Assim, é recomendável que os Colaboradores não falem a respeito de informações obtidas no trabalho em ambientes públicos, ou mesmo nas áreas comuns das dependências da Gestora, e que tomem as devidas precauções para que as conversas por telefone se mantenham em sigilo e não sejam ouvidas por terceiros.

Todo e qualquer material com informações de clientes ou de suas operações é mantido nas dependências da Gestora, sendo proibida a cópia ou reprodução de tais materiais, salvo mediante autorização expressa do superior hierárquico do Colaborador. Ainda, todo e qualquer arquivo eletrônico recebido ou gerado pelo Colaborador no exercício de suas atividades deve ser salvo no diretório exclusivo do cliente ou do projeto a que se refere tal arquivo eletrônico.

Para fins de manutenção das informações confidenciais, os Colaboradores da Gestora devem (i) bloquear o computador quando não o estiver utilizando; (ii) manter anotações, materiais de trabalho e outros materiais semelhantes sempre trancados em local seguro; (iii) descartar materiais usados, destruindo-os fisicamente e (iv) jamais revelar a senha de acesso aos computadores ou sistemas eletrônicos, além do sistema impor a troca de senha periodicamente.

A Gestora concede autorização de acesso aos Colaboradores apenas para as informações e arquivos que se refiram ao departamento no qual o Colaborador atua.

(iii) Segurança da Informação

No que diz respeito à infraestrutura tecnológica, destacamos que todas as informações, sejam dos fundos geridos ou das operações a eles relacionadas, ficam armazenadas em serviços de armazenamento de dados na nuvem (*cloud computing*), cujo acesso é permitido apenas aos administradores da Hectare, além dos membros da área de tecnologia.

Todo software disponibilizado aos Colaboradores deverá ser utilizado exclusivamente para os negócios da Gestora, em conformidade com os acordos de licenciamento firmados.

É realizado o back-up de todas as informações armazenadas no CPD, com vistas a evitar a perda de informações, e viabilizando sua recuperação em situações de contingência.

O acesso aos sistemas de informação da Gestora é feito através de “usuário/senha” que permite que seja acompanhado, de forma precisa, as atividades desenvolvidas por cada um dos Colaboradores. O controle desses dados é de domínio da Gestora, uma vez que o armazenamento

dos dados ocorre em servidores próprios, garantindo, assim, a confidencialidade e confiabilidade da informação.

A concessão de acessos é avaliada conforme o envolvimento de cada colaborador com responsabilidades e/ou projetos específicos.

Todo Colaborador que tiver acesso aos sistemas de informação da Gestora é responsável por tomar as precauções necessárias a fim de impedir o acesso não autorizado aos sistemas. O Colaborador deve manter em local seguro suas senhas e outros meios de acesso aos sistemas, e não os divulgar a terceiros em qualquer hipótese.

A Hectare se reserva o direito de proibir o uso de telefones celulares na área de gestão e de rastrear, monitorar, gravar e inspecionar todo e qualquer tráfego de voz realizado através de contato telefônico e internet, bem como troca de informações escritas transmitidas via internet, ou mesmo intranet, sistema de mensagem instantânea, fax, correio físico e eletrônico (e-mail), e ainda, arquivos armazenados ou criados pelos recursos da informática pertencentes à Gestora ou utilizados em nome dela, a fim de assegurar o fiel cumprimento deste documento, bem como das demais políticas internas e da legislação em vigor.

(iv) Procedimentos Internos para Tratar Eventual Vazamento de Informações Confidenciais, Reservadas ou Privilegiadas

Não obstante todos os procedimentos e aparato tecnológico robustos adotados pela Gestora para preservar o sigilo das informações confidenciais, reservadas ou privilegiadas, conforme definições trazidas pelas políticas internas da Gestora, na eventualidade de ocorrer o vazamento de quaisquer Informações, ainda que de forma involuntária, o fato deverá ser comunicado diretamente à Diretoria de Compliance, ou através do [canal de ética](#), tão logo seja possível.

Na ocorrência do Incidente, a Diretoria de Compliance, primeiramente, identificará se a Informação vazada se refere ao fundo de investimento gerido ou aos dados pessoais de Terceiros relacionados à Gestora. Realizada a identificação, o Diretor de Compliance procederá da seguinte forma:

1. No caso de vazamento de Informações relativas aos fundos de investimento geridos

Imediatamente, seguirá com o rito para publicação de fato relevante, nos termos da regulamentação vigente, a fim de garantir a ampla disseminação e tratamento equânime da Informação. Esse procedimento visa assegurar que nenhuma pessoa seja beneficiada pela detenção ou uso da informação confidencial, reservada ou privilegiada atinente ao fundo de investimento.

2. No caso de vazamento de Dados Pessoais de Terceiros relacionados à Gestora

Neste caso, procederá o mais breve possível para cessar a disseminação da Informação ou

atenuar os seus impactos, conforme o caso. Para tanto, poderá, dentre outras medidas: (i) autorizar a contratação de empresa especializada em consultoria para proteção de dados; (ii) autorizar a contratação de advogados especializados no assunto; (iii) entrar em contato com os responsáveis pelo(s) veículo(s) disseminador(es) da Informação. Sem prejuízo, a Diretoria de Compliance ficará à inteira disposição para auxiliar na solução da questão.

(v) Segregação das Atividades

A Gestora mantém segregação física, lógica, funcional e de processos entre suas diversas áreas, das demais empresas pertencentes ao mesmo grupo econômico (controladas pela “RTSC Administração e Participações Ltda.”), de forma a garantir o maior nível de confidencialidade das informações e manter o sigilo devido das operações realizadas pela Gestora, respeitando, assim, as regras do “chinese wall” quanto à total segregação de estrutura de sistema e de pessoal, conforme exigido pelas normas da Comissão de Valores Mobiliários (CVM) e pelos códigos da ANBIMA.

(a) Segregação de Atividades e Funções

O primeiro nível de segregação se refere às diferenças de atuação e autoridade definidas para as posições de Gestão, Compliance/Risco e Administrativo. Serão mantidos diferentes perfis de acesso físico e eletrônico, sendo certo que o controle será realizado com base nesta divisão.

Ademais, conforme disposto na seção sobre segurança da informação, o acesso aos sistemas de informação da Gestora é feito através de “usuário/senha”, o que permite que seja acompanhado, de forma precisa, as atividades desenvolvidas por cada um dos Colaboradores.

Sem prejuízo dessa segregação, para permitir que as atividades internas ocorram de modo eficaz, algumas informações poderão ser compartilhadas em caso de necessidade (*as needed basis*), nas reuniões dos comitês de cada área da Gestora, sendo certo que os participantes serão responsáveis pela manutenção do sigilo das informações. Não haverá, por outro lado, a qualquer momento, o compartilhamento de informações técnicas e confidenciais das operações da Gestora com outra empresa de seu grupo econômico (conforme detalhado no Formulário de Referência da Gestora).

(b) Segregação das Áreas Comuns

O acesso do público externo será restrito à recepção e às salas de reuniões ou atendimento, exceto mediante prévio conhecimento e autorização da administração, e desde que acompanhadas de Colaboradores. Para antigos Colaboradores, será permitida a sua permanência nas dependências da Gestora, no caso de ter sido chamado pela área de recursos humanos para conclusão do processo de desligamento, de aposentadoria ou outros. O atendimento a Terceiros (parceiros, fornecedores, ex-funcionários etc.) nas dependências da Gestora deve ocorrer, obrigatoriamente, nas salas destinadas para reuniões e visitas.

(c) *Segregação Eletrônica*

Todos os Colaboradores têm acesso à rede e aos sistemas internos da Gestora, mas há restrição de acesso aos computadores pessoais, pastas, e-mails e áreas na rede dedicadas a arquivos pessoais.

A área de *Compliance* da Gestora deverá se certificar, através do monitoramento e testes periódicos, da manutenção da segregação do acesso a pastas, sistemas e arquivos da Gestora conforme o perfil de cada Colaborador e sua respectiva área.

(vi) *Rotinas de segurança*

Periodicamente, a Gestora realiza rotinas de segurança em todo o seu sistema de informação. Dentre as medidas, incluem-se, mas não se limitam:

- i. Verificação do Login dos Colaboradores;
- ii. Periodicamente, exige-se a alteração da senha de acesso dos Colaboradores;
- iii. Testes no firewall;
- iv. Testes nas restrições impostas aos diretórios;
- v. Manutenção periódica de todo o “hardware” por empresa especializada em consultoria de tecnologia de informação;
- vi. Testes no “back-up” (salvamento de informações) periódico, realizado em nossa nuvem.

POLÍTICA DE CIBERSEGURANÇA

(i) Objetivo

Essa Política objetiva estabelecer as diretrizes de Cibersegurança, que visa proteger os ativos de tecnologia e os dados da Gestora, bem como assegurar a confidencialidade, integridade, disponibilidade, legalidade e auditabilidade dos mesmos.

(ii) Diretrizes

A Hectare conta com prestador de serviço especializado para gerenciar sua área de Tecnologia da Informação, cuja supervisão está sob responsabilidade da Diretoria de Compliance da Gestora.

Não obstante, a preocupação com os riscos cibernéticos acomete todos os níveis da Gestora e sua mitigação é um compromisso individual de todos. Para isso, a Hectare:

- Desenvolve e efetua campanhas de conscientização e treinamentos sobre cibersegurança;
- Possui controles de acesso em suas dependências físicas e virtuais, sendo a sua concessão dada a apenas recursos relevantes para o desempenho das atividades e com a possibilidade de rápida revogação, quando necessário;
- Requer definições de senhas de alta complexidade de seus colaboradores e com atualizações contínuas;
- Requer autenticação de múltiplos fatores para o acesso do banco de dados;
- Dispõe do registro de acessos (logs) a sistemas e banco de dados para possibilitar sua auditoria e rastreamento, quando necessário;
- Na contratação de novos sistemas, efetua-se a devida diligência do prestador de serviços e requer-se ambiente de teste, antes do envio à produção;
- Tem implementado recursos anti-malware (antivírus e firewalls) em estações e servidores de rede;
- Impede a instalação e execução de software e aplicações não autorizadas por meio de controles de execução de processos, além parametrizar sites, aplicativos e sistemas em *blocklists* (lista de bloqueios);
- Realiza testes de vulnerabilidades; e
- Revisa os processos e procedimentos de identificação, ações de prevenção, monitoramento, plano de resposta e governança de cibersegurança.

Além disso, na ocorrência de incidentes ou tentativas, é efetuado o respectivo registro, analisado a causa, o impacto e possíveis planos de ações e controles, conforme regulamentações vigentes e o Guia de Cibersegurança da ANBIMA.

Dessa maneira, é dever de todos os colaboradores reportar incidentes, tentativas de incidentes e/ou vulnerabilidades identificadas para a Diretoria de Compliance, assim que tomado o conhecimento.

(iii) *Responsabilidades de Terceiros*

De modo complementar ao item anterior, os parceiros, fornecedores e demais terceiros que se relacionarem com a Gestora também possuem responsabilidades (asseguradas em contratos ou NDAs) de:

- Salvar as informações da Gestora que tiver acesso;
- Conhecer as melhores práticas de Cibersegurança, na utilização dos recursos e dados, primando pela preservação da integridade, confidencialidade e disponibilidade das informações;
- Reportar à Diretoria de compliance, através do e-mail compliance@hectarecapital.com.br, qualquer situação que represente desvio ou violação desta Política, bem como das normas vigentes.

(iv) *Medidas Disciplinares*

As violações a esta Política estão sujeitas às ações disciplinares previstas no Código de Ética e Conduta da Gestora e regulamentações externas vigentes.

POLÍTICA DE CONTRATAÇÃO DE TERCEIROS, RECRUTAMENTO E SELEÇÃO

(i) Aspectos Gerais

Esta Política de Contratação de Terceiros, Recrutamento e Seleção (“Política”) tem por finalidade estabelecer os critérios a serem observados pela Gestora quando da contratação de terceiros para a prestação de determinados serviços, bem como quando da contratação de Colaborador para seu próprio quadro.

A Hectare, no limite da sua responsabilidade enquanto empregadora ou tomadora de serviços, a depender da situação fática, implementará todos os procedimentos necessários ao monitoramento das atividades prestadas por seus Colaboradores e prestadores de serviço contratados, sempre balizada nos princípios da eficiência, boa-fé e transparência, nos termos da legislação e regulamentação vigentes.

(ii) Contratação de Terceiros

Quando da eventual contratação de prestadores de serviço para a Hectare, nas hipóteses em que a legislação e/ou a regulamentação permitir, o terceiro deverá observar os critérios de qualificação técnica, capacidade operacional, licenças, preço e idoneidade. A aferição destas condições será realizada através da análise de documentação e eventual realização de visitas (*Due Diligence*), bem como quaisquer outros procedimentos que sejam julgados necessários para comprovar as qualificações do prestador de serviços contratado.

(iii) Recrutamento e Seleção

A Hectare observará a qualificação adequada para cada posição a ser ocupada, e avaliará não somente a comprovada formação técnica dos candidatos, mas também sua integridade e suas experiências em trabalhos anteriores.

Adicionalmente, especificamente para cargos relacionados à gestão de recursos, no qual o Colaborador exerça o poder final de decisão nos investimentos e desinvestimentos a serem feitos pela Hectare, a contratação do futuro colaborador estará condicionada à devida certificação, nos termos determinados pela Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais – ANBIMA.

TREINAMENTO

(i) Disposições Gerais

Os Colaboradores recebem o devido treinamento sobre todas as políticas e procedimentos internos da Gestora, no ingresso à Hectare, com reciclagem anual.

Além disso, a Gestora, eventualmente, realiza campanhas internas de conscientização de Compliance e Segurança da Informação, bem como financia, total ou parcialmente, cursos de aprimoramento profissional aos Colaboradores, principalmente aos membros da equipe técnica, quando julga viável e importante o seu conteúdo a ser lecionado.

Poderão, ademais, ser ministradas palestras internas destinadas a todos ou parte dos Colaboradores da Gestora, a fim de dar-lhes ciência sobre: (i) as políticas e manuais internos adotados; (ii) novas regulamentações aplicáveis às atividades desenvolvidas pela Gestora; (iii) eventuais problemas ocorridos, sobretudo com a finalidade de alertar e evitar práticas que possam ferir a regulamentação vigente.

As presenças nas referidas palestras e treinamentos são comprovadas mediante assinaturas dos Colaboradores em lista de presença e a assimilação dos respectivos conteúdos são verificados, dependendo da relevância do tema, para assim, avaliar a necessidade de refazer o treinamento ou a palestra pelo colaborador que não obtiver a nota mínima esperada.

Os treinamentos relacionados ao conteúdo das políticas internas são realizados com periodicidade mínima anual, pela Diretoria de *Compliance*, sendo obrigatório a todos os Colaboradores. Quando do ingresso de um novo Colaborador, a Diretoria de *Compliance* aplica o devido treinamento de forma individual, ou em pequeno grupo, para os novos Colaboradores. A Diretoria de *Compliance* poderá, ainda, conforme entender necessário, promover treinamentos esporádicos visando manter os Colaboradores constantemente atualizados em relação às políticas.

(ii) Treinamento PLD-FT

A Diretoria de *Compliance* promove, a cada 12 (doze) meses, juntamente com o treinamento geral aqui previsto, treinamentos específicos e adequados para capacitação de todos os Colaboradores com relação às regras de prevenção à lavagem de dinheiro previstas na Política de Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo (“PLD-FT”) da Hectare e na legislação e regulamentação vigentes aplicáveis, sendo tal treinamento obrigatório a todos os Colaboradores, na forma definida e detalhada na Política de PLD-FT.

HISTÓRICO DE ALTERAÇÕES

| Versão | Data | Aprovação | Alteração realizada |
|---------------|-------------|-----------------------|----------------------------|
| V.1 | 07/2018 | Diretor de Compliance | Criação do documento |
| V.1.1 | 11/2020 | Diretor de Compliance | Atualização do documento |
| V.1.2 | 01/2023 | Diretor de Compliance | Atualização do documento |

Documentos de Apoio

Código de Ética e Conduta

Política de PLD-FT

Política de Negociação de Valores Mobiliários

Classificação do documento:

Confidencial Interno Público