ADAMCAPITAL GESTÃO DE RECURSOS LTDA.

Política de Segurança das Informações, de Proteção de Dados Pessoais e de Segurança Cibernética

Data de aprovação: 20/06/2022

ÍNDICE

POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES, DE PROTEÇÃO DE DADOS PESSOAIS E DE SEGURANÇA CIBERNÉTICA

1 Introdução

A Política de Segurança das Informações, de Proteção aos Dados Pessoais e de Segurança Cibernética ("Política") da ADAMCAPITAL GESTÃO DE RECURSOS LTDA. ("ADAM|Capital" ou "Gestora") é uma declaração formal da Gestora acerca do seu compromisso com a proteção de Informações Sigilosas e Segurança Cibernética (*cybersecurity*), conforme definição adiante, devendo ser cumprida por todos os Colaboradores.

Seu propósito é estabelecer as diretrizes a serem seguidas no que diz respeito à adoção de procedimentos e mecanismos relacionados à segurança de Informações Sigilosas.

2 Objetivo

Esta Política visa proteger as Informações Sigilosas, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das mesmas, conforme art. 4º, §8º, da Resolução CVM n.º 21/21 e conforme a Lei Geral de Proteção de Dados (Lei 13.709, de agosto de 2018), bem como aprimorar a segurança cibernética da Gestora, nos termos do Código de Administração de Recursos de Terceiros editado pela ANBIMA, seguindo as recomendações e diretrizes do Guia de Cibersegurança da ANBIMA, editado em março de 2021.

Via de regra, nenhuma Informação Sigilosa deve ser divulgada, dentro ou fora da Gestora, a quem não necessite de, ou não deva ter acesso a tais informações para desempenho de suas atividades profissionais. Qualquer informação, independentemente

de ser considerada Informação Sigilosa, seja sobre a Gestora, relativa às suas atividades, aos seus sócios, Fundos e Clientes dentre outras, ou obtida em decorrência do desempenho das atividades normais do Colaborador, só poderá ser revelada ou fornecida ao público, à mídia, ou a terceiros de qualquer natureza da maneira e conforme previstos nos documentos internos da Gestora.

Na falta de previsão expressa, a revelação ou fornecimento somente poderá ocorrer com autorização prévia e expressa do Diretor de Gestão de Riscos e de *Compliance*.

3 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.

O Termo de Responsabilidade e Confidencialidade, presente no Manual de *Compliance* e Código de Ética e Conduta, deve ser conhecido e assinado pelos Colaboradores a partir do início de seu vínculo com a Gestora.

4 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;
f) Comunicar imediatamente a Área de Gestão de Riscos e de Compliance sobre qualquer descumprimento ou violação desta Política; e
g) Atuar de forma atenta para evitar que eventos externos comprometam a segurança das informações da Gestora, como por exemplo fraudes e vírus de computador.

Cabe ao Comitê de Gestão de Riscos e de *Compliance*:

a) Estabelecer a governança para o cumprimento desta Política;
b) Deliberar sobre o plano de respostas a eventos relacionados à segurança das Informações Sigilosas; e
c) Definir sanções aos Colaboradores caso aplicável.

5 Conceitos e Princípios

Todas as Informações Sigilosas constituem ativos de valor para a Gestora, e, por conseguinte, precisam ser adequadamente protegidas contra ameaças e ações que possam causar danos e prejuízos para a Gestora, Clientes, Fundos e Colaboradores.

As Informações Sigilosas podem ser armazenadas e transmitidas de diversas maneiras, como, por exemplo, arquivos eletrônicos, mensagens eletrônicas, sites de Internet, bancos de dados, meio impresso, mídias de áudio e de vídeo, dentre outras. Cada uma dessas

maneiras está sujeita a uma ou mais formas de manipulação, alteração, remoção e eliminação do seu conteúdo.

A adoção de políticas e procedimentos que visem a garantir a segurança de Informações Sigilosas deve ser prioridade constante da Gestora, reduzindo-se os riscos de falhas, os danos e prejuízos que possam comprometer a imagem e os objetivos da Gestora. Assim, por princípio, a guarda e segurança das Informações Sigilosas deve abranger três aspectos básicos, destacados a seguir:

(i) Acesso: Somente pessoas devidamente autorizadas pela Gestora devem ter acesso às Informações Sigilosas;
(ii) Integridade: Somente alterações, supressões e adições autorizadas pela Gestora devem ser realizadas às Informações Sigilosas; e
(iii) Disponibilidade: As Informações Sigilosas devem estar disponíveis apenas para os Colaboradores autorizados sempre que necessário ou for demandado.

Para assegurar os 3 (três) aspectos acima, as Informações Sigilosas devem ser adequadamente gerenciadas e protegidas contra furto, fraude, espionagem, perda não intencional, acidentes, mau uso e outras ameaças.

Em cumprimento ao Guia de Cibersegurança da ANBIMA, a Gestora possui quatro pilares principais no seu programa de segurança cibernética:

(i) Identificação e avaliação de riscos (*risk assessment*);
(ii) Ações de prevenção e proteção;
(iii) Monitoramento e testes; e
(iv) Plano de resposta.

A implantação e monitoramento da capacidade da Gestora atender a estes pilares deverá ser feito pelo Diretor de Gestão de Riscos e de *Compliance*. Também a fim de atingir os objetivos dispostos acima, cada segmento de atuação da Gestora terá suas próprias responsabilidades.

A Gestora deverá ter uma abordagem holística em relação à segurança cibernética, sendo obrigação do Diretor de Gestão de Riscos e de *Compliance* promover treinamentos para que os Colaboradores saibam as suas respectivas funções na proteção de Informações Sigilosas, para que possam agir de maneira apropriada frente às situações que requeiram respostas.

6 Modelo Adotado

A Gestora optou por não manter time próprio dedicado à segurança das informações, segurança cibernética, contingência e outros assuntos relacionados com tecnologia da informação, inclusive para a realização de tarefas (e.g. instalações, substituições, configurações), verificações e manutenções periódicas.

Assim sendo, para implementação e monitoramento contínuo da presente Política, a Gestora conta com o suporte e assessoria de empresa terceirizada de tecnologia da informação, a Estratosfera Digital Informática e Serviços Ltda., cujo nome fantasia é Endev (http://www.endev.com.br/) (“Endev”).

Dessa mesma maneira, a Gestora não mantém grupos de trabalho ou outros fóruns para tratar de segurança cibernética. Quando necessário, as matérias relacionadas serão apresentadas pelo Diretor de Gestão de Riscos e de *Compliance* e tratadas no Comitê de Gestão de Riscos e de *Compliance*.

7 Procedimentos de Segurança Cibernética

7.1 Identificação e Avaliação de Riscos (*Risk Assessment*)

A Gestora deverá indetificar os principais riscos cibernéticos aos quais está exposta. Para isso, com o suporte da empresa Endev, é feito um levantamento dos equipamentos, sistemas, base de dados e meios de proteção utilizados a fim de melhor avaliar o grau de risco que a Gestora está exposta. Este documento se encontra presente na sede da Gestora. O Código de Segurança Cibernética da ANBIMA definiu que os ataques mais comuns de criminosos cibernéticos (*cybercriminals*) são os seguintes:

a) *Malware* (e.g. vírus, cavalo de troia, *spyware* e *ransomware*);
b) Engenharia Social (e.g. *pharming*, *phishing scam*, *vishing*, *smishing*, acesso pessoal);
c) Ataques de DDoS e *botnets*; e
d) Invasões (*advanced persistent threats*).

7.2 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. A Gestora trabalha com o princípio de que concessão de acesso deve somente ocorrer se os recursos acessados forem relevantes ao usuário.

Os eventos de login e alteração de senhas são auditáveis e rastreáveis, e 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 já na fase

de desenvolvimento e/ou planejamento. 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 anti-virus e *firewalls* pessoais. Da mesma maneira monitora o acesso a websites e restringe 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 Contingência e Continuidade do Negócio.

Caso exista a necessidade de acesso remoto por parte dos seus Colaboradores, a Gestora possui infraestrutura para que esse acesso ocorra de forma segura, utilizando *virtual private network* ("VPN") e *remote desktop,* que emula virtualmente o uso da estação de trabalho.

Adicionalmente, o acesso de pessoas que não fazem parte do quadro de Colaboradores é restrito à recepção da sede da Gestora e às salas de reunião ou atendimento (quando aplicável). Exceções a esta regra geral somente poderão ser concedidas pela Diretoria, e com a condição de que o visitante esteja acompanhado de pelo menos um Colaborador.

É importante mencionar que a Gestora não possui departamento interno de tecnologia da informação, nem realiza o desenvolvimento de sistemas internamente.

7.3 Monitoramento e Testes

Os sistemas, serviços, dados, informações (incluindo as Informações Sigilosas) disponíveis na Gestora ou por esta disponibilizados para serem usados pelos Colaboradores não devem ser interpretados como sendo de uso pessoal. Todos os Colaboradores devem ter ciência de que o uso está sujeito à monitoramento periódico,

inclusive em equipamentos pessoais acessados durante o expediente da Gestora, fazendo uso da sua rede ou não, sem frequência determinada ou aviso prévio. Esse monitoramento poderá ser realizado automaticamente (*software* e/ou *hardware*), pela Área de Gestão de Riscos e de *Compliance* e/ou por prestador de serviços externo.

Os registros obtidos e o conteúdo dos arquivos poderão ser utilizados com o propósito de determinar o cumprimento do disposto nesta Política, e nos demais documentos internos da Gestora, e, conforme o caso, servir como evidência em processos administrativos, arbitrais e/ou judiciais.

A Gestora possui roteiro de testes indicando as ações de proteção implementadas para garantir seu bom funcionamento e efetividade. Da mesma maneira deve diligenciar de modo a manter inventários atualizados de *hardware* e *software* atualizados, bem como os sistemas operacionais e *softwares* de uso atualizados.

A ADAM|Capital realiza testes de segurança no seu sistema de segurança da informação e proteção de dados, em linha, inclusive, com o Roteiro para a Realização de Testes para a Verificação de Aderência aos Documentos Internos da Gestora. Dentre as medidas, incluem-se, mas sem se limitar:

a) Verificação dos logs dos Colaboradores;
b) Alteração periódica de senha de acesso dos Colaboradores;
c) Segregação de acessos;
d) Manutenção dos *hardwares*; e
e) *Backup* diário, realizado na nuvem.

Sem prejuízo dos testes realizados na forma do Roteiro para a Realização de Testes para a Verificação de Aderência aos Documentos Internos da Gestora, a Gestora realizará, com apoio da empresa Endev e/ou empresa contratada para essa finalidade, simulações

de ataques e respostas da Gestora que seriam possíveis nestes casos. As simulações deverão prever as ferramentas mais usadas pelos criminosos cibernéticos, revelando as principais vulnerabilidades dos sistemas da Gestora, o que permitirá efetuar as correções devidas a tempo de evitar ou mitigar um ataque real.

O backup de todas as informações armazenadas nos servidores será realizado na forma descrita no Plano de Contingência e Continuidade de Negócios da Gestora, com vistas a evitar a perda de informações, e viabilizando sua recuperação em situações de contingência.

As rotinas de *backup* são periodicamente monitoradas.

7.4 Plano de Resposta

Havendo indícios ou de suspeita fundamentada, a empresa Endev deverá ser acionada pela Área de Gestão de Riscos e de *Compliance* para realizar os procedimentos necessários de modo a identificar o evento ocorrido. Os procedimentos a serem aplicados poderão variar de acordo com a natureza e o tipo do evento. Tais eventos poderão ser avaliados de acordo com a sua origem (área da Gestora onde surgiu), probabilidade de ocorrência, impacto causado e complexidade de solução.

Na hipótese de vazamento de Informações Sigilosas ou outra falha de segurança, inclusive em decorrência da ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas de modo a sanar ou mitigar os efeitos no menor prazo possível.

Em caso de necessidade, poderá ser contratada empresa especializada para combater 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.

Eventos que envolvam a segurança das Informações Sigilosas ou que sejam decorrentes de quebra de segurança cibernética deverão ser formalizados em relatório para deliberação durante o Comitê de Gestão de Riscos e de *Compliance*. Tanto o evento, quanto as medidas corretivas adotadas e a deliberação do comitê deverão, ainda que resumidamente, constar no Relatório de Controles Internos.

8 Diretrizes de Segurança da Informação

8.1 Adoção de Comportamento Seguro

Independentemente do meio e/ou da forma em que se encontrem, as Informações Sigilosas podem ser encontradas na sede da Gestora e fazem parte do ambiente de trabalho de todos os Colaboradores. Portanto, é fundamental para a proteção delas que os Colaboradores adotem comportamento seguro e consistente, com destaque para os seguintes itens:

a) Os Colaboradores devem assumir atitude proativa e engajada no que diz respeito à proteção das Informações Sigilosas;
b) Os Colaboradores devem compreender as ameaças externas que podem afetar a segurança das Informações Sigilosas, tais como vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos, etc., bem como fraudes destinadas a roubar senhas de acesso aos sistemas de tecnologia da informação em uso e aos servidores;
c) Todo tipo de acesso aos dados e informações da Gestora, em especial as Informações Sigilosas, que não for expressamente autorizado é proibido;
d) Assuntos relacionados ao desempenho de atividades e funções na Gestora não devem ser discutidos em ambientes públicos ou em áreas expostas (e.g. meios de transporte, locais públicos, encontros sociais);

e) As senhas de acesso do Colaborador aos sistemas da Gestora são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive a outros Colaboradores), anotadas em papel ou em sistema visível ou de acesso não protegido;

f) Os Colaboradores devem bloquear seus computadores sempre que se ausentarem de suas estações de trabalho;

g) A instalação de *softwares* para uso dos Colaboradores nas estações de trabalho deve ser feita pela equipe de serviços de informática da Gestora, no caso a empresa Endev, pelo Diretor de Gestão de Riscos e de *Compliance* ou por Colaborador com autorização para esta finalidade;

h) Arquivos eletrônicos de origem desconhecida não devem ser abertos e/ou executados nos computadores da Gestora;

i) Mensagens eletrônicas e seus anexos são para uso exclusivo do remetente e destinatário e podem conter Informações Sigilosas. Portanto, não podem ser parcial ou totalmente divulgadas, usadas ou reproduzidas sem o consentimento prévio do remetente ou do autor. Toda e qualquer divulgação, uso e/ou reprodução não expressamente autorizada é proibida;

j) O acesso remoto à rede, às Informações Sigilosas e sistemas da Gestora somente será permitida mediante autorização do Diretor de Gestão de Riscos e de *Compliance*, e desde que seja estritamente necessário para o desempenho das funções do Colaborador. O Colaborador será corresponsável pela segurança do acesso remoto aos sistemas e Informações Sigilosas da Gestora;

k) O Colaborador deve evitar realizar acesso remoto à rede da Gestora a partir de um dispositivo público, e, caso o faça, deverá limpar o *cache* e deletar todos os arquivos temporários; e

l) Documentos impressos e arquivos contendo Informações Sigilosas devem ser adequadamente armazenados e protegidos, sendo vedada a retirada da

sede da Gestora sem a autorização prévia do superior hierárquico do Colaborador.

O uso do e-mail corporativo é exclusivo para assuntos relacionados aos negócios conduzidos pela Gestora. Desde que não haja abusos, o eventual uso do e-mail para assuntos particulares é tolerado. É terminantemente proibido o envio de mensagens e arquivos anexos que possam causar constrangimento à terceiros, bem como com conteúdo político, ilegal ou outro que possa colocar a reputação da Gestora em risco.

A Gestora se reserva o direito de monitorar o uso dos dados, informações, serviços, sistemas e demais recursos de tecnologia disponibilizados aos seus Colaboradores, e que os registros e o conteúdo dos arquivos assim obtidos poderão ser utilizados para detecção de violações aos documentos internos da Gestora e, conforme o caso, servir como evidência em processos administrativos, arbitrais ou judiciais.

A Área de Gestão de Riscos e de *Compliance* implantará as medidas necessárias para realizar o monitoramento, bem como para estabelecer as permissões de acesso aos documentos e arquivos da Gestora. Nesse sentido, o monitoramento poderá ser realizado pela Área de Gestão de Riscos e de *Compliance* mediante:

a) Gravação dos ramais telefônicos internos;
b) Gravação em vídeo do ambiente da sede da Gestora;
c) Registro de mensagens de e-mail;
d) Registro de acesso à Internet;
e) Registro de acesso à rede interna;
f) Registro de acesso à documentos e arquivos; e
g) Outros tipos de gravação e registro implantados pela Gestora.

Esse monitoramento poderá ser realizado automaticamente (*software* e/ou *hardware*), pela Área de Gestão de Riscos e de Compliance e/ou por prestador de serviços externo. Apenas a Área de Gestão de Riscos e de *Compliance* poderá acessar os arquivos contendo as gravações e registros do monitoramento realizado, bem como, mediante autorização prévia do Diretor Responsável, o Diretor de Gestão de Riscos e de *Compliance* poderá contratar prestadores de serviços externos para realizar o monitoramento.

O acesso será realizado aleatoriamente, de maneira inopinada e sem periodicidade definida. Os documentos, dados e informações encaminhados pelos prestadores de serviços serão para uso exclusivo do Diretor de Gestão de Riscos e de *Compliance*.

Sempre que necessário será lavrado termo de monitoramento e acesso aos arquivos contendo registros e gravações.

8.2 Gestão de Acesso a Sistemas de Informação e a Outros Ambientes Lógicos

O uso das Informações Sigilosas e dos recursos de tecnologia disponibilizados pela Gestora são monitorados, e os registros decorrentes do uso poderão ser utilizados para verificação e evidência da adequação das regras desta Política, e demais regras internas da Gestora, através de monitoramento a ser efetuado pela Área de Gestão de Riscos e de *Compliance*.

Todo acesso às Informações Sigilosas, aos ambientes lógicos e à sede da Gestora deve ser controlado, de forma a garantir acesso apenas às pessoas expressamente autorizadas pela Área de Gestão de Riscos e de *Compliance*.

O controle de acesso deve ser documentado e formalizado, contemplando os seguintes itens:

a) Pedido formal de concessão e cancelamento de autorização de acesso do usuário aos sistemas;
b) Utilização de identificador do Colaborador (ID de Colaborador) individualizado, de forma a assegurar a responsabilidade de cada Colaborador por suas ações e omissões;
c) Verificação se o nível de acesso concedido é apropriado ao perfil do Colaborador e se é consistente com a Política de Segregação das Atividades;
d) Remoção imediata de autorizações dadas aos Colaboradores afastados ou desligados da Gestora, ou que tenham mudado de função, se for o caso; e
e) Revisão periódica das autorizações concedidas.

8.3 Utilização da Internet

O uso da Internet deve ser predominantemente voltado às atividades relacionadas aos negócios e serviços da Gestora, e para a obtenção de informações e dados necessários ao desempenho dos trabalhos. A Internet pode ser eventualmente utilizada para fins pessoais com moderação desde que não prejudique as atividades dos Colaboradores na Gestora, ou coloque esta em risco.

8.4 Sites na Internet

O acesso à sites externos na Internet é monitorado. Os arquivos contendo os registros das tentativas de acesso e dos acessos são armazenados nos servidores da Gestora.

É expressamente proibido acessar sites na Internet com conteúdo impróprio ao ambiente de trabalho.

Adicionalmente, a Área de Gestão de Riscos e de *Compliance* poderá ser informada sobre acessos e tentativas de acesso à determinados sites.

8.5 Ramais Telefônicos

Os ramais telefônicos utilizados na sede da Gestora pelos Colaboradores da Área de Gestão e da Área Comercial são gravados, e o conteúdo das conversas são armazenados em arquivos nos servidores da Gestora. Conforme já esclarecido anteriormente, a Área de Gestão de Riscos e de *Compliance* possui livre acesso as gravações com o propósito de verificação de conteúdo.

Ao término da verificação, a Área de Gestão de Riscos e de *Compliance* emitirá termo de monitoramento, nos termos do Anexo I, informando o arquivo acessado, a data do acesso e se foram identificados indícios eventual infração ao disposto nesta Política, e nos demais documentos internos da Gestora.

8.6 Telefones Celulares

Os Colaboradores deverão evitar utilizar telefones celulares durante o horário de expediente enquanto estiverem na sede da Gestora. Os aparelhos deverão ser mantidos no modo “silencioso” e somente poderão ser atendidas ligações de reconhecida importância.

8.7 Mensagens Instantâneas

A comunicação por mensagens instantâneas de texto e voz pela Internet para assuntos particulares deve ser evitada durante o horário de expediente, enquanto os Colaboradores estiverem na sede da Gestora, mas não está proibida. Por outro lado, a comunicação por mensagens instantâneas de texto e voz pela Internet para assuntos relacionados com as atividades da Gestora está permitida. Em caso de necessidade, os Colaboradores devem

permitir o acesso a todas as mensagens instantâneas com o propósito de avaliar eventuais infrações ao disposto nos documentos internos.

8.8 Utilização e Conexão de Equipamentos

Somente é permitido o uso de equipamentos homologados e devidamente contratados pela Gestora.

A utilização de equipamentos pessoais por terceiros nas instalações da Gestora e a conexão destes na rede interna e à Internet requer autorização prévia e expressa da Área de Gestão de Riscos e de *Compliance*. Os Colaboradores estão autorizados à conectar seus telefones celulares e computadores pessoais diretamente à rede interna e à Internet, desde que utilizem suas credenciais de acesso.

A conexão de dispositivos móveis de armazenamento (e.g. USB Drive) é bloqueada e somente poderá ser realizada mediante autorização prévia e expressa da Área de Gestão de Riscos e de *Compliance.*

8.9 Acesso de Terceiros

O acesso de terceiros aos arquivos e sistemas da Gestora será possível, na forma definida pelo Diretor de Gestão de Riscos e de *Compliance*, mas deve sempre ser precedido da assinatura de um contrato de confidencialidade que estabeleça penalidade no caso de infração. Ademais, o terceiro deverá garantir à Gestora, ainda que contratualmente, de que possui os controles necessários à boa guarda e proteção das informações aos quais terá acesso.

9 Proteção de Dados Pessoais

9.1 Escopo e Abrangência:

A ADAM|Capital está comprometida em preservar a privacidade de dados pessoais e de dados sensíveis[1] que forem coletados ou aos quais tiver acesso em função do uso do site ou por conta do desempenho de suas atividades, e com o cumprimento das leis e regulamentos em vigor, em especial da Lei Federal n. 13.709/2018 ("LGDP") e da (Lei Federal n. 12.965/2014 ("Marco Civil da Internet") e o Decreto 8.771/2016, que regulamentou o o Marco Civil da Internet, dentre outros normas que possam ser aplicáveis.

Por conta disso, estabeleceu, as diretrizes, princípios e regras previstas nesta Política, as quais servirão de guia para a coleta, registro, processamento, armazenamento, uso, compartilhamento e eliminação de dados pessoais, fornecendo o arcabouço para o correto tratamento e proteção dos dados pessoais em seu poder.

Essas diretrizes, princípios e regras se aplicam a todos os Colaboradores da Gestora, e englobam os dados pessoais que se encontrem armazenados em qualquer meio, e abrangem toda e qualquer forma de tratamento que possa ser empregada e esteja disponível para a Gestora.

Faz-se necessário, entretanto, informar, tal como foi feito em outros documentos, que a Gestora não realiza a distribuição das cotas dos fundos de investimentos para os quais foi contratada para gerir a carteira de títulos e valores mobiliários. A atividade de distribuição é desempenhada por empresas contratadas para esta finalidade.

[1] Dados sensíveis são aqueles sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. O tratamento de dados

Portanto, eventual conhecimento de dados pessoais de cotistas, caso ocorra, será não intencional e, salvo nas hipóteses de adimplemento de obrigações contratuais ou legais, não será por solicitação prévia, e decorrerá de processos e sistemas mantidos pelos administradores dos Fundos, pelos distribuidores contratados ou por outras empresas, os quais estão igualmente obrigados a proteger dados pessoais de seus clientes.

Assim sendo, o escopo da proteção de dados pessoais no âmbito da Gestora está, em grande parte, limitado aos dados pessoais de seus Colaboradores e de pessoas físicas e jurídicas com as quais tiver estabelecido relações jurídicas. Também estão abrangidos por esta proteção os dados de candidatos à vagas na Gestora, de fornecedores e outros com os quais a Gestora manteve contato para atender alguma demanda relevante e específica.

Eventual tratamento de dados pessoais ocorrerá respeitando o disposto no art. 7º, da LGPD, e, quando aplicável, o art. 11º, em especial para obtenção de consentimento do titular, e cumprimento de obrigação legal e regulatória.

9.2 Princípios Norteadores:

A Gestora compromete-se a obter dados pessoais de maneira justa e legal, e suas ações serão norteadas no princípio da boa fé e nos princípios abaixo, os quais estão elecandos no art. 6º da Lei 13.709/2018:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

sensíveis somente ocorrerá nas hipóteses previstas no art. 11º, da LGPD.

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

9.3 Direitos:

Em respeito aos direitos fundamentais de liberdade, de intimidade e de privacidade, e, ainda, ao disposto no art. 18º, da Lei 13.709/2018, o titular dos dados pessoais tem direito de solicitar à Gestora, em relação aos seus dados, a qualquer momento e mediante requerimento expresso. Esses direitos estão exemplificados abaixo, todavia o seu exercício em face da Gestora deve ser analisado em cada caso concreto.

a) confirmação de existência de tratamento;
b) acesso aos dados;
c) correção de dados incompletos, inexatos ou desatualizado;
d) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei 13.709/2019;
e) portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
f) eliminação dos dados pessoais tratados com o consentimento do titular, exceto em determinadas situações e respeitados os limites técnicos das atividades, conforme determinado na Lei;
g) informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
h) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e
i) revogação do consentimento, nos termos da Lei.

9.4 Período de Armazenamento dos Dados Pessoais:

Os dados pessoais serão armazenados pela Gestora durante o período de tempo necessário para o atingimento dos objetivos para os quais foram coletados. Porém, este

período poderá ser ampliado para o cumprimento de obrigação legal, regulatória ou contratual.

9.5 Cooperação com Autoridades:

A divulgação de dados pessoais para o cumprimento de lei, determinação judicial, regulatória ou de órgão competente ao qual a Gestora estiver sujeita somente ocorrerá nos estritos termos e nos limites requeridos para o cumprimento da obrigação, sendo que os titulares dos dados, na medida do possível e desde que não configure infração, inadimplemento ou cause prejuízo à Gestora, serão notificados sobre tal divulgação, para que tomem as medidas apropriadas.

Adicionalmente, a Gestora cooperará com a Autoridade Nacional de Proteção de Dados (ANPD) em qualquer problema em relação à proteção de dados e dentro dos limites previstos na Lei e nas demais regulamentações sobre a matéria, porém sem renunciar a quaisquer defesas e/ou recursos disponíveis.

9.6 Governança:

As matérias relacionadas aos dados pessoais, dados sigilosos e ao tratamentos destes serão apresentadas pelo Encarregado pelo Tratamento de Dados Pessoais para deliberação no Comitê de Gestão de Riscos e de *Compliance*.

9.7 Obrigação de Reporte:

Os Colaboradores estão obrigados a comunicar imediatamente ao Encarregado pelo Tratamento de Dados Pessoais sobre toda e qualquer suspeita ou indício de evento que possa ter comprometido os dados pessoais de posse da Gestora para a devida apuração. Caso necessário, o Encarregado pelo Tratamento de Dados Pessoais notificará, em prazo compatível com a severidade do evento, a Autoridade Nacional de Proteção de Dados.

9.8 Registro de Eventos:

Os eventos reportados que tenham sido apurados e tiverem resultado no comprometimento de dados pessoais serão registrados no Relatório de Controles Internos.

9.9 Treinamento:

A Gestora treinará seus Coloboradores sobre a proteção de dados pessoais e de dados sigilosos de acordo com a sua Política de Treinamento e Reciclagem de Colaboradores.

10 Pessoas Responsáveis pelo Cumprimento do Disposto nesta Política

10.1 Responsável pela Política de Segurança das Informações, Proteção de Dados e de Segurança Cibernética:

A responsável pelo cumprimento do disposto nesta Política é a Diretora de Gestão de Riscos e de *Compliance,* a sra. Camila R. V. de Souza.

10.2 Encarregado pelo Tratamento de Dados Pessoais (Data Protection Officer – DPO):

Com o propósito de atender a Lei 13.709/2018 (a "LGPD"), a Gestora determinou que a função de "Encarregado pelo Tratamento de Dados Pessoais", prevista no art. 41 da Lei, será exercida cumulativamente pela Diretora de Gestão de Riscos e de *Compliance*, tendo ela sido indicada para exercê-la. Neste sentido, faz saber que a sra. Camila R. V. de Souzaserá responsável pelas atividades previstas na LGPD e nas demais normas aplicáveis.

11 Endereço Eletrônico

A presente Política está disponível no endereço eletrônico da Gestora: http://www.adamcapital.com.br/.

Eventuais comunicações para a Área de Gestão de Riscos e de *Compliance* relacionados com esta Política devem ser enviadas para: compliance@adamcapital.com.br. Entretanto, para assuntos relacionados especificamente ao tratamento de dados pessoais, as comunicações deverão ser enviadas para: dados@adamcapital.com.br.

12 Revisões e Atualizações

Esta Política será revisada ao menos uma vez a cada semestre calendário. Não obstante as revisões estipuladas, poderá ser alterada sem aviso prévio e sem periodicidade definida em razão de circunstâncias que demandem tal providência.

A Área de Gestão de Riscos e de *Compliance* informará oportunamente aos Colaboradores sobre a entrada em vigor de nova versão deste documento e a disponibilizará na página da Gestora na Internet, conforme indicado acima.

13 Disposições Gerais

Não obstante o disposto na presente Política, deverá ser observado o Roteiro para a Realização de Testes para a Verificação de Aderência aos Documentos Internos da Gestora. Esse documento contém os principais aspectos a serem considerados na realização de testes para verificação de aderência da Gestora e de seus Colaboradores aos diversos documentos internos editados pela Gestora.

14 Vigência

Esta Política revoga todas as versões anteriores e passa a vigorar na data de sua aprovação pelo Comitê de Gestão de Riscos e de *Compliance*. Eventual incompatibilidade entre as versões anteriores e a atual versão desta Política, se existirem, serão tratadas caso a caso pela Área de Gestão de Riscos e de *Compliance*.

15 ANEXO I

TERMO DE MONITORAMENTO DE GRAVAÇÕES TELEFÔNICAS

Nesta data, _____, foi acessado o arquivo _____ contendo as gravações telefônicas efetuadas pelo ramal _____ e [não] foram identificados indícios que possam indicar eventual infração ao disposto na Política de Segurança das Informações, Proteção de Dados Pessoais e de Segurança Cibernética e nas demais políticas internas da ADAM|Capital Gestão de Recursos Ltda.

[Data]

[Assinatura]

16 ANEXO II

TERMO DE ADESÃO DE TERCEIRO À POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES, DE PROTEÇÃO DE DADOS PESSOAIS E DE SEGURANÇA CIBERNÉTICA

Nesta data, eu, _____, inscrito no CPF/MF sob o nº _____ , declaro que li e estou plenamente de acordo com as disposições da Política de Segurança das Informações, de Proteção de Dados Pessoais e de Segurança Cibernética aprovados pela ADAM|Capital em [inserir data]. Comprometo-me a cumprir com os termos dispostos na mesma, preservando a confidencialidade das informações as quais terei acesso.

Rio de Janeiro, [Data]

[Assinatura]