Política de Regras, Procedimentos e Controles Internos

Altre Gestão de Investimentos Imobiliários Ltda.

Julho 2022

1 INTRODUÇÃO

Esta Política de Regras, Procedimentos e Controles Internos ("**Política**") visa definir os princípios, conceitos, valores e procedimentos para coordenar os padrões éticos, profissionais e legais de práticas, bem como assegurar, por meio de um controle interno adequado, o cumprimento permanente das regras, políticas e regulamentos atuais relacionados aos diferentes tipos de investimentos e à atividade de gestão de carteiras de valores mobiliários da Altre Gestão de Investimentos Imobiliários Ltda. ("**Gestora**" ou "**Altre**") para o exercício da atividade de administração de carteiras de valores mobiliários, na categoria "gestor de recursos", nos termos da Resolução da Comissão de Valores Mobiliários ("**CVM**") nº 21, de 25 de fevereiro de 2021, conforme alterada ("**Resolução CVM 21**").

Esta Política deve ser lida em conjunto com o Código de Ética e as demais políticas da Gestora, observado que todos os termos iniciados em letra maiúscula que não forem aqui definidos têm seu significado atribuído no Código de Ética da Gestora.

A Altre tem como principal objetivo a prestação de serviços de gestão de carteiras de valores mobiliários para atuar na gestão de Fundos de Investimentos Imobiliários ("**FII**"), a serem constituídos de acordo com a Instrução da CVM n.º 472, de 31 de outubro de 2008, conforme alterada ("**Instrução CVM 472**"), podendo atuar também na gestão de Fundos de Investimentos em Participação ("**FIP**"), constituídos de acordo com a Instrução CVM nº 578, de 30 de agosto de 2016, conforme alterada, ou outros veículos de investimento e/ou sociedades de propósito específico com foco na gestão de ativos imobiliários ("**Veículos**").

A Altre pretende de realizar a gestão de recursos de terceiros com foco em investimentos em dois principais grupos de ativos imobiliários, quais sejam, (i) Imóveis *Value Add*: imóveis destinados a desenvolvimento, investimentos para reforma, ampliação, recuperação e/ou modernização, voltados para venda ou locação; e (ii) Imóveis com Renda Contratada: imóveis para obtenção de renda por meio de locação, observado que, em ambos os casos, sua estratégia poderá envolver a participação em empreendimentos imobiliários, inclusive em *Green Field*, no Brasil ou no exterior, por meio de quaisquer dos ativos permitidos pela regulamentação para FII, nos termos do artigo 45 da Instrução CVM 472 ("**Ativos Imobiliários**").

Como a Altre é sociedade indiretamente controlada pela Votorantim S.A. ("**VSA**"), as Pessoas sob Supervisão estão sujeitas, de forma supletiva ao Código de Ética, a esta Política e aos demais manuais e políticas da Gestora, ao Programa de Compliance da VSA, incluindo ao Manual do Programa de Compliance e ao Código de Conduta, disponíveis na seguinte página da internet: https://www.votorantim.com.br/governanca/ ("**Programa de Compliance da VSA**").

Além dos procedimentos e ações definidos nesta Política, o cumprimento expresso e integral das leis, regras, regulamentos e políticas globais do Grupo Altre, aplicáveis no Brasil e em outros países onde o Grupo Altre possa estar presente, é responsabilidade de todas as Pessoas sob Supervisão.

2 PROTEÇÃO DAS INFORMAÇÕES DE PROPRIEDADE EXCLUSIVA DA EMPRESA E DO INVESTIDOR

2.1 Procedimentos para a Divulgação Adequada de Informações

À luz das disposições de sigilo estabelecidas no Código de Ética, salvo se adequado no contexto de suas responsabilidades profissionais, uma Pessoa sob Supervisão não poderá revelar a qualquer pessoa não associada à Gestora qualquer informação relativa aos investidores dos Veículos geridos pela Altre ("**Investidores**" ou "**Investidor**", conforme o contexto), incluindo dados pessoais fornecidos à Gestora por qualquer Investidor, agente ou contratado; listas e arquivos de Investidores ou outras informações do Investidor. Não se enquadram nessa vedação as comunicações (i) com pessoas envolvidas em uma operação ou aqueles que sejam mandatários em nome de um Investidor; (ii) com pessoas que prestem serviços jurídicos, contábeis, administrativos ou outros serviços ao respectivo Veículo ou Investidor; (iii) conforme exigido por lei; ou se (iv) especificamente solicitado por um Investidor.

Os registros comerciais da Gestora, informações dos profissionais, informações financeiras, software, licenças, contratos, arquivos de computador e planos de negócios; modelos, pesquisa de propriedade exclusiva, direitos autorais ou outros materiais pagos por um Veículo ou pela Gestora; e as análises e outros dados ou informações são de propriedade exclusiva da Gestora, indisponíveis perante terceiros. Todas essas informações, sejam ou não materiais, são estritamente confidenciais e não podem ser divulgadas.

As Pessoas sob Supervisão tomarão precauções especiais para não divulgar informações relativas a recomendações ou possíveis operações que ainda não estejam fechadas ou que estejam sob negociação, exceto quando (i) seja necessário ou apropriado no contexto das atribuições do seu trabalho; (ii) no contexto da elaboração de relatórios a serem prestado aos Investidores; (iii) no contexto da elaboração de qualquer relatório a que pessoas tenham direito a acesso devido a disposições de um acordo de gestão de investimentos ou outro documento similar que governe o funcionamento da Gestora; (iv) conforme exigido por lei (nesse caso, mediante autorização do Diretor de Compliance); e (v) após a informação estar de outra forma disponível ao público.

A Gestora tem para com todo e qualquer Investidor um dever primordial de lealdade. Esse dever inclui não se apropriar indevidamente de informações e/ou estratégias desenvolvidas com o objetivo de utilizá-las em negociações pessoais (ou negociações para outras contas) por Pessoas sob Supervisão e para uso na administração do capital Gestora. De maneira geral, as políticas de negociações pessoais da Gestora encontradas no Código de Ética devem evitar o uso e a apropriação indevida de informações, mas é dever de cada Pessoa sob Supervisão de maneira individual não realizar operações em que acredite estar sob posição privilegiada pelo acesso a informações específicas que recebeu ou geradas por conta da gestão dos investimentos mantidos pela Gestora.

3 CLASSIFICAÇÃO DE DADOS

3.1 Categorias de Classificação de Dados

A Gestora acredita que as proteções de segurança da informação devem ser proporcionais à classificação dos dados a serem protegidos (*i.e.,* quanto mais sensíveis ou cruciais forem os dados forem para o negócio, maiores devem ser as proteções). A Gestora adotará uma política de classificação de dados que, em regra, enquadra seus dados em uma das seguintes categorias:

(i) Dados Públicos (Dados de Alerta Verde): Dados públicos são dados que a Gestora classificará como aqueles que serão passíveis de disponibilização ao público em geral. Isso inclui, por exemplo, informações disponíveis no website da Gestora acessíveis ao público, conteúdo acessível ao público em páginas de mídias sociais ou perfis gerenciados pela Gestora e informações acessíveis pelo público em geral sobre a Gestora através de seus arquivamentos regulamentares.

(ii) Dados Internos da Gestora (Dados da Alerta Amarelo): Os dados internos da empresa sobre os negócios ou operações da Gestora e que, embora não necessariamente confidenciais, garantirão certo grau de privacidade. Exemplos incluem, mas não se limitam, determinadas informações sobre os controles internos ou procedimentos operacionais da Gestora, e informações sobre vendedores, fornecedores, contratados e investimentos ou qualquer informação cuja divulgação possa ser exigida por lei ou por autoridade competente.

(iii) Dados Confidenciais (Dados de Alerta Vermelho): Os dados confidenciais compreenderão os dados do mais alto grau de sensibilidade e criticidade de ação para a Gestora e seus negócios. Exemplos incluem, mas não estão limitados a, quaisquer Dados Pessoais (conforme definido adiante) sobre os Investidores (antigos, atuais e potenciais) e Pessoas sob Supervisão; informações de recursos humanos detidos pela Gestora (tais como nomes, datas de nascimento, números de previdência social, informações de conta pessoal de corretagem, informações sobre folha de pagamento e informações médicas); informações ou pesquisas relativas aos valores mobiliários, empresas ou investimentos feitos ou sob consideração pela Gestora; dados utilizados em controles de acesso; e informações que devam ser mantidas em sigilo por força de obrigações contratuais ou de leis ou regulamentos federais, estaduais ou locais ("**Dados Confidenciais**").

(iv) Dados Pessoais (Dados de Alerta Vermelho): qualquer informação relativa a uma pessoa identificada ou identificável, exceto aquelas enquadradas nos itens "i" e "ii" acima ("**Dados Pessoais**").

O acesso da Pessoa sob Supervisão será segmentado de acordo com a classificação dos dados bem como em sua necessidade de conhecê-los dada suas atribuições profissionais. O Diretor de Compliance deverá trabalhar em conjunto com os colaboradores da área de TI da Gestora para analisar o acesso da Pessoa sob Supervisão a essas categorias de classificação de dados com base na necessidade do acesso e, dará especial atenção àquelas que terão acesso a Dados Confidenciais e aos Dados Pessoais.

Os dados da área de gestão de recursos de terceiros da Altre somente serão acessíveis ao Diretor de Gestão e aos colaboradores de sua equipe e ao Diretor de Compliance, para o desempenho de suas funções.

3.2 Titularidade de Dados

Com exceção do material claramente de propriedade de terceiros, tais como seus dados pessoais confidenciais, a Gestora é a legítima titular de todas as informações comerciais armazenadas ou transmitidas através de seus sistemas. A menos que a Gestora tenha celebrado um acordo específico por escrito, todas as informações comerciais desenvolvidas enquanto uma Pessoa sob Supervisão estiver empregada pela Gestora são de propriedade da Gestora.

Pessoas sob Supervisão, fornecedores e quaisquer outros terceiros não poderão copiar o software fornecido pela Gestora para qualquer meio de armazenamento, transferir tal software para outro computador ou divulgar tal software a terceiros externos sem permissão prévia do Diretor de Compliance.

3.3 Classificação e Manuseio da Informação

As informações da Gestora, e as informações que tenham sido confiadas à Gestora, devem ser protegidas de forma compatível com o seu grau de sensibilidade. Medidas de segurança devem ser empregadas independentemente do meio no qual a informação está armazenada, dos sistemas que a processam ou dos métodos através nos quais ela circula. A informação deve ser protegida de forma compatível com sua classificação, não importando o estágio ou o ciclo de criação da informação, devendo ser considerando até o estágio de sua destruição. Por exemplo, documentos impressos que sejam considerados sensíveis devem ser picotados, os registros eletrônicos que sejam considerados sensíveis devem ser protegidos por senha conforme aplicável. Observadas as regras previstas nesta Política, especialmente, aquelas dispostas no item 10 adiante, as Pessoas sob Supervisão não devem compartilhar documentos com qualquer pessoa fora da Gestora ou conceder a terceiro acesso à rede Gestora sem o consentimento do Diretor de Compliance.

4 CONTROLE DE ACESSO À INFORMAÇÃO E PROTEÇÃO DE DADOS

4.1 IDs de usuário e Senhas

Para garantir que o acesso às informações e à rede da Gestora seja limitado às Pessoas sob Supervisão e afiliados externos com necessidade de acesso, a Gestora exigirá que cada indivíduo que acesse os sistemas de informação da Gestora tenha um ID de usuário único e uma senha exclusiva ("**Usuário**"). Esses IDs de Usuário serão utilizados para restringir os privilégios do sistema com base em atribuições de trabalho, responsabilidades de projeto e outras atividades comerciais. Cada usuário será pessoalmente responsável por seu ID de Usuário e senha. Todos os computadores e dispositivos que acessem o e-mail e/ou dados da Gestora devem ter uma senha definida para todas as contas de Usuário e devem ser configurados para bloquear automaticamente a tela quando deixados sem supervisão após um determinado período. Além disso, após 10 (dez) tentativas de *login*, as contas de Usuário serão temporariamente bloqueadas por 10 (dez) minutos.

A Gestora poderá, a seu critério, limitar a capacidade de uma Pessoa sob Supervisão de imprimir, encaminhar ou salvar um documento. Quando necessário, a Gestora criptografará dados, documentos, e-mails ou anexos sensíveis, conforme o item 5.2 abaixo.

Os computadores da Gestora serão preparados com uma configuração básica padrão de hardware e software. Os empregados da Gestora deverão solicitar permissão ao Diretor de Compliance para alterar essa base padrão. A Gestora reconhece que os direitos de acesso podem ser atualizados ou encerrados com base em várias mudanças de profissionais ou de sistemas.

4.2 Criptografia

Criptografia significa o processo de transformação de informações, utilizando um algoritmo, para tornar tais informações ilegíveis para qualquer outra pessoa que não aqueles que tenham a necessidade específica de conhecê-las.

A Gestora poderá utilizar *software* de criptografia que permita às Pessoas sob Supervisão garantir a segurança dos dados da Gestora por meio de proteção de arquivos sensíveis com senha e criptografia e do uso de e-mail e outros métodos de transmissão, como por exemplo, por meio de um portal on-line. Além disso, todos os computadores, *laptops*, *tablets* e telefones celulares dos profissionais da Gestora poderão ser criptografados, tornando os dados ilegíveis em caso de perda ou roubo. Nenhum software de criptografia instalado em equipamentos fornecidos pela Gestora poderá ser adulterado, desabilitado ou alterado de qualquer forma.

4.3 Acesso Remoto

Todas as Pessoas sob Supervisão terão a capacidade de acessar a rede da Gestora ao trabalhar remotamente, por meio do portal Gestora. A Gestora emprega um duplo fator de autenticação para a realização do *login* remoto na rede Gestora. Além disso, os Usuários e suas credenciais serão mantidos e monitorados pela área de TI da Gestora, sob supervisão do Diretor de Compliance, para garantir que todos os Usuários estejam atualizados e que nenhum Usuário apresente risco para o sistema da Gestora. As Pessoas sob Supervisão que acessem a rede da Gestora remotamente estarão obrigadas a instalar um *software* de proteção contra vírus em seus computadores pessoais ou dispositivos de acesso remoto. Conforme aplicável e mediante solicitação, algumas Pessoas sob Supervisão poderão precisar apresentar seus dispositivos à área de TI da Gestora para prévia inspeção como condição de acesso remoto.

Todos os *smartphones*/ *tablets* que se conectarem aos serviços de comunicações da Gestora exigirão senha de no mínimo de 4 (quatro) dígitos ou reconhecimento de impressão digital ou reconhecimento facial para destravar o dispositivo para utilização de tais serviços. Enquanto o e-mail da Gestora estiver instalado em um dispositivo de uma Pessoa sob Supervisão, esta não poderá desativar a função de senha. As Pessoas sob Supervisão serão avisadas de que quando utilizarem um dispositivo pessoal para se conectar ao sistema de e-mail, a Gestora terá controle total sobre a capacidade de limpar os dados de tal dispositivo a qualquer momento para fins de segurança.

A Gestora se reserva o direito de conduzir inspeções surpresa dos Usuários que possuam acesso remoto. Tais inspeções surpresa poderão incluir visitas a sites remotos e inspeção do conteúdo de um computador utilizado para acessar os sistemas Gestora.

4.4 Detecção de Atividade Não Autorizada

Além de sólidas políticas para evitar uma ameaça à segurança cibernética de sua rede, a Gestora também adotará políticas e procedimentos destinados a detectar atividades não autorizadas. A Gestora buscará regularmente a presença de usuários, dispositivos, conexões e softwares não autorizados em sua rede e nos dispositivos móveis de seus profissionais. No âmbito desta política, a Gestora atualizará os sistemas operacionais e softwares em sua rede quando necessário; tais atualizações ajudarão a reduzir as vulnerabilidades da rede, uma vez que as atualizações frequentemente abordam ameaças conhecidas ou antecipadas.

A Gestora usará programas para auxiliar na prevenção e detecção de software não previamente aprovados, impedindo-os de rodar na rede Gestora e nos dispositivos dos empregados. A Gestora monitorará regularmente eventos e conexões através do *firewall* da Gestora para detectar quaisquer violações, ataques ou acesso a informações sensíveis. A Gestora garantirá que softwares antivírus e/ou anti-*malware* sejam instalados em todos os computadores e que o acesso ao servidor seja definido e periodicamente auditado.

A Gestora monitorará sistemas de fiscalização de perímetro para detectar tentativas de *login* falhadas, tentativas de *login* não autorizadas, desativação de acesso e contas de usuários inativas.

Como parte de seus esforços para manter esta Política, Gestora realizará anualmente uma avaliação por terceiro independente em que testará a vulnerabilidade dos sistemas que manterá. Tal avaliação verificará a autenticidade da configuração do firewall e da fragmentação antivírus, analisará a segurança do dispositivo de rede e procurará evidências de atividades de *malware*.

4.5 Uso Aceitável de Dispositivos Pessoais

Empregados que utilizem computadores pessoais enquanto trabalham em casa deverão manter as mesmas proteções que os computadores da Gestora possuem nesses tipos de dispositivos, incluindo proteção antivírus e senhas fortes. Embora seja permitido o uso da maioria dos dispositivos dentro do ambiente do escritório, o Diretor de Compliance se reservará o direito de que alguns aplicativos em específico sejam implementados na rede e no sistema da Gestora.

4.6 Plano de Destruição de Dados e Equipamentos

A área de TI da Gestora, sob supervisão do Diretor de Compliance, será responsável por, periodicamente, realizar o inventário dos dispositivos e sistemas físicos da Gestora; inventário dos dispositivos e sistemas de software da Gestora; criará mapas de recursos de rede, conexões e fluxos de dados (incluindo locais onde os dados dos Investidor estarão armazenados); e catalogará as conexões à rede da Gestora a partir de fontes externas.

A Gestora manterá os livros e registros por um período de no mínimo 5 (cinco) anos, conforme o item 11.7 abaixo. Os e-mails trocados entre prestadores de serviços e Investidores e e-mails internos também são arquivados segundo a política da Gestora e serão mantidos por um período mínimo de 5 (cinco) anos. Profissionais da Gestora não devem destruir documentos que ainda não estejam arquivados na rede de armazenamento. Documentos impressos ou duplicados em papel contendo informações sensíveis dos Investidores e que estão disponíveis na rede Gestora poderão ser destruídos, após a análise da área de TI da Gestora, sob supervisão do Diretor de Compliance. Os equipamentos da Gestora não poderão ser doados, dados de presente ou destruídos, mas sim entregues à área de TI da Gestora para descarte. Qualquer dúvida sobre destruição de dados, documentos ou equipamentos deve ser encaminhada ao Diretor de Compliance.

4.7 Equipamentos Extraviados

A Gestora instalará um programa de limpeza remota em todos os computadores portáteis e dispositivos móveis de seus profissionais. Caso o computador e/ou dispositivo móvel seja extraviado ou roubado, ou esteja fora do controle de um empregado por mais de 24 (vinte e quatro) horas, o profissional deverá notificar a área de TI da Gestora, que tomará as devidas precauções para desativar as informações consonantes no referido *laptop* ou dispositivo móvel. Além disso, todos os computadores, *laptops*, *tablets* e telefones celulares dos profissionais da Gestora poderão ser criptografados, tornando os dados ilegíveis em caso de perda ou roubo.

5 ACESSO À INTERNET

O acesso à internet é fornecido pela Gestora e é considerado um recurso imprescindível para que os profissionais da Gestora possam exercer suas atividades da melhor maneira possível. O acesso à internet fornecido pela Gestora não deve ser usado para entretenimento, filmes de *streaming*/programas de TV, videogames, entre outros. Pessoas sob Supervisão devem ter ciência que a Gestora se reserva o direito de monitorar o uso da internet pelas Pessoas sob Supervisão em seus dispositivos profissionais e, se for constatado que uma Pessoa sob Supervisão está utilizando esses recursos de maneira inadequada com suas atividades profissionais ou que exponha a Gestora a riscos cibernéticos, poderão ser tomadas medidas disciplinares.

Os nomes e senhas das redes sem fio estão sujeitos a alterações por razões de segurança a qualquer momento, com pouca ou nenhuma notificação. Além disso, a rede interna sem fio da Gestora ser incluirá 2 (duas) formas de identificação: (1) conhecendo a senha; e (2) filtrada por endereço *mac*. A Gestora poderá utilizar a rede sem fio do Grupo Altre ou contar com rede sem fio autônoma, sendo que, em ambos os casos, será operada pelo time de TI da Gestora, que será compartilhado com o Grupo Altre.

Alguns sites de internet serão bloqueados por roteadores e firewalls da Gestora. Essa lista será constantemente monitorada e atualizada conforme necessário. Qualquer Pessoa sob Supervisão que visite sites pornográficos ou outros sites imorais, antiéticos ou relacionados a jogos (isto é, jogos de azar) sofrerá medidas disciplinares e poderá ser desligada. A Gestora não será responsável pelas ações de suas Pessoas sob Supervisão quando se trata de downloads e software ilegais de qualquer tipo e somente fornecerá softwares legítimos e totalmente licenciados. As Pessoas sob Supervisão serão advertidas a não clicar em links que não reconheçam e não deverão baixar ou instalar softwares que sejam provenientes da internet sem autorização prévia. Qualquer dúvida quanto ao uso adequado da internet deve ser encaminhada diretamente ao Diretor de Compliance.

6 SEGURANÇA CIBERNÉTICA (*CIBERSEGURANÇA*)

As iniciativas de segurança cibernética da Gestora ("**Iniciativas de Cibersegurança**") terão como objetivo a (i) criação de um ambiente seguro onde as informações são armazenadas; (ii) proteção dos Dados Confidenciais e dos Dados Pessoais tratados pela Gestora, incluindo, mas não se limitando, aos Dados Pessoais de Investidores e das Pessoas sob Supervisão, e (iii) criação de um mecanismo para avaliar a conformidade das medidas de cibersegurança e a prontidão no controle e mitigação de riscos na indústria de valores mobiliários.

6.1 Requisitos de Cibersegurança

As Iniciativas de Cibersegurança visarão tratar dos tópicos a seguir:

(i) Governança e Avaliação do Risco;

(ii) Direitos e Controles de Acesso;

(iii) Prevenção de Perda de Dados;

(iv) Gestão de Fornecedores;

(v) Resposta a Incidentes; e

(vi) Treinamento.

7.1.1. Governança e Avaliação do Risco

(A) Governança

Como parte de seu programa de cibersegurança, a Gestora deverá criar uma equipe de resposta a incidentes ("**IRT**"), que incluirá empregados da Gestora e da VSA, para adequadamente monitorar e avaliar periodicamente a rede de computadores da Gestora e os riscos que esta enfrenta com relação à cibersegurança. Os procedimentos adotados e implementados pela IRT serão detalhados mais adiante na seção "Resposta a Incidentes".

Pelo menos uma vez por ano, a IRT ***(i)*** apresentará à alta administração do Grupo Altre um resumo das conclusões da IRT – se a alta administração julgar necessário, a IRT apresentará quaisquer descobertas ao Diretor de Compliance ou, caso entendam necessário, a todos os Investidores caso um incidente atinja um alto nível de preocupação; e ***(ii)*** analisará os processos de avaliação de risco da Gestora para identificar potenciais ameaças à segurança cibernética e quaisquer esforços responsivos de reparação empreendidos pelo ou em nome da Gestora.

(B) Avaliação do Risco

Os avanços tecnológicos proporcionam facilidades e permitem o uso de novas ferramentas pelas instituições, permitindo agilidade na criação e disponibilidade dos serviços, aplicação no meio, entre outros avanços. Por outro lado, o uso crescente de tais ferramentas aumenta o vazamento de informações e os riscos de ciberataques, ameaçando o sigilo, a integridade e disponibilidade dos dados e/ou sistemas das instituições.

Ameaças cibernéticas podem variar de acordo com a natureza, vulnerabilidade, informação ou ativos de cada organização. As consequências para as instituições podem ser significativas em termos operacionais, risco de imagem, danos financeiros ou perda de vantagem competitiva, podendo tais danos serem irreparáveis.

Dado o cenário mencionado acima, indicamos abaixo os métodos mais comuns de ciberataques:

(i) *Malware* – software projetado para corromper computadores e redes:

(b) Vírus: software que causa danos à máquina, à rede, ao software e ao banco de dados;

(c) Cavalo de Tróia: aparece dentro de outros softwares e cria uma porta para a invasão de computadores;

(d) Espiões: software mal-intencionado que coleta e monitora o uso de informações; e

(e) *Ransomware*: software mal-intencionado que bloqueia o acesso a sistemas e bancos de dados, solicitando um resgate a fim de restabelecer o acesso.

(ii) Engenharia Social – métodos de manipulação para obter informações sensíveis, como senhas, dados pessoais e número de cartão de crédito:

(a) *Pharming*: direciona você para um site fraudulento sem seu conhecimento;

(b) *Phishing*: links de e-mail, fingindo ser uma pessoa ou empresa confiável, enviando e-mails oficiais tentando obter informações confidenciais;

(c) *Vishing*: finge ser uma pessoa ou empresa confiável e, através de ligações telefônicas, tenta obter informações confidenciais;

(d) *Smishing*: finge ser uma pessoa ou empresa confiável e, através de mensagens de texto, tenta obter informações confidenciais;

(e) Acesso pessoal: pessoas localizadas em locais públicos como bares, cafés e restaurantes que recolhem qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

(iii) DDoS (ataque de negação de serviços) e ataques de *botnet* – ataques destinados a negar ou atrasar o acesso aos serviços ou sistemas da instituição. No caso de *botnets*, o ataque vem de grande número de computadores infectados usados para criar e enviar *spam* ou vírus, inundando uma rede com mensagens que resultam em negação de serviço.

(iv) Ameaças persistentes avançadas – ataques de intrusos sofisticados usando conhecimento e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Além dos ciberataques, a Gestora pode estar sujeita a mau funcionamento dos sistemas utilizados e atos/omissões de seus profissionais, o que pode resultar na perda e/ou adulteração de dados e Dados Confidenciais.

7.1.2. Prevenção de Perdas e Dados

A fim de evitar a ocorrência de perdas e dados, a Gestora determinará quais dados garantem a maior proteção para ajudar a evitar que ataques cibernéticos à segurança dos softwares e sistemas da Gestora causem danos significativos. A Gestora estabelecerá procedimentos para monitorar e evitar violações de dados (ver item Segurança da Informação abaixo), exigirá criptografia ou as precauções adequadas em relação à transferência de Dados Confidenciais (conforme descrito nos itens acima) e estabelecerá regras relativas ao gerenciamento de dispositivos móveis. A Gestora adotará as medidas de segurança cibernéticas atualizadas e seguindo as melhores práticas do mercado, observado que poderá implementar, mas sem limitação, as seguintes medidas: (i) regras relativas à *firewall*; (ii) roteadores com capacidade de limitação de uso e lista de controle de acesso à *websites*; (iii) atualização regular de seu *software* antivírus e/ou anti-*malware*; (iv) instalação em todos os computadores da Gestora, de *softwares* de proteção contra vírus ou malwares; e/ou (v) implementação de filtro de *spam* e de lista de controle de acesso ou limpeza de acesso.

O *software* de proteção contra vírus e *malware* poderá ser instalado em todos os computadores de uso doméstico ou dispositivos de acesso remoto, acessados pelos profissionais da Gestora. Além disso, a equipe de compliance ("**Equipe de Compliance**") monitorará os profissionais que trabalharem remotamente para garantir que esses não representarão um risco para a rede Gestora.

A Gestora também monitorará a distribuição não autorizada de informações sensíveis fora da Gestora através de canais de distribuição alternativos como, por exemplo, por *e-mail*.

A Gestora adotará uma política com relação à solicitação de mudanças nas informações bancárias dos Investidores, instruções de pagamento dos fornecedores e instruções de financiamento das negociações. Especificamente, a Gestora exige que qualquer mudança nas informações de transferência via cabo ou informações bancárias que divirjam das informações constantes no contrato de subscrição inicial do Investidor seja acompanhada de uma ligação telefônica confirmando tal mudança junto ao investidor. Da mesma forma, a Gestora exige que qualquer solicitação referente ao pagamento ou outras mudanças suspeitas em relação ao financiamento de investimentos ou informações de fornecedores seja verificada através de uma ligação telefônica para um ponto de contato estabelecido ou verificado.

7.1.3. Gestão de Contratação de Terceiros

A Gestora somente selecionará prestadores de serviços terceirizados após a devida diligência e geralmente escolherá aqueles que são conhecidos e estabelecidos dentro de seus segmentos. Ao contratar um prestador de serviços terceirizado com acesso a Dados Confidenciais, a Gestora garantirá que existam proteções adequadas para a não divulgação e a confidencialidade de tais informações. Caso o prestador de serviço terceirizado necessite ter acesso a Dados Confidenciais, a Gestora garantirá que a companhia contratada mantenha uma política de monitoramento e segurança cibernética a qual a Gestora deverá ter acesso previamente à prestação dos serviços.

Além disso, a Gestora fornecerá uma cópia desta Política aos principais prestadores de serviços terceirizados que tenham acesso a Dados Confidenciais e, monitorará, rotineiramente, suas atividades bem como o seu controle de acesso. A Gestora solicitará que os principais prestadores de serviços terceirizados enviem à Gestora notificação no caso de quaisquer mudanças significativas nos sistemas, componentes ou serviços do fornecedor que possam potencialmente ter impacto de segurança para a Gestora ou seus dados.

7.1.4. Resposta a Incidentes

Conforme acima mencionado, a Gestora criará uma IRT para monitorar adequadamente a sua rede e mitigar os riscos eventualmente enfrentará com relação à cibersegurança. A IRT incluirá o Diretor de Compliance, assim como outros profissionais dos departamentos de tecnologia e Compliance da VSA. Pelo menos uma vez por semestre, e mais frequentemente, se necessário, a IRT se reunirá para identificar os riscos particulares que a Gestora enfrenta do ponto de vista da cibersegurança e analisará quaisquer incidentes ou potenciais incidentes, se houver. A Gestora manterá informações básicas sobre os eventos esperados na rede Gestora e monitorará regularmente essas expectativas.

A IRT conduzirá, ou designará um terceiro para conduzir avaliações periódicas do risco e para identificar ameaças à segurança cibernética, vulnerabilidades e potenciais consequências comerciais, bem como ameaças à segurança física dos sistemas. Continuamente, a IRT testará seus processos de detecção de eventos, bem como suas respostas a incidentes e quaisquer esforços de reparação realizados pela Gestora ou em seu nome. Conforme mencionado acima, a IRT também monitorará os principais prestadores de serviço terceirizados da Gestora com acesso a Dados Confidenciais para garantir que tais prestadores de serviços sejam capazes de cumprir esta Política. Qualquer ameaça, incidente ou violação de segurança cibernética deve ser comunicada imediatamente ao Diretor de Compliance, que informará a IRT.

É responsabilidade de cada Pessoa sob Supervisão, fornecedor ou terceiro afiliado comunicar imediatamente qualquer suspeita de invasão, atividade ou comportamento errático do sistema ao Diretor de Compliance, que informará a IRT. Da mesma forma, uma Pessoa sob Supervisão deverá notificar o Diretor de Compliance caso qualquer informação sensível seja perdida, roubada ou revelada/desviada involuntariamente. Se necessário, no caso de o incidente requerer maior cuidado, a IRT envolverá a alta administração da Gestora e da Altre Properties, advogados externos ou os próprios Investidores.

Ao ocorrer um incidente ou violação da rede Gestora, a IRT poderá entender que o evento exige notificação à alta administração, autoridades reguladoras, agências ou partes afetadas, conforme o caso. A IRT é responsável por determinar quais eventos requerem notificação ou alertas aos seus profissionais, prestadores de serviços terceirizados ou reguladores. No caso de prejuízo real a Veículo sob a gestão da Altre, a IRT documentará os fatos pertinentes que cercam o prejuízo, o montante da perda e o reembolso pela cobertura de seguro de cibersegurança, se houver. A Gestora poderá contratar, ainda, seguro de cibersegurança para cobertura de eventuais ataques cibernéticos.

7 SEGURANÇA DA INFORMAÇÃO

7.1 Privacidade das Pessoas Sob Supervisão

As Pessoas sob Supervisão devem ter ciência e concordam que a Gestora, para gerenciar sistemas e reforçar a segurança, poderá, a seu exclusivo critério, registrar, revisar e utilizar qualquer informação armazenada ou que circule em seus sistemas a seu próprio benefício. A Gestora poderá armazenar as atividades dos usuários como por exemplo, o tráfego de e-mail, números de telefone discados e sites visitados. Além disso, a administração da Gestora reserva-se o direito de monitorar, inspecionar ou remover de seus sistemas de informação qualquer material que considere ofensivo ou potencialmente ilegal. Esse exame pode ocorrer com ou sem o consentimento, presença ou conhecimento das Pessoas sob Supervisão envolvidas. Os sistemas de informação sujeitos a tal exame incluem, mas não estão limitados, a sistemas de correio eletrônico, qualquer dispositivo controlado pela Gestora, arquivos de correio de voz, arquivos de *spool* de impressora, saída de fax, gavetas de mesa e áreas de armazenamento.

7.2 Uso Pessoal de Sistemas e Armazenamento de Dados Pessoais

Os sistemas de uso de informação da Gestora serão destinados à utilização somente para fins profissionais, dessa forma os arquivos pessoais de uma Pessoa Sob Supervisão, tais como documentos, fotos, vídeos ou música, não devem ser armazenados no disco compartilhado da Gestora. O uso pessoal eventual e limitado é permitido se não representar um risco ao sistema da Gestora e não consumir mais do que uma quantidade trivial de recursos que poderiam ser usados para fins profissionais, bem como não impedir qualquer atividade profissional. É proibido o uso dos sistemas de informação da Gestora para uso de correspondência em cadeia, solicitações de caridade, material de campanha política, trabalho religioso, transmissão de material questionável ou qualquer outro uso não profissional.

Nenhum software pessoal deve ser instalado nos sistemas de informação da Gestora sem a aprovação expressa do Diretor de Compliance. A Gestora não é responsável por quaisquer Dados Pessoais armazenados nos computadores ou servidores da empresa e poderá apagar esses dados sem aviso prévio. Além disso, a Gestora não investirá recursos da empresa na recuperação de Dados Pessoais no caso de perda destes.

8 PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS

O objetivo do "**Plano de Contingência e Continuidade de Negócios**" é estabelecer as medidas a serem tomadas para evitar um impacto negativo considerável na condução das atividades da Gestora. Essas contingências incluem, por exemplo, crises econômicas, pandemias, falhas operacionais e/ou desastres naturais.

Todos os profissionais possuem acesso remoto às redes da Gestora como parte dos procedimentos de recuperação de desastres da Gestora. Nos casos de ocorrência de quaisquer eventos ou sinistros que possam tornar impraticável, paralisar ou comprometer temporariamente o exercício de suas atividades, a Gestora deverá seguir os procedimentos aqui definidos e trabalhar em conjunto com um provedor de serviços em nuvem para retomar as atividades o mais brevemente possível.

8.1 Diretrizes de Prevenção e Tratamento de Contingências

Para a implementação efetiva deste Plano de Contingência e Continuidade de Negócios, a Gestora procurará conhecer e reparar os principais pontos de vulnerabilidade de suas instalações e equipamentos. Para este fim, a empresa tomará medidas que lhe permitam:

(i) Conhecer e minimizar os danos no período pós-contingência;

(ii) Minimizar prejuízos para si, seus clientes e profissionais decorrentes da interrupção de suas atividades; e

(iii) Normalizar as atividades de gestão o mais rapidamente possível.

De modo geral, as etapas para a execução deste plano são as seguintes:

(i) A identificação de interdependências entre as instalações, equipamentos e processos comerciais da Gestora com outras empresas e/ou com terceiros contratados;

(ii) Listagem das diferentes atividades da Gestora e identificação daquelas com alta relevância estratégica e/ou aquelas com alto potencial de risco financeiro, físico ou operacional;

(iii) Lista de instalações, equipamentos, terceiros contratados que possam representar dificuldades ou restrições para a aplicação deste plano; e

(iv) Verificação da adequação dos meios de prevenção e proteção às características da operação e do negócio.

8.2 Disseminação do Plano

A fim de reduzir e controlar eventuais prejuízos devido à ocorrência de contingências, todos os empregados da Gestora devem estar cientes dos procedimentos de backup e proteção de informações (confidenciais ou não), planos de evacuação física do local e melhores práticas para a saúde e segurança no local de trabalho.

8.3 Plano de Recuperação de Negócios

A Gestora mantém a identificação atualizada de seus principais procedimentos profissionais de modo que, em caso de contingências, será possível retomar as operações com os menores custos de operação e a menor perda de tempo, de recursos humanos, físicos e materiais possível.

Durante o desenvolvimento do plano de recuperação de negócios, conforme descrito nesta Política, foram levados em conta os backups de servidores, bancos de dados e arquivos, assim como a estruturação da computação em nuvem. Os backups realizados são:

(i) Backup diário do banco de dados e armazenamento das versões anteriores por 30 (trinta) dias com fechamento mensal por 5 (cinco) anos.

(ii) Backup de arquivos em tempo real e armazenamento em nuvem.

Proteger os dados na forma descrita acima constitui o procedimento central da Gestora para a rápida recuperação do estado operacional em caso de falha do disco rígido do equipamento. O acesso aos arquivos de backup armazenados na sede da Gestora ou fora da sede da Gestora seguirá esta Política. A Gestora adotará medidas atualizadas e seguindo as melhores práticas de mercado para proteger e assegurar seus dados, observado que poderá implementar, mas sem limitação, as seguintes medidas: (i) possuir 2 (dois) ambientes de nuvem diferentes para proteger e assegurar seus dados, ambos localizados externamente;(ii) ter 2 (dois) provedores de internet com firewalls duplos configurados para alta disponibilidade de navegação, monitoramento e permissão de conteúdo; e (iii) criptografar todos os dados armazenados em nuvens.

Devido a esses procedimentos, caso as Pessoas sob Supervisão não tenham acesso às instalações físicas da Gestora, elas poderão acessar (após a devida autenticação) aos sistemas da Gestora. O método de replicação virtual utilizado pela Gestora proporcionará a continuidade de negócios (BC) e solução de recuperação de desastres (DR) que permitirá a replicação de servidores e dados de missão crítica entre diferentes plataformas IaaS (*Infrastructure as a Service*) o mais rápido possível com o mínimo de perda de dados.

Além disso, para a rápida e efetiva retomada das operações após a ocorrência de uma contingência, a Gestora manterá procedimentos que lhe permitam:

(i) Manter os procedimentos de gestão de pessoal e operações administrativas mesmo durante os efeitos da contingência;

(ii) Retornar permanentemente ao uso das instalações de sua sede após a ocorrência da contingência; e

(iii) Avaliar os prejuízos ocorridos devido à interrupção dos negócios.

Além disso, como todo o ambiente de dados da Gestora será baseado em nuvem, a empresa entende que, em caso de contingências, as pessoas poderão acessar o ambiente da Gestora a partir de seus computadores pessoais e manter seu trabalho normalmente, não havendo, portanto, necessidade de um escritório alternativo.

8.4 Tratamento de Contingências Operacionais

A fim de lidar com contingências diretamente relacionadas à operação comercial, os procedimentos devem ser mantidos atualizados para permitir que a empresa:

(i) Aumente rapidamente seu contingente de pessoal técnico qualificado e/ou fornecedores se a demanda por serviços aumentar rapidamente sem a consequente redução na qualidade da prestação do serviço;

(ii) Substitua qualquer empregado em caso de saída, no menor tempo possível;

(iii) Identifique novos mercados e/ou produtos potenciais se houver períodos curtos ou longos de recessão na demanda de seus clientes atuais;

(iv) Permaneça sempre competitiva e inovadora a fim de evitar perder sua participação no mercado, explorando seus pontos fortes e diminuindo constantemente suas fragilidades; e

(v) Mantenha um fluxo de caixa que, a critério do Diretor de Compliance, seja capaz de atender a despesas imprevistas.

O Diretor de Compliance será o responsável pela prevenção de prejuízos e implementação do plano de contingência da Gestora.

8.5 Testes de Contingência

O teste de contingência será realizado anualmente a fim de permitir que a Gestora esteja preparada para dar continuidade às suas atividades.

Os testes a serem implementados serão os seguintes:

(i) Acesso remoto aos sistemas e e-mails através de endereço externo;

(ii) Acesso aos dados armazenados externamente;

(iii) Testes de falhas; e

(iv) Outros testes necessários para a continuidade das atividades.

O resultado do teste é registrado no documento de teste de contingência.

8.6 Ativação do Mecanismo de Resposta

Os profissionais da Gestora serão os responsáveis por comunicar ao Diretor de Compliance toda e qualquer situação que possa, ainda que potencialmente, originar uma situação que possa levar à ativação dos procedimentos de contingência estabelecidos neste plano.

A ativação do plano de contingência ficará a critério e sob a responsabilidade da Equipe de Compliance, trabalhando em conjunto com a equipe de TI. Em caso de necessidade, poderá ser contratada uma empresa especializada no combate ao evento identificado, bem como na resposta ao eventual dano.

A fim de ser adequadamente evitada, a Gestora adotará os seguintes mecanismos de resposta para cada contingência específica:

(i) Indisponibilidade da Sede:

Caso o escritório não esteja disponível durante o horário comercial, as Pessoas sob Supervisão permanecerão disponíveis e desempenharão suas funções em sistema de *home office*;

(ii) Indisponibilidade de Servidores (Nuvem)

Uma vez verificada a indisponibilidade, a Gestora ativará seu plano de recuperação de desastres e iniciará a transição para a ativação de seu local DR. Isto deve ser relativamente rápido, mas em caso de atraso, os profissionais da Gestora devem permanecer trabalhando normalmente e, quando apropriado, executar suas tarefas em sistema de *home office*;

(iii) Indisponibilidade de Conexão com o Provedor de Internet

A indisponibilidade pode ser dividida em 2 (duas) hipóteses: (i) se a indisponibilidade for inferior a 4 (quatro) horas, será avaliada a necessidade de substituição temporária dos provedores de acesso à internet, assim como haverá um contato com os provedores de internet para que a conexão seja restaurada; e (ii) se a indisponibilidade for superior a 04 (quatro) horas, ou se não houver previsão para restauração da conexão, os provedores de acesso à internet serão substituídos e uma empresa especializada será realocada para restaurar a conexão, ou encontrar uma solução alternativa, ainda que temporária, se o fornecedor terceirizado de tecnologia da informação da Gestora não puder resolver. Os profissionais permanecerão na sede da Gestora e ali desempenharão suas funções;

(iv) Redução de Profissionais

A Gestora avaliará a possibilidade de transporte até sua sede e determinará as funções a serem desempenhadas pelos profissionais disponíveis até que uma solução alternativa seja encontrada, mesmo que temporariamente. Os profissionais que não conseguirem chegar à sede da Gestora permanecerão disponíveis e desempenharão suas funções em sistema de *home office*; e

(v) Tempo de Resposta da Pessoa Sob Supervisão

É responsabilidade de cada Pessoa Sob Supervisão manter seus atuais meios de contato e sendo do conhecimento da Gestora. Da mesma forma, é responsabilidade de cada profissional estar acessível e comunicar seus respectivos locais assim que tomar conhecimento de um evento que possa comprometer a continuidade de suas funções, ainda que momentaneamente, ou dos negócios da Gestora.

9 CONTRATAÇÃO E MONITORAMENTO DE TERCEIROS

O objetivo deste dispositivo é estabelecer critérios qualitativos mínimos e orientar o processo de seleção, contratação e monitoramento de indivíduos e entidades que possam ter interesse em iniciar e manter um relacionamento comercial com a Gestora.

Este é um procedimento real de *Know Your Partner* – KYP, focado no conhecimento do terceiro a ser contratado, nos procedimentos de integridade instituídos e observados pelas empresas que operam com a Gestora.

Os critérios e processos aqui estabelecidos visam proporcionar o mínimo indispensável de segurança operacional e jurídica, evitando conflitos de interesse de forma a manter a Gestora em conformidade com o Código ANBIMA de Regulação e Melhores Práticas de Administração de Recursos de Terceiros e outras normas e regras aplicáveis à matéria.

9.1 Análise de Mercado

Sempre avaliar se:

(i) esse prestador de serviços pode gerar qualquer potencial conflito de interesse com o gestor de recursos, administrador fiduciário ou cotista dos Veículos geridos pela Gestora;

(ii) o valor cobrado é justo em relação ao serviço oferecido e ao valor de mercado; e

(iii) há benefícios recebidos pela Gestora e seus profissionais derivados de tal contratação, ou se os benefícios são direcionados ao Veículo ou ao Investidor.

9.2 Processo de Pré-Seleção

Durante o processo de contratação, os profissionais devem obter informações qualitativas sobre o terceiro interessado em iniciar vínculos legítimos com a Gestora, a fim de permitir um melhor julgamento durante a pré-seleção. As informações a serem obtidas devem incluir:

(i) A data de início das atividades;

(ii) Qualificações dos principais sócios/executivos;

(iii) Lista de clientes (passados e atuais) e objeto da contratação;

(iv) Busca na rede mundial de computadores sobre notícias negativas sobre o terceiro; e

(v) Outras informações qualitativas que possam ser relevantes para melhor avaliar o terceiro.

O terceiro deverá estar legalmente constituído, gozar de boa reputação, ter capacidade econômica, financeira e técnica compatível com o objeto do contrato e com a assunção de responsabilidades contratuais.

Cópias do cartão de registro no Cadastro Nacional da Pessoa Jurídica (CNPJ) e documentos constitutivos e/ou corporativos relevantes devem ser solicitados ao terceiro. Se necessário, devem ser solicitadas cópias das demonstrações financeiras dos últimos 3 (três) anos e referências bancárias e técnicas do terceiro.

Além disso, os seguintes aspectos devem ser considerados durante o processo de pré-seleção:

(i) Estrutura da empresa;

(ii) Boa reputação (no caso de uma pessoa jurídica, a reputação dos sócios e dos principais executivos também deve ser considerada);

(iii) Nível de satisfação de outros clientes, passados e presentes;

(iv) Estrutura para atender o objeto da Contratação;

(v) Capacidade econômica e financeira;

(vi) Código de Conduta e Ética, ou similar;

(vii) Política Anticorrupção, ou similar;

(viii) Política de Combate à Lavagem de Dinheiro, ou similar;

(ix) Qualquer documento, procedimento e/ou formulário relacionado com a integridade e o cumprimento das regras; e

(x) Selo de Associado ou Aderente à ANBIMA, quando aplicável, ou, se não for o caso, as razões para não obtê-lo.

Após a revisão do procedimento de *due diligence* realizado, o profissional responsável pela contratação classificará o fornecedor de acordo com seu risco potencial, segundo o **Anexo I** desta Política.

O início das atividades dos empregados estará vinculado à formalização do contrato e nenhum pagamento poderá ser feito antes da conclusão do contrato. Os acordos celebrados para formalização do contrato deverão ter os requisitos contidos no artigo 19 do Código ANBIMA de Regulação e Melhores Práticas de Administração de Recursos de Terceiros, devendo prever, no mínimo, conforme aplicável:

(i) As obrigações e deveres das partes envolvidas;

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

(iii) A obrigação de cumprir suas atividades em conformidade com as disposições previstas no Código ANBIMA de Regulação e Melhores Práticas de Administração de Recursos de Terceiros e na regulamentação em vigor específica, no que aplicável, para cada tipo de fundo de investimento; e

(iv) Que os terceiros contratados devem, no limite de suas atividades, deixar à disposição da Gestora, quando aplicável, todos os documentos e informações exigidos pela regulamentação em vigor que sejam necessários para a elaboração de documentos e informes periódicos obrigatórios, salvo aqueles considerados confidenciais, nos termos da regulamentação em vigor.

Os empregados responsáveis pelo processo de seleção de fornecedores manterão registros atualizados dos fornecedores, eliminando aqueles sobre os quais haja qualquer dúvida relativa a má conduta, comportamento antiético, comportamento ilícito ou que possam ter uma má reputação no mercado.

9.3 Não Aplicabilidade do Processo de Pré-Seleção

A Gestora poderá deixar de aplicar os procedimentos ora estabelecidos, a seu critério exclusivo, quando o terceiro não estiver relacionado ao negócio principal do gestor de recursos e tiver uma clara capacidade econômica, financeira e/ou técnica para satisfazer o objeto da contratação e para cumprir suas responsabilidades e arranjos contratuais.

9.4 Outras Disposições

Como parte do Grupo Altre, a Gestora é atendida pelo centro de serviços compartilhados da VSA, denominado Centro de Excelência ("**COE**"), compartilhando, entre outros, os serviços das áreas de TI com outras investidas da VSA. Os prestadores de serviços de TI do COE que atendem a Gestora estão sujeitos às medidas prévias de *due diligence* para a contratação e monitoramento de terceiros relacionados à tecnologia, sistemas e/ou infraestrutura de informação, visando à proteção de dados.

9.5 Seleção de Intermediários

A Gestora, com a prestação de serviços adequados que garantam a melhor execução das ordens para Veículos sob sua gestão, juntamente com a preservação dos interesses e, consequentemente, de seus Investidores, adota um cuidadoso processo de seleção e contratação de intermediários.

Esse processo é baseado na devida investigação de potenciais corretores-distribuidores de valores mobiliários para permitir que a Gestora adquira um conhecimento profundo de potenciais prestadores de serviços.

Ao avaliar potenciais prestadores de serviços, a Gestora adota 3 (três) princípios para selecionar corretores que irão intermediar ativos financeiros para Veículos sob sua gestão:

(i) Estrito cumprimento do dever fiduciário;

(ii) Reconhecida capacidade de execução; e

(iii) Mínimo impacto financeiro.

Com base nestes princípios, os intermediários devem ser considerados como terceiros, para fins de aplicação do Processo de Pré-seleção, incluindo a suposição de que o Processo de Pré-seleção poderá não ser realizado quando o intermediário for Associado ou Aderente aos códigos ANBIMA.

9.6 Monitoramento

O monitoramento das atividades realizadas por terceiros para a Gestora, assim como os próprios terceiros, é de responsabilidade da área que solicitou a contratação. O monitoramento deve ser contínuo durante a vigência da contratação, e o terceiro avaliado proporcionalmente ao serviço prestado, com ênfase em eventuais disparidades de tempo, qualidade e quantidade esperada.

Além disso, o monitoramento deve ser capaz de identificar preventivamente atividades que possam resultar em riscos para a Gestora, e os respectivos relatórios devem ser enviados para a Equipe de Compliance.

No caso de qualquer fato novo ou mudança significativa, é possível reavaliar a contratação de terceiros.

É importante notar que este monitoramento se baseia no princípio dos melhores esforços, já que a Gestora e seus profissionais não podem estar presentes no dia a dia de terceiros contratados a todo tempo.

9.7 Manutenção de Documentos

Todos os manuais, relatórios, atas e outros documentos relacionados a essa seleção de terceiros e à presente Política serão mantidos em arquivos físicos ou armazenados digitalmente no escritório da Gestora por um mínimo de 5 (cinco) anos.

10 SEGREGAÇÃO DE ATIVIDADES

10.1 Segregação das Atividades de Compliance, Gestão de Risco e Investimento e de Consultoria Especializada

As Equipes de Compliance é independente e segregada das atividades realizadas pela equipe responsável pela gestão da carteira de investimentos da Altre ("**Equipe de Investimento**"), e a Equipe de Compliance não participará de nenhuma atividade relacionada à tomada de decisão dos investimentos, incluindo, mas não se limitando, à gestão das carteiras, negociações de corretagem ou participação em análises de investimento, a menos que se relacione ao impacto do referido investimento ou de suas contrapartes para fins de análise de risco ou de compliance (conforme aplicável).

As comunicações entre as atividades realizadas pela Equipe de Compliance e as atividades da Equipe de Investimento serão realizadas por meio de reuniões e relatórios preparados pela

Equipe de Investimento e pela participação, como ouvinte, exclusivamente, do Diretor de Compliance no Comitê de Investimentos, ambos com a finalidade de permitir que a Equipe de Compliance possa (i) se certificar do cumprimento das normas e regulamentos internos, incluindo o Código de Ética, esta Política e demais regras da Altre; (ii) supervisionar (a) a exposição de risco da carteira gerida pela Altre, (b) as decisões de investimento tomadas pelo Diretor de Gestão (incluindo a verificação de que a carteira está de acordo com a Política de Gestão de Risco da Gestora), e (c) da elaboração de relatórios referentes à exposição de risco; (iii) acessar ao risco comercial e/ou de contraparte; e (iv) preparar os relatórios anuais nos termos das leis e regulamentos aplicáveis.

A Gestora também possui como atividade secundária à sua principal atividade de gestão de recursos, a prestação de serviços de consultoria especializada. Tal atividade será incidental e inerente às atividades de gestão de recursos e, portanto, não representa uma linha de negócios independente, não demanda qualquer tipo de prévio registro perante a autoridade reguladora e nem é conflitante com a atividade de gestor de recursos de carteiras. Considerando que não há conflito de interesses entre essa atividade e a atividade principal da Gestora, não há uma segregação física, nem funcional. Os eventuais serviços de consultoria serão executados pelas mesmas Equipes de Investimento e de Compliance, observado que não haverá conflito de interesses (pela natureza diversa dos ativos) e que há mecanismos nas políticas da Gestora que endereçam eventuais situações de conflito de interesses.

10.2 Segregação de Atividades no âmbito da VSA

Como mencionado acima, a Gestora é atendida pelo COE, compartilhando os serviços das áreas de TI, seguros e serviços administrativos gerais com outras investidas da VSA. Adicionalmente, a Gestora é atendida por prestador de serviço terceirizado e especializado, que também atende à Altre Properties, para a prestação de serviços financeiros e de contabilidade.

Visando mitigar potenciais conflitos de interesses, a Altre Properties e as demais investidas da VSA terão atividades segregadas da Gestora.

Nesse sentido, a Gestora possuirá segregação física das instalações entre Altre e Altre Properties, com espaço dedicado e com acesso controlado para as atividades da Altre, especialmente a segregação física e de informações das atividades de administração de carteiras de valores mobiliários pela Equipe de Investimento. Adicionalmente, a Gestora adota regras estritas para prevenção e monitoramento do cumprimento e investimentos pessoais de todos os seus parceiros e Pessoas sob Supervisão conforme previsto nesta Política e no Código de Ética da Altre.

A Gestora adotará, ainda, seus melhores esforços para evitar potenciais conflitos de interesses, de modo que para aumentar de maneira completa a segregação de informações, os seguintes procedimentos deverão ser observados:

1. a segregação física das instalações entre Altre e Altre Properties, com espaço dedicado e com acesso controlado para as atividades da Altre; assim como a segregação física e lógica entre suas áreas dentro de suas próprias instalações, conforme aplicável;

2. a preservação de informações confidenciais por todas as Pessoas sob Supervisão, proibindo a transferência de informações a terceiros não qualificados que possam usá-las indevidamente. As informações confidenciais serão mantidas somente por

terceiros essenciais para o desenvolvimento dos projetos, não podendo ser compartilhadas com outros terceiros sem o consentimento prévio do Diretor de Compliance;

3. implementação e manutenção de programas de treinamento para diretores, funcionários, terceiros e prestadores de serviços que tenham acesso a informações confidenciais e/ou participem do processo de tomada de decisão de investimento; e

4. o acesso restrito a arquivos e dados, assim como a adoção de controles que restringem e permitem identificar indivíduos que têm acesso a informações confidenciais.

Não obstante o exposto acima, os potenciais conflitos de interesse envolvendo Veículos geridos pela Altre deverão ser previamente identificados, monitorados e divulgados pela Gestora aos seus investidores e clientes, nos termos da regulamentação e autorregulamentação aplicáveis.

Nesse sentido, a Altre tem como preceitos básicos a transparência e divulgação às partes envolvidas de situações de potencial conflito de interesses entre seus fundos e clientes, preceitos estes corroborados na regulamentação aplicável aos FIP e FII, que exige necessariamente a divulgação e aprovação de atos que configurem potencial conflito de interesses (por exemplo, artigos 9º e 24, inc. XII da Instrução CVM nº 578, para FIP, e artigo 18, inc. XII da Instrução CVM nº 472 para FII).

Ademais, eventuais conflitos de interesse serão expostos com destaque dentro do regulamento dos futuros Veículos e, caso necessário, serão objeto de deliberação prévia em assembleia de cotistas, para que seja dado o devido *disclaimer* a potenciais investidores, nos termos da regulamentação em vigor. Adicionalmente, a Altre contará com prestadores de serviços terceirizados e especializados que serão engajados para condução de processos de auditoria técnica e legal dos ativos em prospecção pela Gestora, bem como, sempre que houver potencial conflito de interesses e um valor de mercado não seja claramente estabelecido para um ativo, a Altre contratará ou fará com que seja contratado laudo de avaliação dos ativos a serem adquiridos pelos veículos sob sua gestão, de forma a garantir que a transação seja feita de acordo com parâmetros de mercado.

O Diretor de Compliance será responsável pela promoção da avaliação e monitoramento independente das atividades realizadas pela Altre e quaisquer conexões com o Grupo Altre.

11 TREINAMENTO

Como parte de seu programa de controles internos, a Gestora dará treinamento sobre esta Política para todas as Pessoas sob Supervisão e, se necessário, para afiliados e prestadores de serviços terceirizados. O treinamento poderá incluir, entre outros tópicos, instrução sobre a criação de senhas fortes, detecção de e-mails de *phishing*, dispositivos aprovados, sincronização de dispositivos pessoais e redução da exposição a e-mails. O treinamento ocorrerá periodicamente e sua frequência dependerá de uma série de fatores, incluindo, mas não se limitando, à evolução das ameaças à segurança. O treinamento pode se dar na forma de reuniões em toda a empresa, distribuição de materiais escritos ou orientação fornecida por e-mail. O Diretor de Compliance será responsável por manter um registro de quaisquer orientações ou materiais escritos fornecidos durante tal treinamento.

(i) Integração Inicial

Além disso, sempre que um profissional for contratado, e antes do início efetivo de suas atividades, ele participará de um processo de integração e treinamento onde adquirirá conhecimento sobre as atividades da empresa, regras, políticas e códigos internos, assim como informações sobre as principais leis e regulamentos que regem as atividades da Gestora. Esse será um treinamento de integração com o objetivo de demonstrar as políticas, os códigos e a filosofia da empresa. O treinamento inicial também abordará os diferentes produtos oferecidos pela Gestora.

Ao ser contratado e iniciar as atividades, o empregado receberá, além desta Política, os seguintes Códigos e Políticas, conforme aplicáveis às funções que serão exercidas:

(a) Código de Ética (todos os profissionais);

(b) Política de Decisão, Alocação e Divisão de Ordens de Investimento (profissionais que necessitem conhecer esta política, em razão das funções que serão exercidas);

(c) Política de Gerenciamento do Risco (todos os profissionais);

(d) Política de Combate à Lavagem de Dinheiro e à Corrupção (todos os profissionais);

(e) Política de Segregação de Atividades (todos os profissionais);

(f) Política de Voto (profissionais que necessitem conhecer esta política, em razão das funções que serão exercidas);

(g) Política de Investimento em Crédito Privado (profissionais que necessitem conhecer esta política, em razão das funções que serão exercidas); e

(h) Política de Aquisição e Monitoramento de Ativos Imobiliários (profissionais que necessitem conhecer esta política, em razão das funções que serão exercidas).

(ii) Treinamento contínuo

Em conformidade com esta norma e os valores de nossa instituição, a Gestora adotará um programa anual de reciclagem de seus profissionais, a fim de garantir que eles estejam sempre atualizados sobre os termos e responsabilidades aqui descritos, estando todos obrigados a participar de tais programas de reciclagem.

Esse programa anual de reciclagem de profissionais consiste, entre outras atividades, em uma apresentação presencial das políticas mencionadas no capítulo acima, que aborda os principais pontos das políticas em vigor no momento da apresentação, a fim de manter os seus profissionais sempre alinhados com as regras dos órgãos reguladores e da própria empresa.

Além disso, no caso de qualquer mudança nas políticas, devido a exigências regulatórias ou outros motivos, a Gestora poderá conduzir um eventual programa de reciclagem a fim de fornecer-lhes a nova política bem como apresentar as mudanças e novos pontos abordados por tal política.

Finalmente, deve-se observar que o processo do treinamento inicial e o programa de reciclagem contínua serão desenvolvidos e controlados pelo Diretor de Compliance e exigem o compromisso total dos profissionais com seu atendimento e dedicação.

(iii) Programas de Treinamento

Um programa de treinamento eficaz inclui disposições para garantir que: ***(i)*** o treinamento seja contínuo, incorporando eventos atuais e mudanças em códigos, políticas e produtos, bem como leis e regulamentos relativos à sua atividade; ***(ii)*** o treinamento se concentre na educação dos profissionais sobre as políticas e valores da empresa; e ***(iii)*** o treinamento exponha as consequências do não cumprimento da política e procedimentos estabelecidos por parte de um profissional (multa, suspensão, rescisão do contrato de trabalho no caso de profissionais ou exclusão da sociedade no caso de sócios); e ***(iv)*** o conteúdo do treinamento para cada Pessoa sob Supervisão também seja específico para as atividades realizadas por cada um deles.

12 VIOLAÇÕES E MEDIDAS DISCIPLINARES

12.1 Violações

Deixar de cumprir com esta Política é uma conduta inadequada, vista como um assunto sério que deve ser relatado e tratado e que pode levar a uma medida disciplinar. A existência de normas, políticas e procedimentos é condição essencial para assegurar a perenidade. Cuidar para que sejam seguidos a todo tempo é responsabilidade de cada um.

Descumprimento de normas e regras da Altre não são tolerados e são passíveis de punição. Caso tenha ocorrido uma violação, a natureza de qualquer medida disciplinar ou corretiva será determinada pelo Diretor de Compliance, que poderá consultar o Comitê de Compliance sobre o tema, bem como outros especialistas, incluindo os departamentos Jurídico e de Recursos Humanos. As medidas corretivas dependerão da gravidade da violação e de outras circunstâncias relevantes.

É importante esclarecer que casos de violação que incluam uma infração da lei serão encaminhados às autoridades policiais competentes.

12.2 Comportamento Esperado

Caso uma Pessoa sob Supervisão presencie ou saiba de uma violação a esta Política, esperamos que essa pessoa exponha as questões imediatamente ao seu superior direto. Caso a violação inclua a Pessoa Sob Supervisão em questão, esta deve procurar o Diretor de Compliance ou a Linha Ética, além de cooperar com possíveis investigações sobre tal violação.

Investigações internas incluem aspectos procedimentais sérios e, por essa razão, somente podem ser realizadas pela equipe apropriada.

12.3 Medidas Disciplinares

Medidas disciplinares têm por objetivo estabelecer regras para garantir os padrões de comportamento exigidos e devem ser aplicadas em todas as situações em que um comportamento estiver em desacordo com esses padrões. As aplicações dependerão da gravidade da violação e de outras circunstâncias relevantes e podem incluir:

(i) Advertência verbal ou por escrito;

(ii) Suspensão; e

(iii) Demissão com ou sem justa causa.

A aplicação de penalidades deve ser feita, tanto quanto possível, logo em seguida à falta cometida, sob pena de caracterizar o perdão tácito. Admite-se um período maior de tempo para

a aplicação de penalidade quando a falta requerer apuração de fatos e das devidas responsabilidades.

Os casos de aplicação da gestão de consequências devem ser discutidos no âmbito do Comitê de Compliance, com a decisão final cabendo ao Diretor de Compliance.

13 DISPOSIÇÕES GERAIS

Esta Política está disponível no website da Gestora, de acordo com o Artigo 16, III, da Resolução CVM 21.

14 VIGÊNCIA E ATUALIZAÇÃO

Esta Política será revisada anualmente pela Gestora e será alterada na medida em que houver a necessidade de atualizar seu conteúdo. Além disso, esta Política poderá ser alterada a qualquer momento, se as circunstâncias assim o exigirem.

* * *

Anexo I
Metodologia de Avaliação do Risco e Monitoramento Individualizado

Com vistas ao cumprimento do novo Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, após a análise do terceiro, a Equipe de Compliance classificará o terceiro com o potencial de (i) Baixo Risco; (ii) Médio Risco; ou (iii) Alto Risco, conforme segue:

1. Metodologia e Avaliação

1.1. Baixo Risco

Terceiros com Potencial Baixo Risco: a Gestora pode deixar de aplicar os procedimentos de pré-seleção estabelecidos nesta política a seu exclusivo critério quando também se verificar que o terceiro, cumulativamente: (i) possui destacada capacidade econômica e financeira e/ou técnica para satisfazer o propósito do contrato, (ii) possui capacidade para cumprir as responsabilidades contratuais estabelecidas; e (iii) possui reputação ilibada e (iv) é membro/associado da ANBIMA, quando aplicável.

1.2. Médio Risco

Terceiros com Potencial Médio Risco: a Gestora adotará os procedimentos estabelecidos nesta política, e documentos adicionais poderão ser solicitados conforme o caso. Serão classificados como de Médio Risco terceiros que não possam ser classificados como de Baixo Risco, mas que não tenham sua atividade relacionada com a atividade fim da Gestora.

1.3. Alto Risco

Terceiros com Potencial Alto Risco: a Gestora sujeitará o terceiro à mais completa investigação, de acordo com os procedimentos adotados na Política Anticorrupção, Código de Ética, Combate à Lavagem de Dinheiro e outros documentos e certificados necessários de terceiros. Será classificado como de Alto Risco o terceiro que não se enquadrar nas hipóteses anteriores.

Uma vez classificado como um terceiro de Alto Risco, a decisão final sobre a contratação desse terceiro caberá ao Comitê de Compliance, juntamente com um relatório derivado de sua análise da documentação recebida pelo terceiro durante o Processo de Pré-seleção.

2. Monitoramento

Terceiros serão supervisionados e reavaliados de acordo com sua classificação por grau de risco e segundo os artigos 23 e 24 do Código ANBIMA de Regulação e Melhores Práticas de Administração de Recursos de Terceiros, como se segue:

(i) Baixo Risco: Uma vez a cada 36 (trinta e seis) meses;

(ii) Médio Risco: Uma vez a cada 24 (vinte e quatro) meses; e

(iii) Alto Risco: Uma vez a cada 12 (doze meses).