POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA E PROTEÇÃO DE DADOS

Versão	Atualizada em	Responsável:
3	Setembro/2024	Isabela Amoroso Lima Scuracchio

Sumário

1. APLICABILIDADE

Essa política aplica-se a todos os Colaboradores, prestadores de serviços, que em razão de suas atividades e funções que precisam ter controle sobre as informações a que tenham acesso, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da Gestora, ou que acesse informações a ela pertencentes. Todo e qualquer usuário de recursos computadorizados da nossa instituição tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

2. OBJETIVO

A Política de Segurança da Informação, Cibernética e Proteção de Dados, da Sonata Gestora de Recursos Ltrda. ("Gestora"), estabelece os mecanismos de segurança da informação e segurança cibernética com a finalidade de assegurar a confidencialidade, a integridade, disponibilidade, legalidade, autenticidade e auditabilidade dos dados e dos sistemas de informação utilizados, bem como visa o processo de preservação e legalidade das informações.

Esta Política tem por objetivo contribuir para o aprimoramento da segurança, tanto informacional quanto cibernética da Gestora, estabelecendo medidas a serem tomadas para identificar e prevenir contingências que possam causar prejuízo para as atividades da Gestora.

Em atenção aos dispositivos da Resolução CVM nº 21/21, do Código ANBIMA de Administração e Gestão de Recursos de Terceiros, do Guia ANBIMA de Cibersegurança e da Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709/2018, a Gestora elaborou a presente Política e procurou identificar os eventos com maior possibilidade de ocorrência, bem como as informações de maior sensibilidade ("Informações Confidenciais e Informações Privilegiadas"), com o propósito de mitigar os riscos à sua atividade.

3. PREMISSAS E DEFINIÇÕES

Adiante, a Gestora abordará os principais mecanismos e procedimentos de prevenção as ameaças ao patrimônio, à imagem e, principalmente, aos negócios da Gestora.

Todas as diretrizes aqui dispostas são de responsabilidade da Área de Compliance da Gestora, sob a direção do Comitê de Risco e Compliance da Gestora.

Ademais, para implementação e monitoramento contínuo da presente Política, a Gestora conta com o suporte e assessoria da empresa terceirizada de tecnologia da informação (área de TI).

4. PROGRAMA DE SEGURANÇA DA GESTORA

4.1 Princípios De Segurança Da Informação

A Gestora entende como segurança da informação todas as regras, os direitos e deveres de todos os colaboradores e terceiros contratados, visando à proteção adequada dos que compartilham a informação.

Toda a informação coletada, gerada ou desenvolvida por qualquer colaborador e terceiro contratado

constitui como ativo e propriedade intelectual da Gestora. Independente da forma apresentada, compartilhada ou armazenada, todas as informações devem ser utilizadas para uma finalidade específica e justificável, coberta pelos princípios da segurança da informação, tais como, confidencialidade, integridade, disponibilidade, legalidade, autenticidade e auditabilidade, com o propósito de reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas que possam comprometer esses princípios básicos.

As informações podem ser apresentadas nas mais distintas formas escritas, faladas, transmitidas, digitadas, armazenadas ou processadas em qualquer equipamento, papel, telefone, programa de computador, base de dados ou outro meio existente.

Seja qual for o estado ou o meio do qual a informação seja apresentada ou compartilhada, ela deverá estar sempre protegida adequadamente, de acordo com as normas definidas nesta política.

4.2 Princípios de Segurança Cibernética e Identificação de Riscos

Os avanços tecnológicos criam facilidades e possibilitam o uso de novas ferramentas para a atuação das instituições, permitindo agilidade na construção e disponibilização de serviços, aplicação dos meios de comunicação, entre outros avanços. Por outro lado, o aumento do uso de tais ferramentas potencializa o vazamento de informações e os riscos de ataques cibernéticos, ameaçando a confidencialidade, a integralidade e a disponibilidade dos dados e/ou dos sistemas das instituições.

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

Diante desse cenário, os métodos mais comuns de ataques cibernéticos são os seguintes:

- *Malware* – softwares desenvolvidos para corromper computadores e redes:
  - Vírus: software que causa danos a máquina, rede, softwares e banco de dados;
  - Cavalo de Troia: aparece dentro de outro software e cria uma porta para a invasão do computador;
  - *Spyware*: software malicioso para coletar e monitorar o uso de informações; e
  - *Ransomware*: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

- Engenharia Social – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:
  - *Pharming*: direciona o usuário para um site fraudulento, sem o seu conhecimento;
  - *Phishing*: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
  - *Vishing*: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;

  - *Smishing*: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;
  - Acesso pessoal; pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

- Ataques de DDoS (*distributed denial of services*) e botnets - ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos botnets, o ataque vem de um grande número de computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.
- Invasões (*advanced persistent threats*) - ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Ainda, além de ataques cibernéticos, a Gestora pode estar sujeita a mal funcionalidades dos sistemas utilizados e a atos/omissões de seus Colaboradores, que podem acarretar no perdimento e/ou adulteração de dados e Informações Confidenciais.

Não se imitando aos riscos citados acima, a Gestora relaciona todos os processos e ativos relevantes, em seu processo de avaliação de riscos, incluindo equipamentos, sistemas e dados, necessários ao adequado funcionamento das atividades exercidas pela Gestora, de modo a identificar suas vulnerabilidades e possíveis cenários de ameaça.

Os possíveis impactos dependem ainda da rápida detecção e resposta após a identificação do ataque. Uma vez definidos os riscos, ações de prevenção e proteção deverão ser tomadas de acordo com esta política e conforme orientação do Diretor de Compliance da Gestora.

A avaliação dos riscos e as ações de prevenção inerentes às atividades desempenhadas pela Gestora estão descritas no Anexo II da presente Política.

4.3 Classificação da Informação

As informações são classificadas de maneira a serem adequadamente protegidas quanto ao seu acesso e uso, sendo que, para aquelas consideradas de alta criticidade, são necessárias medidas especiais de tratamento. A classificação das informações deverá seguir a seguinte ordem:

- **Pública**: É uma informação da Gestora ou de seus clientes com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade.

- **Interna:** É uma informação da Gestora que ela não tem interesse em divulgar, onde o acesso por parte de indivíduos externos à empresa deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem da organização, porém, não com a mesma magnitude de uma informação confidencial. Pode ser acessada sem restrições por todos os empregados e terceiros contratados da Gestora.

- **Confidencial:** É uma informação crítica para os negócios da Gestora ou de seus clientes. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais à Gestora ou aos seus clientes. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por empregados, clientes e/ou fornecedores.

- **Privilegiada:** É a informação relevante ainda não divulgada publicamente e que seja obtida de forma privilegiada (em decorrência da relação profissional ou pessoal mantida com um cliente, com pessoas vinculadas a empresas analisadas ou investidas ou com terceiros). As informações privilegiadas devem ser mantidas em sigilo por todos que a elas tiverem acesso, seja em decorrência do exercício da atividade profissional ou de relacionamento pessoal.

- **Restrita:** É toda informação que pode ser acessada somente por usuários da Gestora explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

Nenhuma informação interna, confidencial, privilegiada e restrita pode ou deve ser discutida por qualquer colaborador ou terceiro contratado pela Gestora, em locais inapropriados, como lugares públicos ou fechados, na presença de terceiros ou pessoas não diretamente relacionadas ao assunto, ou adiante daqueles sem autorização para conhecimento dessas informações. Há impacto negativo e relevante na situação de vazamento desse tipo de informação.

Qualquer informação sobre a Gestora, ou de qualquer natureza relativa às atividades da Gestora e aos sócios, obtida em decorrência do desempenho das atividades normais dos Colaboradores, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado pela Diretoria de Compliance.

A gestão dessas informações é realizada através de um processo de melhoria contínua, partindo dos seguintes mecanismos de supervisão:

- Classificação de informações: conforme mencionado no acima o acesso é restringido e são reforçados os mecanismos de controle e segurança de acordo com a criticidade e sensibilidade de cada dado;

- Equipamentos e Estrutura: Os equipamentos utilizados para o desenvolvimento das atividades da Gestora devem estar sempre atualizados, regra que inclui sistema operacional, antivírus e firewalls, garantindo assim maior proteção às informações neles inseridas. Ainda os cuidados se estendem também à infraestrutura onde são armazenados os dados: que possuem cópias de segurança (backups) atualizadas periodicamente;

- Armazenamento de Dados e Computação em Nuvem: Os serviços de armazenamento de dados e computação em nuvem que contratamos passam por uma seleção interna rígida que avalia a necessidade da terceirização do serviço em questão e a confiabilidade técnica do fornecedor analisado, a fim de garantir que ele possua as qualificações de segurança necessárias;

- Gerenciamento de Acesso: Os acessos dados são restringidos a menor permissão e privilégio possíveis, possuindo a Gestora a capacidade para monitorar e registrar o acesso a dados classificados como sensíveis, sendo exigida a mesma garantia de seus colaboradores e terceiros contratados, conforme Lei Geral de Proteção de Dados (Lei nº 13.709); e

- Capacitação e Atualização: Os colaboradores e os terceiros contratados passam por treinamentos periódicos referentes à prevenção e resposta à incidentes, bem como de melhores práticas de segurança da informação e cibernética, sendo realizadas ainda, avaliações buscando atingir o maior comprometimento de todos os nossos colaboradores.

4.4 Ações de Prevenção e Proteção

Para que se possam prevenir eventuais ataques cibernéticos e vazamento de informações, primeiro deve-se definir quais informações são as de maior sensibilidade para Gestora, assim como aquelas que teriam o maior impacto financeiro, operacional e reputacional para Gestora, em caso de incidente de segurança.

Deste modo, a Gestora segrega as informações geradas pela Gestora, aperfeiçoando a implementação de processos e o devido manuseio, armazenamento, transporte e descarte destas informações.

Através da definição acima, a Gestora se empenhará para manter controles, conforme o nível de criticidade das informações e dados, sendo certo de que a prioridade será escalonada na seguinte ordem de relevância: Red Flag, Yellow Flag e Green Flag.

A partir desse ponto, passamos a mencionar os procedimentos de prevenção e proteção adotados pela Gestora:

4.5 Estrutura de TI

Até de forma a estabelecer os principais equipamentos, procedimentos e sistemas de Tecnologia da Informação da Gestora, segue lista exemplificativa dos recursos da Gestora:

- Backup diário local e externo;
- Computadores corporativos com acesso à nuvem, todos com extensão de garantia de hardware;
- Acesso ao sistema de informações de posição dos fundos e gerenciamento de riscos;
- Sistema de Firewall redundante com sistema de detecção de intrusos e bloqueio automático com acesso auditados – Nuvem corporativa com acessos auditados;
- Switches Giga com telefonia IP (PoE) e a rede local (Giga Ethernet);
- Sistema de correio eletrônico com anti spam e recursos de regras para controle de envio de e-mails;
- Nobreak com gerenciamento, para prevenção de surtos elétricos e estabilização elétrica de todas as tomadas dos equipamentos sensíveis da empresa, como os ativos de TI e mesa de operação;
-

- Sistema de Proxy com regras de conteúdo de acesso às páginas da internet;
- Utilização de questionário de diligência para contratação de serviço de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior, disponibilizado no site da ANBIMA, quando aplicável.

Todos os Colaboradores, ao tomarem conhecimento de qualquer incidente referente à segurança da informação e cibernética, devem notificar o fato, imediatamente à área de Compliance.

4.6 Disponibilização e uso

Todos os computadores disponibilizados para os Colaboradores da Gestora têm por objetivo o desempenho das atividades profissionais na gestora, não devendo ser utilizado para quaisquer outros fins.

Todo o processo de criação e exclusão de usuário, instalação de softwares e aplicativos, permissão de acesso, entre outras funcionalidades informáticas, são realizados pela área de TI, mediante aprovação do processo pela Área de Compliance.

A disponibilização e uso dos computadores da Gestora respeitam as seguintes regras:

- A cada novo Colaborador, a área de *Compliance* autorizará, mediante solicitação, a criação de novo usuário e a disponibilização técnica de recursos;
- Todos os equipamentos devem ser preparados e testados pela área de TI, mediante supervisão e aprovação da Área de *Compliance*.
- A Área de *Compliance* autorizará, mediante solicitação, a retirada ou substituição do computador disponibilizado para o usuário;
- Cada computador tem o seu usuário gestor, que é responsável por esse equipamento. O controle das máquinas é de responsabilidade da área de TI, mediante supervisão e aprovação da Área de *Compliance*.
- A identificação do usuário é feita através do login e senha, que através do registro de logs utilizado pela Gestora é sua assinatura eletrônica no servidor da Gestora.
- Será apenas permitida senhas com no mínimo 08 (oito) caracteres alfanuméricos, maiúsculos e minúsculos. A reutilização de senhas obedecerá ao ciclo mínimo de 05 (cinco) vezes.
- Não será permitida a utilização da mesma senha para projetos e serviços diferentes realizados pela Gestora, não devendo ser criada uma senha única padrão para todos os serviços e áreas em que um mesmo Colaborador atue.
- É permitido apenas 3 tentativas máximas de autenticação de senha, sendo todas malsucedidas, será bloqueado o acesso, o qual apenas poderá ser reestabelecido através de solicitação a área de *Compliance*.
- A senha possui validade de 180 (cento e oitenta) dias e sua troca será solicitada automaticamente quando da expiração da mesma.
- Todos os eventos de login e alteração de senhas são auditáveis e rastreáveis, podendo ser solicitados pela área de *Compliance* à área de TI.

4.7 Softwares

A implantação e configuração de softwares da Gestora respeitam as seguintes regras:

- Todos os softwares, programas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados pela área de TI, mediante supervisão e aprovação da Área de *Compliance.*
- É desabilitado aos usuários implantar novos programas ou alterar configurações sem a permissão formalizada da Área de *Compliance*.
- É desabilitado ao usuário implantar ou alterar componentes físicos em seus computadores.
- 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 à Internet requer autorização prévia e expressa da Área de *Compliance*. Os Colaboradores estão autorizados a 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) somente poderá ser realizada mediante autorização prévia e expressa da Área de *Compliance*.

4.8 Registros

A Gestora mantém por 05 (cinco) anos todos os logs de sistemas, e verifica regularmente, quaisquer desvios de padrão de todos os computadores, arquivos em rede, sejam softwares, hardwares ou acessos que não sejam autorizados.

Nesse sentido, através dos logs realizados pela gestora, a Gestora consegue manter a integridade, autenticidade e auditabilidade das informações e sistemas, conforme previstos na Resolução CVM nº21/21.

4.9 Responsabilidades do usuário

O Colaborador é o custodiante dos recursos disponibilizados a ele, devendo este cuidar adequadamente do equipamento.

O Colaborador também deve garantir a sua integridade física e o seu perfeito funcionamento, seguindo as regras e orientações fornecidas pela Gestora.

Ainda, o Colaborador deve adotar um comportamento seguro condizente com a Política, devendo:

- Não compartilhar nem divulgar sua senha a terceiros;
- Não transportar Informações Confidenciais da Gestora em qualquer meio (CD, DVD, *pendrive*, papel, etc.) sem as devidas autorizações e proteções;
- Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais, etc.);
- Não abrir mensagens de origem desconhecida, ou links suspeitos mesmo que advindos de origem conhecida;
- Armazenar e proteger adequadamente documentos impressos e arquivos

eletrônicos que contêm Informações Confidenciais; e

- Seguir corretamente as políticas para uso de internet e correio eletrônico estabelecidas conforme disposto na presente Política.

4.10 Outras Proteções aos Computadores

- Proteção de tela no computador e/ou proteção de ausência (após um tempo de inatividade, o computador bloqueia o sistema, exigindo senha para ser usado novamente).
- Bloqueio de sistemas de gerenciamento de computador à distância.

4.11 Regras e responsabilidades do uso da Internet

O Colaborador é responsável por todo acesso realizado com a sua autenticação.

Quando o usuário se comunicar através de recursos de tecnologia da Gestora, este deve sempre resguardar a imagem da Gestora, evitando entrar em sites de fontes não seguras, ou, de fontes não conhecidas, salvo quando comunicado e devidamente autorizado pela Área de Compliance.

O usuário é proibido de acessar endereços de internet (sites) que:

- Possam violar direitos de autor, marcas, licenças de programas (softwares) ou patentes existentes.
- Possuam conteúdo pornográfico, relacionado a sexo, exploração infantil ou ao crime de pedofilia.
- Defendam atividades ilegais, menosprezem, depreciem ou incitem o preconceito a determinadas classes como sexo, raça, orientação sexual, religião, nacionalidade, local de nascimento ou deficiência física.
- Possuam origem suspeita ou que não se atenham aos padrões de segurança adequados, assim como possuírem links suspeitos.

O usuário deve garantir que está cumprindo a legislação em relação ao direito autoral, licença de uso e patentes existentes e que o uso do material foi autorizado, no mínimo, pelo gestor da sua área.

4.12 Bloqueio de endereços de Internet

Periodicamente, a Área de *Compliance* irá revisar e bloquear o acesso para os endereços da Internet que não estejam alinhados com esta Política e com o Código de Ética da Gestora.

4.13 Uso de correio eletrônico particular

É proibida a utilização profissional de correio eletrônico particular, a não ser em situação de contingência com a devida autorização da área de Compliance.

A Gestora disponibiliza endereços de seu correio eletrônico para utilização do usuário no desempenho de suas funções profissionais (ex.: usuario@sonatainvest.com.br). O endereço eletrônico disponibilizado

para o usuário é individual, intransferível e pertence à Gestora. Esse endereço não deve ser usado em hipótese alguma para fins particulares.

O endereço eletrônico cedido para o usuário deve ser o mesmo durante todo o seu período de vínculo com a Gestora.

Se houver necessidade de troca de endereço, a alteração será realizada pela área de TI, mediante autorização e supervisão da Área de Compliance.

4.14 Endereço eletrônico de programas ou de comunicação corporativa

É permitido que um programa aplicativo ou um programa de sistema possua um endereço de correio eletrônico. Nesse caso, é obrigatória a existência de um usuário responsável por acompanhar as mensagens emitidas e recebidas por esse endereço.

É permitida a existência de endereços de correio eletrônico para o envio de mensagens tipo comunicação interna da Gestora.

O endereço de correio eletrônico disponibilizado para os Colaboradores e as mensagens associadas a esse correio eletrônico são de propriedade da Gestora.

4.15 Acesso à distância ao e-mail

O usuário pode acessar o seu correio eletrônico cedido pela Gestora mesmo quando estiver fora do ambiente da empresa, através do serviço de correio eletrônico via Internet.

O Colaborador deve ter o mesmo zelo com a utilização do correio eletrônico à distância tal qual estivesse no ambiente físico da Gestora.

4.16 Responsabilidades e forma de uso de Correio Eletrônico

O Colaborador que utiliza um endereço de correio eletrônico é responsável por todo acesso, conteúdo de mensagens e uso relativos ao seu e-mail.

É proibido criar, copiar ou encaminhar mensagens ou imagens que:

- Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;
- Façam parte de correntes de mensagens, independentemente de serem legais ou ilegais;
- Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física;
- Possuam informação pornográfica, obscena ou imprópria para um ambiente profissional;
- Sejam susceptíveis de causar qualquer tipo de prejuízo a terceiros;
- Defendam ou possibilitem a realização de atividades ilegais;

- Sejam ou sugiram a formação ou divulgação de correntes de mensagens;
- Possam prejudicar a imagem da Gestora; e
- Sejam incoerentes com o Código de Ética da Gestora.

É proibido reproduzir qualquer material recebido pelo correio eletrônico ou outro meio, que possa infringir direitos de autor, marca, licença de uso de programas ou patentes existentes, sem que haja autorização expressa do autor do trabalho e da organização.

O Colaborador deve estar ciente que uma mensagem de correio eletrônico da Gestora é um documento formal e, portanto, possui as mesmas responsabilidades de um documento convencional em papel timbrado da entidade.

Exceto quando especificamente autorizado para tal, é proibido emitir opinião pessoal, colocando-a em nome da Gestora.

Deve observar se o endereço do destinatário corresponde realmente ao destinatário desejado. O Colaborador deve ser diligente em relação:

- Aos usuários que receberão a mensagem (Destinatário/ To, Copiado/Cc e Copiado Oculto/Bcc);
- Ao nível de sigilo da informação contida na mensagem;
- Aos anexos da mensagem, enviando os arquivos apenas quando for imprescindível e garantindo a confidencialidade dos mesmos;
- Ao uso da opção Encaminhar (*Forward*), verificando se é necessária a manutenção das diversas mensagens anteriores que estão encadeadas.

O Colaborador deve deixar mensagem de ausência quando for passar um período maior do que 24 (vinte e quatro) horas sem acessar seu correio eletrônico. Essa mensagem deve indicar o período de ausência e o endereço do substituto para quem deve ser enviada a mensagem.

4.17 Cópias de segurança do Correio Eletrônico

Para que seja possível uma gestão segura, efetiva, confiável, administrável e passível de auditoria o e-mail corporativo da Gestora fica na nuvem contratado junto a um reconhecido provedor desse tipo de serviço, qual seja, o Google Drive fornecido pelo Google.

4.18 Armazenamento em Nuvem (Cloud)

A Gestora realizará o armazenamento das Informações Confidenciais e quaisquer outros dados na Nuvem (Cloud).

De forma a possuir um ambiente seguro de nuvem, considerando aplicações WEB, se prezará pela confiabilidade, disponibilidade e integridade do armazenamento da mesma.

4.19 Contratação de Terceiros para Serviços de Armazenamento na Nuvem

Fornecedores, prestadores de serviços e parceiros (“Terceiros”) podem representar uma fonte

significativa de riscos para a Gestora em relação à Cibersegurança. Neste sentido, a Gestora só poderá contratar serviços de nuvem de grandes empresas de tecnologia que devem ter os seus papéis listados em bolsa de valores e valor de mercado acima de R$100.000.000,00. Nesse sentido, a Gestora assegura a verificação da capacidade do potencial prestador de serviço de contratação de serviços de processamento e armazenamento de dados em nuvem, conforme definidos no Regras de Procedimentos de Deveres Básicos da ANBIMA, sendo verificado no minimo:

(i) O acesso da Gestora aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;
(ii) A confidencialidade, a integridade, a disponibilidade e a recuperação das informações e dados processados ou armazenados pelo prestador de serviço;
(iii) A sua aderência a cerificações exigidas pela Gestora ou reguladores para a prestação do serviço a ser contratado, caso aplicável;
(iv) O provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
(v) A identificação e a segregação dos dados dos clientes, funcionários, colaboradores ou terceiros relevantes por meio de controles físicos ou lógicos;
(vi) A qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes, funcionários, colaboradores e terceiros relevantes.

Outros serviços com utilização da tecnologia em Nuvem também devem ser considerados para fins das regras aqui presentes, sendo necessário aplicar os mesmos procedimentos aos provedores destes serviços, tal como, porém, não exclusivamente:

(i) *Software as a Service* (SaaS) – utilização do software do provedor por meio de subscrição, eliminando a necessidade de instalação e execução nos computadores;
(ii) *Platform as a Service* (PaaS) – desenvolvimento, teste, uso e controle sobre softwares próprios; e
(iii) *Infrastructure as a Service* (IaaS) – utilização e controles sobre softwares próprios e de terceiros, sistemas operacionais, servidores, unidades de armazenamento e rede – contratação de servidores virtuais.

Por fim, a Gestora pode deixar de realizar os procedimentos aqui dispostos, desde que respeitada a previsão da Política de Seleção, Contratação e Monitoramento de Terceiros. Adicionalmente, a Gestora poderá utilizar o questionário de due diligence para contratação de serviço de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior, disponibilizado no site da ANBIMA.

5. MONITORAMENTO E TESTES DE CONTINGÊNCIA

O monitoramento dos controles existentes e estabelecidos nessa Política serão realizados e executados por empresa de tecnologia terceirizada (área de TI), sob supervisão da Área de Compliance. O referido

monitoramento acontecerá de forma contínua, sem periodicidade.

Os Testes de Contingência serão realizados anualmente, de modo a permitir que a Gestora esteja preparada para a continuação de suas atividades, assim como a mitigar eventuais riscos operacionais ou reputacionais. Outras informações acerca dos Testes de Contingência estão no Plano de Continuidade de Negócios da Gestora. O documento Plano de Continuidade de Negócios possui maior detalhamento sobre o tema abordado.

6. PLANO DE RESPOSTA

Conforme as melhores práticas de mercado, a Gestora desenvolveu um Plano de Resposta para indícios, suspeita fundamentada, vazamento de Informações Confidenciais ou outra falha de segurança.

Na hipótese de verificação de uma das hipóteses acima, inclusive em decorrência da ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas, devendo cada área responsável agir conforme o disposto na presente Política. Estas providências consistem em:

Empresa de TI Terceirizada – Área de TI (Sob Supervisão do *Compliance*):

a) Verificação e Auditoria dos Logs;
b) Elaboração de relatórios internos, contendo as informações que foram potencialmente vazadas;
c) Execução de aplicativos externamente ou em sistemas afetados para eliminar aplicativos indesejados;
d) Desinstalação de software;
e) Execução de varreduras *offline* para descobrir quaisquer ameaças adicionais;
f) Formatação e reconstrução do sistema operacional;
g) Substituição física de dispositivos de armazenamento
h) Reconstrução de sistemas e redes;
i) Restauração de dados provenientes do backup realizado diariamente;
j) Entre outros.

Compliance:

a) Criação de relatório baseado no laudo pericial elaborado pela Empresa de TI Terceirizada, de forma a constar eventuais consequências reputacionais e jurídicas derivadas dos danos ocasionados pelo incidente de segurança;
b) Em caso de confirmação do incidente de segurança e eventual vazamento de informações confidenciais, elaborar notificação aos clientes afetados informando o ocorrido.

BackOffice:

a) Análise de dados perdidos e suas influências frente ao planejamento contábil e aos ativos da Gestora.
b) Realizar planejamento de contenção de risco de liquidez frente a possibilidade de resgate de investimentos da Gestora resultantes do incidente de segurança.

Em caso de necessidade, poderá ser contratada empresa especializada no combate ao evento identificado, assim como nas respostas ao eventual dano.

Todo e qualquer incidente ocorrido, assim como os resultados do Plano de Resposta, deverão ser devidamente classificados por nível de severidade, arquivados e documentados pela área de Compliance, bem como ser formalizado no Relatório de Controles Internos da Gestora.

Caso o evento tenha sido causado por algum Colaborador, deverá ser avaliada a sua culpabilidade, nos termos do Código de Ética da Gestora.

7. CONFIDENCIALIDADE

Conforme estabelecido no Termo de Responsabilidade e Confidencialidade constante no Anexo II, nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a terceiros não Colaboradores da Gestora. Fica vedada qualquer divulgação, no âmbito pessoal ou profissional, que não esteja em acordo com as normas legais.

Estão dispensados de assinar o Termo de Confidencialidade os terceiros contratados, que em seu contrato de prestação de serviço haja uma cláusula de confidencialidade.

Qualquer informação sobre a Gestora, seu know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras, estatísticas, logísticas ou relacionadas às estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e/ou dos fundos geridos pela Gestora, operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento geridos pela gestora, estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Gestora e/ou de seus sócios e clientes, obtida em decorrência do desempenho das atividades do Colaborador na, ou para a, Gestora, só poderá ser fornecida a terceiros, ao público em geral, aos meios de comunicação de massa ou demais órgãos públicos ou privados se assim for previamente autorizado pela Diretora de Compliance.

A informação obtida em decorrência da atividade profissional exercida na Gestora não pode ser divulgada, em hipótese alguma, a terceiros não Colaboradores ou a Colaboradores não autorizados. Enquadram-se neste item, por exemplo, posições compradas ou vendidas, estratégias de investimento ou desinvestimento, relatórios, estudos realizados (Research) – independentemente destas análises terem sido realizadas pela Gestora ou por terceiros contratados –, opiniões internas sobre ativos financeiros, informações a respeito de resultados financeiros antes da publicação dos balanços e balancetes do fundos de investimento gerido pela Gestora, transações realizadas e que ainda não tenham sido divulgadas publicamente, além daquelas estabelecidas no Anexo II - Termo de Responsabilidade e Confidencialidade.

Na questão de confidencialidade e tratamento da informação, o Colaborador deve cumprir o estabelecido nos itens a seguir.

- ✓ Informação privilegiada

Considera-se informação privilegiada qualquer informação relevante a respeito de qualquer companhia, que não tenha sido divulgada publicamente e que seja obtida de forma privilegiada (em decorrência da

relação profissional ou pessoal mantida com um cliente, com pessoas vinculadas a empresas analisadas ou investidas ou com terceiros).

Exemplos de informações privilegiadas: 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).

As informações privilegiadas devem ser mantidas em sigilo por todos que a elas tiverem acesso, seja em decorrência do exercício da atividade profissional ou de relacionamento pessoal.

Quem tiver acesso a uma informação privilegiada deverá divulgá-la imediatamente a Diretora de Compliance, não devendo divulgá-la a ninguém mais, nem mesmo a outros integrantes da Gestora, profissionais de mercado, amigos e parentes, e nem a utilizar, seja em benefício próprio ou de terceiros. Caso haja dúvida sobre o caráter privilegiado da informação, aquele que a ela teve acesso deve se abster de utilizar tal informação, seja em benefício próprio, de terceiros ou mesmo da Gestora e de seus clientes, bem como deve imediatamente relatar tal fato a Diretora de Compliance. Todos aqueles que tenham acesso a uma informação privilegiada deverão, ainda, restringir totalmente a circulação de documentos e arquivos que contenham essa informação.

- ✓ *Insider Trading, Divulgação Privilegiada e Front Running*

Insider Trading consiste na compra e venda de títulos ou valores mobiliários com base na utilização de Informação Privilegiada, visando à obtenção de benefício próprio ou de terceiros.
Divulgação Privilegiada é a divulgação, a qualquer terceiro, de Informação Privilegiada que possa ser utilizada com vantagem na compra e venda de títulos ou valores mobiliários.

Front Running é a prática de aproveitar alguma Informação Privilegiada para concluir uma negociação antes de outros.

É vedada a prática de todos os procedimentos acima referidos por qualquer integrante da Gestora, seja atuando em benefício próprio, da Gestora, de seus clientes, ou de terceiros.

Deve ser observado o disposto nos itens de "Informação Privilegiada", "Insider Trading", Divulgação Privilegiada e "Front Running" não só durante a vigência de seu relacionamento profissional com a Gestora, mas mesmo depois do seu término.

A utilização ou divulgação de Informação Privilegiada, "Insider Trading", Divulgação Privilegiada e "Front Running", sujeitará os responsáveis às sanções previstas neste Código, inclusive desligamento ou exclusão por justa causa, no caso de Colaboradores que sejam sócios da Gestora, ou demissão por justa causa, no caso de Colaboradores que sejam empregados da Gestora, e ainda às consequências legais cabíveis.

8. PROTEÇÃO DE DADOS PESSOAIS

8.1 Escopo e Abrangência:

A Gestora está comprometida em preservar a privacidade de dados pessoais e de dados sensíveis 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.

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.

É importante observar que 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 às vagas na Gestora, de fornecedores e outros com os quais a Gestora manteve contato para atender alguma demanda relevante e específica.

Vale ressaltar que todo o tratamento de dados pessoais feito pela Gestora está pautado nos requisitos do artigo 7º da Lei Geral de Proteção de Dados, assim como nas premissas do artigo 11 da mesma Lei, quando aplicável. Dessa maneira, o tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

> I. Quando o titular consentir, de forma específica e clara, para finalidades específicas;
> II. Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
>
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> e) proteção da vida ou da incolumidade física do titular ou de terceiros;
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da Lei Geral de Proteção de Dados e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

8.2 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 elencados 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;

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.

8.3 Direitos:

Em respeito aos direitos fundamentais de liberdade, de intimidade e de privacidade, e, ainda, ao disposto no art. 18, da Lei 13.709/2018, o titular dos dados pessoais pode exercer seus direitos ao solicitar à Gestora, 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 13.709/2018;
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.

A Gestora disponibiliza canal de comunicação, através do endereço clientes@sonatainvest.com.br, por meio do qual o Encarregado pelo Tratamento de Dados Pessoais, receberá quaisquer requisições, solicitações, comunicações e/ou manifestações dos titulares de dados pessoais para exercício dos direitos estipulados na Lei Geral de Proteção de Dados em consonância à sua Política de Privacidade. O Encarregado pelo Tratamento de Dados Pessoais, também conhecido como Data Protection Officer (DPO), é o responsável por auxiliar os controladores de dados pessoais em relação ao cumprimento de suas obrigações legais referentes à privacidade. Dessa forma, o DPO atua como uma ponte entre a Gestora, os titulares dos dados (pessoas físicas) e a Autoridade Nacional de Proteção de Dados (ANPD).

8.4 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.

8.5 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.

8.6 Governança:

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

8.7 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.

8.8 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 e no Relatório de Impacto à Proteção de Dados Pessoais, inclusive de dados sensíveis, nos termos do artigo 38 da Lei Geral de Proteção de Dados.

8.9 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.

9. VIGÊNCIA E ATUALIZAÇÃO

A Gestora manterá o programa de segurança da informação e cibernética será continuamente atualizado, identificando novos riscos, ativos e processos e reavaliando os riscos residuais.

O Diretor de Compliance, responsável pela implementação dos procedimentos de segurança da informação, Segurança cibernética e Proteção de Dados, realizará a revisão e atualização deste plano de segurança da informação e cibernética em prazo não superior a 24 (vinte e quatro) meses, ou em prazo inferior sempre que necessário, ou na ocorrência de algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Diretor de Compliance.

10. DIVULGAÇÃO

A Política de Segurança da Informação e Segurança Cibernética, normas e procedimentos relativos ao tratamento dos ativos de informação e/ou dados sigilosos será divulgada a todos os colaboradores e terceiros contratados com o propósito de desenvolver e manter uma efetiva conscientização de segurança, assim como promover o seu fiel cumprimento. A presente Política será divulgada por intermédio de mensagem eletrônica (e-mail), assim como estará disponível em um diretório interno da Gestora, com total acesso a todos os colaboradores e terceiros contratados.

11. MANUTENÇÃO DOS ARQUIVOS

A Gestora manterá armazenado todos os arquivos eletronicamente, pertinentes ao processo de Compliance desta política, pelo prazo mínimo de 05 (cinco) anos, conforme legislação vigente.

ANEXO I

TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E 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 da Informação e Cibernética aprovados pela Sonata Gestora de Recursos Ltda. em agosto de 20XX. Comprometo-me a cumprir com os termos dispostos na mesma, preservando a confidencialidade das informações as quais terei acesso.

São Paulo, [Data]

_____

[Assinatura]

ANEXO II

TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE

Através deste instrumento eu, , inscrito no CPF sob o no , doravante denominado Colaborador, e Sonata Gestora de Recursos Ltda., inscrita no CNPJ/MF sob o n.º 29.996.127/0001-94. ("Gestora").

Resolvem as partes, para fim de preservação de informações pessoais e profissionais dos clientes e da Gestora, celebrar o presente termo de responsabilidade e confidencialidade ("Termo"), que deve ser regido de acordo com as cláusulas que seguem:

São consideradas informações confidenciais ("Informações Confidenciais"), para os fins deste Termo:

Todo tipo de informação escrita, verbal ou apresentada de modo tangível ou intangível, podendo incluir: know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e dos fundos geridos pela Gestora, operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para o fundo de investimento gerido pela Gestora, estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Gestora e a seus sócios ou clientes, independente destas informações estarem contidas em pen-drives, hds, outros tipos de mídia ou em documentos físicos.

Informações acessadas pelo Colaborador em virtude do desempenho de suas atividades na Gestora, bem como informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, trainees ou estagiários da Gestora e/ou de subsidiárias ou empresas coligadas, afiliadas ou controladas pela Gestora ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

1.1 Não são consideradas Informações Confidenciais:

Quaisquer informações que: (i) já forem de domínio público à época em que tiverem sido obtidas pelo Colaborador; (ii) passarem a ser de domínio público, após o conhecimento pelo Colaborador, sem que a divulgação seja efetuada em violação ao disposto neste Termo; (iii) já forem legalmente do conhecimento do Colaborador antes de lhes terem sido reveladas e este não tenha recebido tais informações em confidencialidade; (iv) forem legalmente reveladas ao Colaborador por terceiros que não as tiverem recebido sob a vigência de uma obrigação de confidencialidade; (v) forem ou sejam divulgadas ou requisitadas por determinação judicial, Poder Público e/ou pela autoridade competente, devendo o Colaborador, neste último caso, informar imediatamente ao Diretor de Compliance da Gestora para que as medidas legais cabíveis

sejam tomadas, observado o disposto no item 5 deste Termo.

O Colaborador compromete-se a utilizar as Informações Confidenciais a que venha a ter acesso estrita e exclusivamente para desempenho de suas atividades na Gestora, comprometendo-se, portanto, observadas as disposições das Políticas da Gestora, a não divulgar tais Informações Confidenciais para quaisquer fins ou pessoas estranhas Gestora, inclusive, nesse último caso, cônjuge, companheiro(a), ascendente, descendente, qualquer pessoa de relacionamento próximo ou dependente financeiro do Colaborador.

O Colaborador se obriga a, durante a vigência deste Termo e por prazo indeterminado após sua rescisão, manter absoluto sigilo pessoal e profissional das Informações Confidenciais a que teve acesso durante o seu período na Gestora.

As obrigações ora assumidas ainda persistirão no caso do Colaborador ser transferido para qualquer subsidiária ou empresa coligada, afiliada, ou controlada pela Gestora.

A não observância da confidencialidade e do sigilo, mesmo após o término da vigência deste Termo, estará sujeita a apuração de responsabilidades nas esferas cível e criminal.

O Colaborador entende que a revelação não autorizada de qualquer Informação Confidencial pode acarretar prejuízos irreparáveis e sem remédio jurídico para a Gestora e terceiros, ficando desde já o Colaborador obrigado a indenizar a Gestora, seus sócios e terceiros prejudicados, nos termos estabelecidos a seguir.

O descumprimento acima estabelecido será considerado ilícito civil e criminal, ensejando inclusive sua classificação como justa causa para efeitos de rescisão de contrato de trabalho, quando aplicável, nos termos do artigo 482 da Consolidação das Leis de Trabalho, e desligamento ou exclusão por justa causa do Colaborador se este for sócio da Gestora, sem prejuízo do direito da Gestora de pleitear indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio das medidas legais cabíveis.

O Colaborador expressamente autoriza Gestora a deduzir de seus rendimentos, sejam eles remuneração, participação nos lucros ou dividendos observados, caso aplicáveis, eventuais limites máximos mensais previstos na legislação em vigor, quaisquer quantias necessárias para indenizar danos por ele dolosamente causados, no ato da não observância da confidencialidade das Informações Confidenciais, nos termos do parágrafo primeiro do artigo 462 da Consolidação das Leis do Trabalho, sem prejuízo do direito da Gestora de exigir do Colaborador o restante da indenização, porventura não coberta pela dedução ora autorizada.

A obrigação de indenização pelo Colaborador em caso de revelação de Informações Confidenciais subsistirá pelo prazo durante o qual o Colaborador for obrigado a manter as Informações Confidenciais, mencionados nos itens 2 e 2.1 acima.

O Colaborador tem ciência de que terá a responsabilidade de provar que a informação divulgada indevidamente não se trata de Informação Confidencial.

O Colaborador reconhece e toma ciência que:

Todos os documentos relacionados direta ou indiretamente com as Informações Confidenciais, inclusive contratos, minutas de contrato, cartas, apresentações a clientes, e-mails e todo tipo de correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, planos de ação, modelos de avaliação, análise, gestão e memorandos por este elaborados ou obtidos em decorrência do desempenho de suas atividades na Gestora são e permanecerão sendo propriedade exclusiva da Gestora e de seus sócios, razão pela qual compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na Gestora, devendo todos os documentos permanecer em poder e sob a custódia da Gestora, salvo se em virtude de interesses da Gestora for necessário que o Colaborador mantenha guarda de tais documentos ou de suas cópias fora das instalações da Gestora;

Em caso de rescisão do contrato individual de trabalho, desligamento ou exclusão do Colaborador, o Colaborador deverá restituir imediatamente à Gestora todos os documentos e cópias que contenham Informações Confidenciais que estejam em seu poder;

Nos termos da Lei 9.609/98, a base de dados, sistemas computadorizados desenvolvidos internamente, modelos computadorizados de análise, avaliação e gestão de qualquer natureza, bem como arquivos eletrônicos, são de propriedade exclusiva da Gestora, sendo terminantemente proibida sua reprodução total ou parcial, por qualquer meio ou processo; sua tradução, adaptação, reordenação ou qualquer outra modificação; a distribuição do original ou cópias da base de dados ou a sua comunicação ao público; a reprodução, a distribuição ou comunicação ao público de informações parciais, dos resultados das operações relacionadas à base de dados ou, ainda, a disseminação de boatos, ficando sujeito, em caso de infração, às penalidades dispostas na referida lei;

É expressamente proibida a instalação pelo Colaborador, de softwares não homologados pela Gestora no equipamento do mesmo; e

A senha que foi fornecida para acesso à rede de dados institucionais é pessoal e intransferível e não deverá, em nenhuma hipótese, ser revelada a outra pessoa.

Ocorrendo a hipótese do Colaborador ser requisitado por autoridades brasileiras ou estrangeiras (em perguntas orais, interrogatórios, pedidos de informação ou documentos, notificações, citações ou intimações, e investigações de qualquer natureza) a divulgar qualquer Informação Confidencial a que teve acesso, o Colaborador deverá notificar imediatamente a Gestora, permitindo que a Gestora procure a medida judicial cabível para atender ou evitar a revelação.

Caso a Gestora não consiga a ordem judicial para impedir a revelação das informações em tempo hábil, o Colaborador poderá fornecer a Informação Confidencial solicitada pela autoridade. Nesse caso, o fornecimento da Informação Confidencial solicitada deverá restringir-se exclusivamente aquela a que o Colaborador esteja obrigado a divulgar.

A obrigação de notificar a Gestora subsiste mesmo depois de rescindido o contrato individual de trabalho, ao desligamento ou exclusão do Colaborador, por prazo indeterminado.

Este Termo é parte integrante das regras que regem a relação de trabalho e/ou societária do Colaborador com a Gestora, que ao assiná-lo está aceitando expressamente os termos e condições aqui estabelecidos.

A transgressão a qualquer das regras descritas neste Termo, sem prejuízo do disposto no item 3 e seguintes acima, será considerada infração contratual, sujeitando o Colaborador às sanções que lhe forem atribuídas pela Diretora de Compliance, conforme descrito no Código.

Demais disposições encontram-se disponíveis na Política de Segurança da Informação e Cibernética da Gestora.

Assim, estando de acordo com as condições acima mencionadas, assinam o presente em 02 vias de igual teor e forma, para um só efeito produzirem, na presença das testemunhas abaixo assinadas.

São Paulo, de de 20 .

_____

[COLABORADOR]

_____

SONATA GESTORA DE RECURSOS LTDA

ANEXO III

No exercício de suas atividades, a Gestora se utiliza primordialmente dos processos e ativos da organização identificados.

Para cada processo/ativo identificado, o Compliance avaliará o risco quanto à ameaça cibernética e à segurança da informação e seu impacto na organização, caso o evento de risco se realize, definindo, assim, as correspondentes ações de prevenção e proteção, conforme mapeamento abaixo:

Processo		Grau	Impacto			Ações de
	Ameaças	de Exposição				Prevenção e Proteção
Ativo			Financeiro	Reputação	Operacional	
						Firewall/antivírus/sistema operacional atualizados, backups diários, provedores de serviço na nuvem de boa reputação; uso de códigos/iniciais e não nomes dos clientes; sistemas com login/perfil de acesso; controle de acesso centralizado e conforme Inventário de Informações; logs de acessos e trilha de auditoria.
	Malware	ALTO	MEDIO	MEDIO	ALTO	
Sistemas na "Nuvem"						
	Ataques DDoS	BAIXO	BAIXO	BAIXO	MEDIO	
	Invasões	MEDIO	MEDIO	MEDIO	ALTO	
						Firewall/antivírus/sistema operacional atualizados, backups diários, provedores de serviço na nuvem de boa reputação; controle de acesso centralizado e conforme Inventário de Informações; logs de acessos e trilha de auditoria.
Servidor de Arquivos – Informações Gerais/Documentos	Malware	ALTO	MEDIO	MEDIO	ALTO	
	Ataques DDoS	BAIXO	BAIXO	BAIXO	MEDIO	
	Invasões	MEDIO	MEDIO	ALTO	ALTO	
						Código de Ética e Conduta e Regras e Procedimento de

						Compliance (treinamento e prática)
Contratos e documentos físicos com identificação de qualquer Pessoa Física/Terceiro Contratado/Colaboradores no escritório						Política de Mesa Limpa / armazenamento seguro
	Engenharia Social					Destruição de documentos segura
	Invasão de e-mails	BAIXO	BAIXO	ALTO	BAIXO	Acesso restrito ao escritório / segurança
						Acessos restrito à informação na nuvem conforme controle de acessos definidos
Trading	Engenharia Social					Provedores de e-mail de boa reputação; uso de códigos e contas e não nomes no trading
(e-mail e telefone)	Invasão de e-mails	MEDIO	BAIXO	MEDIO	BAIXO	
Comunicação geral (e-mail e telefone)	Engenharia Social					Provedores de e-mail de boa reputação; uso de nomes abreviados, iniciais ou primeiro nome na comunicação
	Invasão de e-mails	MEDIO	BAIXO	MEDIO	BAIXO	
Contratação de Serviços em Nuvem no país e no exterior	Engenharia Social Malwares Ataques DDoS Invasões (Advanted Persist Threats)	CRÍTICO	ALTO	ALTO	ALTO	Seguir as diretrizes emanadas no documento Regras e Procedimentos de Deveres Básicos – ANBIMA, integrante ao Código AGRT. Questionário DD Cibersegurança, quando aplicável.