TS GESTÃO E CONSULTORIA IMOBILIÁRIA LTDA.

POLÍTICA DE SEGREGAÇÃO, CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA.

Vigência: dezembro - 2018
Data da Última Revisão: maio - 2022
Versão 4

ÍNDICE

1. INTRODUÇÃO

Esta Política de Segregação, Confidencialidade e Segurança da Informação e Cibernética ("Política") é elaborada em conformidade com o disposto na Resolução CVM nº 21, de 25 de fevereiro de 2021 ("Resolução CVM nº 21"), e nos Códigos ANBIMA aplicáveis e aderidos pela **TS GESTÃO E CONSULTORIA IMOBILIÁRIA LTDA.** ("Gestora"), tendo por objetivo estabelecer princípios, conceitos e valores que orientam a conduta de todos aqueles que possuam cargo, função, posição, relação societária, empregatícia, comercial, profissional, contratual ou de confiança ("Colaboradores") com a Gestora, tanto na sua atuação interna quanto na comunicação com os diversos públicos.

Conforme previsto no item 3.1 desta Política, o objetivo da Gestora consiste na atuação no mercado financeiro imobiliário, tendo como principal atividade, portanto, a gestão de fundos de investimento com foco em ativos imobiliários, sendo que estes serão constituídos como fundos de investimento imobiliário (FII), focados na aquisição direta de imóveis para exploração ou comercialização ("Fundos").

Assim sendo, esta Política reúne algumas diretrizes que devem ser observadas pelos Colaboradores da Gestora no desempenho da atividade profissional.

2. POLÍTICA DE CONFIDENCIALIDADE

2.1. Sigilo e Conduta

Por informação confidencial entende-se toda e qualquer informação não disponível ao público, ou seja, informação eletrônica, escrita ou falada da qual o Colaborador tenha acesso dentro da Gestora, incluindo: dados da Gestora, seus sócios, diretores, Investidores, Colaboradores, bem como de relatórios de órgãos reguladores, autorreguladores e do poder público, dados de inspeções e fiscalizações, materiais de marketing e demais informações de propriedade da Gestora.

Não se caracteriza descumprimento desta Política a divulgação de informações confidenciais quando em atendimento a determinações legais, de órgãos reguladores e fiscalizadores e quando a divulgação se justificar, por força da natureza do negócio, a advogados, auditores e contrapartes.

As seguintes diretrizes devem ser seguidas por todos os Colaboradores:

- As informações confidenciais devem ser tratadas de forma ética e sigilosa e de acordo com as leis e normas internas vigentes, evitando-se mau uso e exposição indevida.
- A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada.
- A concessão de acessos às informações confidenciais deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades.
- A identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.
- Segregação de instalações, equipamentos e informações comuns, quando aplicável.
- A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento.
- Qualquer risco ou ocorrência de falha na confidencialidade e na segurança da informação devem ser reportados à Diretora de *Compliance*, Risco e PLD.

Conforme disposto em termo disponibilizado em sistema próprio pela Gestora, assinado por cada Colaborador, nenhuma informação confidencial, privilegiada ou reservada deve, em qualquer hipótese, ser divulgada fora do âmbito das atividades da Gestora. Fica vedada qualquer divulgação, no âmbito pessoal ou profissional, que não esteja em acordo com as normas legais e de *compliance* da Gestora (especialmente, mas não de forma limitada, aquelas transcritas no **Anexo I** desta Política).

Na questão de confidencialidade e tratamento da informação, o Colaborador deve cumprir o estabelecido nos itens a seguir, sem prejuízo do disposto na regulamentação aplicável.

2.1.1. Informações Confidenciais, Privilegiadas ou Reservadas

São consideradas informações confidenciais, para os fins desta Política, independente destas informações estarem contidas em discos, pen-drives, fitas, e-mails, outros tipos de mídia ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre a Gestora, sobre as empresas pertencentes ao seu conglomerado, seus sócios e clientes, incluindo:

a) *Know-how* técnicas, cópias, diagramas, modelos, amostras, programas de computador;
b) Informações técnicas, financeiras ou relacionadas a estratégias de investimento e desinvestimento ou comerciais; incluindo saldos, extratos e posições de clientes dos Fundos de que é gestora;
c) Operações estruturadas, demais operações e seus respectivos valores analisadas ou realizadas pelos Fundos de que é gestora;

d) Relatórios, estudos e opiniões internas sobre ativos financeiros;
e) Relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;
f) Informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Gestora e a seus sócios ou clientes;
g) Informações a respeito de resultados financeiros antes da publicação dos balanços, balancetes e/ou demonstrações financeiras dos Fundos de que é gestora;
h) Transações realizadas e que ainda não tenham sido divulgadas publicamente; e
i) Outras informações obtidas junto a sócios, diretores, funcionários, *trainees*, estagiários ou jovens aprendizes da Gestora ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

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

Nenhuma informação confidencial deve ser deixada a vista. Ao usar uma impressora coletiva, o Colaborador deve recolher o documento impresso imediatamente.

Adicionalmente, após a utilização do respectivo documento que contenha informação confidencial, o Colaborador deverá destruí-lo, ou arquivá-lo nos termos do item 4.1.3 abaixo.

Fica terminantemente proibido que os Colaboradores discutam ou acessem remotamente informações confidenciais, privilegiadas ou reservadas em locais públicos.

A Gestora reserva-se o direito de solicitar aos Colaboradores, a qualquer momento, a assinatura de termo próprio, mediante sistema disponibilizado pela Gestora, atestando o pleno conhecimento das regras e obrigações previstas nesta política. No entanto, a ausência de celebração do termo entre a Gestora e o respectivo Colaborador não exime este de observar e cumprir integralmente com a presente política.

Para fins desta Política, considera-se informação privilegiada ou reservada qualquer informação relevante, no âmbito de atuação da Gestora, que não tenha sido divulgada publicamente e que seja obtida de forma privilegiada, ou seja, em decorrência da relação profissional ou pessoal mantida com um cliente, com pessoas vinculadas às empresas analisadas, com prestadores de serviço, ou com quaisquer terceiros.

Exemplos de informações privilegiadas são informações verbais ou documentadas a respeito de resultados operacionais de empresas, alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores

mobiliários, inclusive ofertas iniciais de ações (IPO), projetos imobiliários e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da Gestora e que ainda não foi devidamente levado à público.

As informações privilegiadas devem ser mantidas em sigilo por todos os Colaboradores que a elas tiverem acesso, seja em decorrência do exercício da atividade profissional, de relacionamento pessoal ou mesmo de forma involuntária, zelando para que subordinados e terceiros contratados que tiveram contato com as informações privilegiadas também o façam, mediante a assinatura de termo de confidencialidade ou cláusula contratual estabelecendo tal obrigação, respondendo o Colaborador pelos danos causados na hipótese de descumprimento.

Caso os Colaboradores tenham acesso acidental, por qualquer meio, a informação privilegiada, deverão levar tal circunstância ao imediato conhecimento da Diretora de *Compliance*, Risco e PLD, indicando, além disso, a fonte da informação privilegiada assim obtida. Os Colaboradores que, desta forma, acessem a informação privilegiada, deverão abster-se de fazer qualquer uso dela ou comunicá-la a terceiros, exceto quanto à comunicação à Diretora de *Compliance*, Risco e PLD anteriormente mencionada.

2.1.2. Insider Trading, “Dicas” e Front-running

Insider Trading significa a compra e venda de títulos ou valores mobiliários com base no uso de informação privilegiada, com o objetivo de conseguir benefício próprio ou para terceiros (compreendendo os Colaboradores da Gestora e pessoas a eles vinculadas).

“Dica” é a transmissão, a qualquer terceiro, estranho às atividades da Gestora, de informação privilegiada que possa ser usada com benefício na compra e venda de títulos ou valores mobiliários.

Front-running significa a prática que envolve aproveitar alguma informação privilegiada para realizar ou concluir uma operação antes de outros.

É expressamente proibido valer-se das práticas descritas acima para obter, para si ou para outrem, vantagem indevida mediante negociação, em nome próprio ou de terceiros, de títulos e valores mobiliários, sujeitando-se o Colaborador às penalidades descritas nesta Política e na legislação aplicável, incluindo eventual demissão por justa causa, além de eventuais consequências penais aplicáveis.

As regras de “*Informação Privilegiada*”, “*Insider Trading*, Dicas e *Front-running*” devem ser respeitadas não só durante a vigência de seu relacionamento com a Gestora, mas também após o seu término, não podendo utilizar informações materiais e não públicas

a quem teve acesso em decorrência de sua atuação profissional na gestora ou não.

3. CONFLITO DE INTERESSES E SEGREGAÇÃO DAS ATIVIDADES

3.1 Introdução

Atualmente, a Gestora desempenha atividades voltadas para a gestão de carteiras de valores mobiliários, está representada pela gestão de fundos de investimento imobiliário e distribuição de cotas de fundos de que é gestora, nos termos permitidos pela Resolução CVM nº 21, as quais são exaustivamente reguladas pela Comissão de Valores Mobiliários ("CVM"), bem como possui equipe especializada que presta serviços de consultoria **imobiliária, não sendo, portanto, aplicável a consultoria de valores mobiliários, a qual é regulada pela CVM na Resolução CVM nº 19, de 25 de fevereiro de 2021 ("Resolução CVM nº19").**

3.2. Conflito entre atividades da Gestora

A atividade de gestão de carteiras de valores mobiliários desenvolvidas pela Gestora exige credenciamento específico e está condicionada a uma série de providências, dentre elas a segregação total de suas atividades de administração de carteiras de valores mobiliários de outras que futuramente possam vir a ser desenvolvidas (com exceção da distribuição de cotas de Fundos que é gestora, conforme regulamentação em vigor) pela Gestora ou empresas controladoras, controladas, ligadas ou coligadas, bem como prestadores de serviços.

Neste sentido, todo e qualquer serviço alheio à gestão de carteira de valores mobiliários deverá ser executado com ampla transparência e especial cuidado quanto aos potenciais conflitos. Assim, a Gestora irá exercer todo e qualquer atividade com lealdade em relação aos seus clientes/investidores, evitando quaisquer práticas que possam ferir a relação fiduciária com eles mantida.

Os Colaboradores da Gestora devem notificar a Diretora de Compliance, Risco e PLD se tomarem conhecimento sobre quaisquer conflitos de interesse real ou potencial. Os Colaboradores da Gestora são responsáveis por garantir que os conflitos de interesse sejam tratados de maneira apropriada e de acordo com os deveres fiduciários da Gestora para com seus Clientes.

Caso seja identificada uma situação de potencial conflito de interesse, a Diretora de Compliance, Risco e PLD determinará que a prospecção do novo negócio seja suspensa até que o potencial conflito de interesses seja resolvido, ou interrompida de forma sumária e definitiva, na hipótese de um conflito absoluto e irremediável. Com relação à confidencialidade e integridade das informações, os Colaboradores possuem uma senha de usuário para acesso aos sistemas da Gestora, visando a proteção e

segregação de todos os arquivos e documentos, sendo certo que os membros da equipe de gestão de recursos de terceiros e os membros da equipe de consultoria imobiliária terão diretórios separados.

Considerando que a Gestora poderá contratar terceiros para a prestação de serviços de *back office*, a Gestora adota regras e procedimentos internos capazes de assegurar a completa segregação de funções, atividades e responsabilidades relacionadas com a gestão e distribuição de cotas de Fundos de que é gestora.

Caso a Gestora contrate os serviços mencionados acima, todos os Colaboradores que tiverem suas atividades profissionais relacionadas com a administração de carteiras de valores mobiliários e distribuição de cotas de Fundos de que é gestora, serão alocados em local diverso dos demais prestadores de serviços, incluindo acesso exclusivo por meio de ponto eletrônico, disponibilização de linhas telefônicas específicas e diretório de rede privativo e restrito, acessível somente mediante login e senha individuais.

Todas e quaisquer informações e/ou dados de natureza confidencial (incluindo, sem limitação, todas as informações técnicas, financeiras, operacionais, econômicas, bem como demais informações comerciais) referentes à Gestora, suas atividades e seus clientes e quaisquer cópias ou registros dos mesmos, orais ou escritos, contidos em qualquer meio físico ou eletrônico, que tenham sido direta ou indiretamente fornecidos ou divulgados em razão da atividade de administração de carteiras de valores mobiliários e distribuição de cotas de Fundos, desenvolvidas pela Gestora, não deverão ser divulgadas a terceiros (incluindo prestadores de serviços de *back office*) sem a prévia e expressa autorização da Diretora de Compliance, Risco e PLD.

Neste sentido, todos os Colaboradores deverão respeitar as regras e segregações estabelecidas nesta Política e guardar o mais completo e absoluto sigilo sobre as informações que venham a ter acesso em razão do exercício de suas atividades. Para tanto, todos os Colaboradores da Gestora, ao firmar termo próprio disponibilizado em sistema pela Gestora, atestam expressamente concordância com as regras aqui estabelecidas, e se abstém de divulgar informações confidenciais, privilegiadas ou reservadas que venha a ter acesso, mesmo após o desligamento da Gestora.

3.3 Outras Atividades

A Gestora **não** tem a intenção de realizar outras atividades que não aquelas descritas em seu Contrato Social, notadamente gestão de recursos de terceiros e consultoria imobiliária e, portanto, não estará sujeita às regras de segregação de consultoria de valores mobiliários estabelecidas na Resolução CVM nº 19.

3.4. Tratamento de Conflito de Interesses no Relacionamento com Outras Empresas do mesmo Grupo Econômico da Gestora

A Gestora é uma empresa integrante do grupo Tishman Speyer ("Grupo Tishman Speyer"). As empresas do Grupo Tishman Speyer diretamente relacionadas à estrutura societária da Gestora são: (i) Tishman Speyer Properties LP; (ii) TSP Brazil LLC; (iii) TSP Participações Ltda.; (iv) TSP Incorporações Residenciais Ltda.; e (v) TSM Desenvolvimento Imobiliário Ltda.

O Grupo Tishman Speyer é líder como proprietário, incorporador, operador e administrador de fundos do mercado imobiliário de primeira classe no mundo inteiro. Fundado em 1978, o Grupo Tishman Speyer opera ativamente nos Estados Unidos, Europa, América Latina e Ásia, e muitas das mais prestigiadas corporações do mundo contam com o Grupo Tishman Speyer para atender às suas necessidades relacionadas a espaço.

Além da consultoria imobiliária, as empresas do grupo atuam também nas atividades de desenvolvimento imobiliário e administração predial, preponderantemente com relação aos ativos que receberão investimento dos veículos constituídos pelo Grupo Tishman Speyer, os quais podem estar situados tanto no Brasil quanto no exterior. O Grupo Tishman Speyer busca exercer todos os seus negócios de forma sinérgica, contudo, mantendo-se cada empresa independente, autônoma e autossuficiente em seus respectivos negócios.

Em que pese a existência de empresas exercendo atividades diversas dentro do setor de Real Estate brasileiro, a Gestora não vislumbra, em um primeiro momento, nenhum conflito de interesses impeditivo entre as empresas do Grupo Tishman Speyer. Para o tratamento de conflitos que potencialmente possam existir, considerando as situações fáticas, a Gestora se utiliza de quatro regras de salvaguarda:

I. A Gestora atesta, para todos os fins, que todo e qualquer ato que configure potencial conflito de interesse será submetido para a discussão e deliberação da assembleia geral de cotistas competente, em atendimento ao artigo 18, inciso XII, c/c artigo 34, ambos da ICVM 472. Dentre os atos que configuram potencial conflito de interesse, estão as operações entre contrapartes ou intermediários financeiros do mesmo conglomerado ou grupo econômico, bem como operações entre veículos de investimento geridos pela Gestora. Desta forma, sempre que uma operação dos fundos de investimento geridos pela Gestora envolver, de algum modo, empresas integrantes do Grupo Tishman Speyer, direta ou indiretamente, os cotistas dos fundos de investimento sob gestão da Gestora receberão informações completas sobre a relação existente entre as empresas que lhes permitam avaliar o cenário antes de tomarem uma decisão em sede de assembleia;

II. Sem prejuízo do disposto acima, todo e qualquer benefício recebido pela Gestora, diretamente ou indiretamente, através de empresas do Grupo Tishman Speyer, serão integralmente revertidos aos seus clientes, conforme estabelecido na regulamentação em vigor; e

III. Os Colaboradores do Grupo Tishman Speyer observam os mesmos deveres de confidencialidade estabelecidos na presente Política. Desta forma, os Colaboradores do Grupo Tishman Speyer atestam conhecer as políticas da Gestora, em sistema próprio da Gestora, e se comprometem a guardar sigilo sobre qualquer informação relevante à qual tenham acesso privilegiado, até sua divulgação ao mercado, bem como zelar para que subordinados e terceiros de sua confiança também o façam, respondendo pelos danos causados na hipótese de descumprimento.

4. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

4.1 Segurança da Informação e Cibernética

Todas as informações produzidas e utilizadas internamente pelos Colaboradores devem ser consideradas como ativos da Gestora e se constituem em vantagem competitiva. A proteção dessas informações e a preservação de sua confidencialidade, através de adoção dos procedimentos delineados nesta Política, é de responsabilidade e obrigação de todos os Colaboradores e uma prioridade para a Gestora.

A utilização dos ativos e sistemas da Gestora, incluindo computadores, telefones, internet, e-mail e demais aparelhos se destina prioritariamente a fins profissionais, devendo, portanto, evitar o uso indiscriminado deles para fins pessoais.

Cada funcionário da Gestora é responsável em utilizar o correio eletrônico (e-mail) de forma adequada e em conformidade com esta política. Qualquer dúvida relacionada a esta política deve ser dirigida à área de Tecnologia da Informação ou ao Departamento de Recursos Humanos. O sistema de e-mail é de propriedade da Gestora e é disponibilizado para uso nos negócios da empresa. Todas as comunicações e informações transmitidas, recebidas ou armazenadas neste sistema são registros da empresa e são de propriedade da Gestora.

Os Colaboradores não têm o direito de privacidade pessoal em qualquer material armazenado, criado, recebido ou enviado através do sistema de e-mail da Gestora. A Gestora, a seu critério, como proprietária do referido sistema, poderá exercer o direito de monitorar, acessar, recuperar e excluir qualquer material armazenado, criado,

recebido ou enviado através do sistema de e-mail, por qualquer motivo e sem autorização de qualquer Colaborador.

O Colaborador da Gestora deve estar ciente de que, ao apagar mensagens de sua caixa de e-mail, elas não serão realmente apagadas do sistema. Todas as mensagens de e-mail são armazenadas em um sistema central de back-up.

Mesmo que a Gestora tenha o direito de recuperar e ler todas as mensagens de e-mail, estas ainda devem ser tratadas como confidenciais por outros funcionários e acessadas apenas pelo destinatário. Os Colaboradores não estão autorizados a recuperar ou ler mensagens de e-mail que não lhes são destinadas.

Os Colaboradores devem ser bem-educados com outros usuários do sistema e sempre se comportarem de uma forma profissional. E-mails algumas vezes mal orientados ou encaminhados podem ser vistos por outras pessoas que não o destinatário. Os usuários devem escrever as comunicações de e-mail com cuidado, ou com a mesma responsabilidade que eles usariam para cartas ou memorandos internos escritos em papel timbrado da Gestora.

A política contra o assédio sexual da Gestora aplica-se plenamente ao sistema de e-mail. A violação dessas políticas poderá causar o desligamento do Colaborador. Portanto, nenhuma mensagem de e-mail deve ser criada, enviada ou recebida se contiver material intimidativo, hostil, ofensivo ou de distinção étnica, sexual, etária, de orientação sexual, estado civil, regional, física, religiosa ou quaisquer outras classificações protegidas por lei.

O sistema de correio eletrônico não pode ser utilizado para divulgar causas religiosas ou políticas, bem como divulgar empresas comerciais, organizações de fora ou outras solicitações de trabalho não relacionados. Os Colaboradores não podem enviar correio eletrônico não solicitado (spam) a pessoas com quem eles não têm um relacionamento anterior. O sistema de e-mail não será utilizado para envio (upload) e recebimento (download) de materiais protegidos por direitos autorais, segredos comerciais, informações financeiras de propriedade ou de materiais semelhantes sem autorização prévia da gestão da Gestora.

Os funcionários com dúvidas sobre se certas informações são protegidas por direitos autorais, de propriedade ou inapropriadas para a transferência, devem decidir- se em favor da não transferência da informação e consultar a Diretora de *Compliance*, Risco e PLD. Além disso, nenhum Colaborador pode usar o sistema de e- mail da Gestora para qualquer outra atividade ilegal.

Como os registros e arquivos de e-mails no computador podem estar sujeitos a descoberta em litígio, os funcionários da Gestora devem evitar fazer declarações em arquivos digitais ou de e-mail que não reflitam favoravelmente a Gestora.

Todo Colaborador deve ser cuidadoso na utilização do seu próprio equipamento e sistemas e zelar pela boa utilização dos demais. Caso algum Colaborador identifique a má conservação, uso indevido ou inadequado de qualquer ativo ou sistemas deve comunicar o fato à Diretora de *Compliance*, Risco e PLD.

4.1.1. Senhas de acesso

A senha e *login* para acesso aos dados contidos em todos os computadores, bem como nos e-mails que também possam ser acessados via webmail, devem ser conhecidas pelo respectivo usuário do computador e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros.

Para segurança dos perfis de acesso dos Colaboradores, as senhas de acesso dos Colaboradores são parametrizadas conforme regras estabelecidas globalmente, bem como são criptografadas com chaves de 128 bits, dificultando, portanto, sua decodificação e, consequentemente, a utilização dos *logins* dos Colaboradores por terceiros não autorizados.

Dessa forma, o Colaborador pode ser responsabilizado inclusive caso disponibilize a terceiros a senha e *login* acima referidos, para quaisquer fins.

Cada Colaborador é responsável ainda por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

Todo Colaborador deve ser cuidadoso na utilização do seu próprio equipamento e sistemas e zelar pela boa utilização dos demais. Caso algum Colaborador identifique a má conservação, uso indevido ou inadequado de qualquer ativo ou sistemas deve comunicar o fato através do Canal de Denúncias ou, alternativamente, a Diretora de Compliance, Risco e PLD.

4.1.2 Monitoramento e Controle de Acesso

O acesso pelos Colaboradores nas dependências da Gestora é realizado por meio de crachá de acesso, pessoal e intransferível, o qual é disponibilizado a cada Colaborador no momento de sua contratação. Não obstante, o acesso de pessoas estranhas à Gestora somente é permitido com a autorização expressa da equipe da Gestora.

O ambiente de pastas de rede é segregado por pastas, sendo assim, os usuários da Gestora possuem acessos apenas às pastas necessárias para a execução de suas respectivas tarefas no dia a dia. Para acessar ou modificar as permissões de acesso, se faz necessária a aprovação pelo criador da respectiva pasta ou do processo em questão.

Nesse sentido, caso a atividade de algum Colaborador na Gestora seja alterada, a área de Segurança da Informação deverá ser comunicada para verificar se o acesso às pastas do Colaborador será o mesmo em decorrência da alteração de atividade e, em caso negativo, deverá cortar e/ou incluir o acesso às pastas aplicáveis ao Colaborador. Ainda, caso o Colaborador seja desligado da Gestora, ele terá seu acesso às pastas imediatamente cortado pela área de Segurança da Informação, após prévia comunicação da área de Recursos Humanos.

Todos os anexos dos e-mails recebidos pelos Colaboradores da Gestora são rigidamente verificados pelos servidores, de modo que os Colaboradores sequer receberão e-mails que tenham sido identificados como suspeitos após tal verificação.

Adicionalmente aos controles acima, o ambiente de tecnologia da Gestora é monitorado 24 (vinte e quatro) horas por dia, durante os 7 (sete) dias da semana, de modo que eventuais falhas e quedas dos servidores são prontamente reportadas aos provedores de serviços responsáveis, para que estes tomem as devidas providências.

4.1.3 Arquivamento de Informações

De acordo com o disposto nesta Política, os Colaboradores deverão manter arquivada toda e qualquer informação, incluindo informações confidenciais, privilegiadas ou reservadas bem como documentos e extratos que venham a ser necessários para a efetivação satisfatória de possível auditoria ou investigação em torno de possíveis investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro (conforme Política de Prevenção e Combate à Lavagem de Dinheiro e Financiamento ao Terrorismo da Gestora), em conformidade com o inciso IV do Artigo 18 da Resolução CVM nº 21, em locais seguros, de modo a evitar o acesso de pessoas não autorizadas às informações ali contidas.

4.1.4. Identificação e avaliação de Riscos (risk assessment):

A Gestora identificou e avaliou os principais riscos cibernéticos aos quais está exposta. Os ataques mais comuns de criminosos cibernéticos (*cybercriminals*) são os seguintes:

a) *Malware* (vírus, cavalo de troia, *spyware* e *ransomware*);
b) Engenharia Social;
c) *Phishing scam*;
d) Acesso pessoal;
e) Ataques de DDoS e *botnets*; e
f) Invasões (*advanced persistent threats*).

4.1.5. Ações de prevenção e proteção.

A Gestora adota regras para concessão de senhas de acesso a dispositivos corporativos, sistemas e rede, em função da relevância para acesso à sede e à rede, incluindo aos servidores.

Nesse sentido, a Gestora mantém controles de rede e de sistemas, incluindo antivírus, anti-*malware, firewall*, detecção de invasão e sistemas de prevenção de ataque, monitoramento de rede e de sistemas e filtros de internet. Adicionalmente, a Gestora criptografa todos os laptops.

Os Colaboradores devem informar imediatamente qualquer situação de violação de política de privacidade à área de Segurança da Informação da Gestora, que irá investigar o incidente imediatamente.

Os eventos de *login* e alteração de senhas (conforme apontado no item 4.1.1 acima) são auditáveis e rastreáveis.

O acesso remoto a arquivos e sistemas internos ou na nuvem têm controles adequados. Outro ponto importante é que, ao incluir novos equipamentos e sistemas em produção, a Gestora deverá garantir que sejam feitas configurações seguras de seus recursos. Devem ser feitos testes em ambiente de homologação e de prova de conceito antes do envio à produção.

A Gestora conta com recursos anti-*malware* em estações e servidores de rede, como antivírus e *firewalls*. Da mesma maneira, a Gestora pode monitorar o acesso a websites e restringir a execução de softwares e/ou aplicações não autorizadas.

A Gestora realiza, também, backup das informações e dos diversos ativos da instituição, conforme as disposições do presente documento e do Plano de Continuidade de Negócios.

4.1.6. Aplicação

A efetividade desta Política depende da conscientização de todos os Colaboradores e do esforço constante para que seja feito bom uso das Informações Sigilosas e dos Ativos disponibilizados pela Gestora ao Colaborador.

Esta Política deve ser conhecida e obedecida por todos os Colaboradores que utilizam os recursos de tecnologia disponibilizados pela Gestora, sendo de responsabilidade individual e coletiva o seu cumprimento.

4.1.7. Responsabilidades na Gestão da Política

Cabe a todos os Colaboradores:

a) Cumprir fielmente esta Política;
b) Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança das Informações Sigilosas;
c) Proteger Informações Sigilosas contra acesso, modificação, destruição ou divulgação não autorizados pela Gestora;
d) Assegurar que os recursos de tecnologia à sua disposição sejam utilizados apenas para as finalidades aprovadas ou não proibidas expressamente pela Gestora;
e) Cumprir as leis e normas que regulamentam os aspectos relacionados ao direito autoral e propriedade intelectual no que se refere às Informações Sigilosas; e
f) Comunicar imediatamente à Diretora de Risco, Compliance e PLD sobre qualquer descumprimento ou violação desta Política.

4.1.8. Plano de Resposta a incidentes

Havendo indícios ou suspeita fundamentada, a área de Segurança da Informação da Gestora deverá ser acionada para realizar os procedimentos necessários de modo a identificar a ocorrência do evento. Na hipótese de vazamento de informações confidenciais, privilegiadas ou reservadas ou outra falha de segurança, inclusive em decorrência da ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas. Em caso de necessidade, poderá ser contratada empresa especializada no combate ao evento identificado.

Caso o evento tenha sido causado por algum Colaborador, deverá ser avaliada a sua culpabilidade, nos termos do Manual de *Compliance* e Código de Ética e Conduta.

5. TREINAMENTO E VERIFICAÇÃO DE CONTROLES MEDIANTE TESTES PERIÓDICOS

5.1 Treinamento e Testes Periódicos

A Gestora possui um processo de treinamento de todos seus Colaboradores, especialmente aqueles que tenham acesso a informações confidenciais, privilegiadas

ou reservadas, o qual se encontra determinado no Manual de Compliance da Gestora.

5.2. Verificação de Controles Mediante Testes Periódicos

Ainda, a Gestora entende que é fundamental a realização de testes periódicos de segurança das informações e cibernética.

Nesse sentido, a Gestora, através de sua Diretora de *Compliance*, Risco e PLD, realizará anualmente a verificação dos procedimentos adotados nesta Política, de modo a verificar o seu cumprimento pelos Colaboradores e assegurar a eficácia dos procedimentos adotados.

Para tanto, a Diretora de *Compliance*, Risco e PLD será o responsável pelo tratamento das questões de segurança das informações e cibernéticas, devendo verificar, aleatoriamente, (i) os e-mails repassados pelos Colaboradores, (ii) o modo adotado pelos Colaboradores para utilização dos ativos, sistemas, servidores e rede de informações da Gestora, e (iii) do histórico de acessos às áreas restritas da Gestora.

A presente Política deverá ser revisada pela Diretora de *Compliance*, Risco e PLD, no mínimo, a cada 24 (vinte e quatro meses).

ANEXO I

PRINCIPAIS NORMATIVOS APLICÁVEIS ÀS ATIVIDADES DA TS GESTÃO E CONSULTORIA IMOBILIÁRIA LTDA.

Resolução CVM nº 21/21
Resolução CVM nº 19/21
Ofício-Circular CVM/SIN 05/14
Lei 9.613/98
Código ANBIMA de Administração de Recursos de Terceiros
Código ANBIMA para Distribuição de Produtos de Investimento
Código ANBIMA de Certificação

Data Base: Janeiro/2022[1]

[1] **Atenção:** Todo Colaborador deve checar a vigência e eventuais alterações dos normativos contidos neste Anexo previamente à sua utilização.