MILES CAPITAL

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA E PROTEÇÃO DE DADOS

Versão	Atualizada em	Responsável:
1	Agosto/2021	Henrique Hauser
2	Fevereiro/2022	Henrique Hauser
3	Outubro/2023	Fernando Shirakawa
4	Janeiro/2024	Albert Munck
4	Fevereiro/2025	André Franco Branco

SUMÁRIO

Essa Política de Segurança da Informação e Cibernética visa proteger as informações de propriedade e/ou sob guarda da **Miles Capital Ltda**. ("Gestora"), garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das mesmas.

1. APLICAÇÃO

Essa política aplica-se a todos os Colaboradores, prestadores de serviços, sistemas, 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

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 n.º 21/2021 e do Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, a Gestora procurou identificar os eventos com maior possibilidade de ocorrência, bem como as informações de maior sensibilidade ("Informações Confidenciais"), com o propósito de mitigar os riscos à sua atividade.

3. PREMISSAS E DEFINIÇÕES

Diante da possibilidade de vazamento, alteração, destruição e qualquer outra forma de prejuízo em relação às Informações Confidenciais, o que é de extremo valor para a Gestora, dado o princípio fundamental de confiança que a gestora trabalha para manter junto aos seus clientes, a Gestora utilizou como linha de estruturação de sua Política, o Guia de Cibersegurança da ANBIMA, datado de dezembro de 2021.

O referido documento é um dos principais materiais sobre o tema no Mercado Financeiro, incluindo as melhores referências sobre proteção de dados.

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 Tecnoqualify.

4. PROGRAMA DE SEGURANÇA DA GESTORA

(i) 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 na perda e/ou adulteração de dados e Informações Confidenciais.

(ii) 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.

Assim, classifica-se as informações digitais da instituição em 3 (três) classes diferentes, quais sejam:

a) *Green Flag*:
   - Quaisquer informações e/ou dados que a Gestora teve acesso ou conhecimento por ser de domínio público ("Informação Pública");
   - Quaisquer informações e/ou dados que não estejam sujeitas a compromissos ou acordos de confidencialidade; ou
   - Quaisquer informações e/ou dados que tenham a obrigatoriedade de divulgação por lei ou autoridade competente.

b) Yellow Flag:
   - Quaisquer informações que venham a ter a obrigatoriedade de divulgação por lei ou autoridade competente, mas o termo legal ainda não foi iniciado ou findado (Ex. Data de Divulgação);

c) Red Flag:
   - Todas as Informações Confidenciais, a saber:
   - 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 e carteiras geridas pela Gestora; e
   - 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.

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:

1. 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 simultâneo pela plataforma Sharepoint;
- Computadores corporativos com acesso à Intranet/Internet, 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 – VPN 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;
- CPD local climatizado com sistema de ar-condicionado e com monitoramento de temperatura e com acesso restrito ao local;
- Sistema de *Proxy* com regras de conteúdo de acesso às páginas da internet;

2. Propriedade dos Recursos de TI

Todos os recursos computacionais e de sistemas disponibilizados para os Colaboradores são de propriedade da Gestora. Não é permitida a utilização de notebooks, tablets ou outros

hardwares para operações no âmbito da Gestora, salvo expressa permissão da área de *Compliance*.

3. 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 Tecnoqualify, mediante aprovação da 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 Tecnoqualify, 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 Tecnoqualify, 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 que atendam a requisitos mínimos de segurança (quantidade mínimas de caracteres, necessidade de números, caracteres especiais, dentre outras regras). 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 Tecnoqualify.

4. *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 Tecnoqualify, 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 é permitida e a conexão destes à internet é realizada em rede distinta da utilizada pela Miles no desempenho da sua rotina. Os Colaboradores estão autorizados a conectar seus telefones celulares e computadores pessoais utilizando essa mesma rede.
- 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 *Compliance*.

5. 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 4º, §8º, da Resolução CVM n.º 21/21.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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@milescapital.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 Tecnoqualify, mediante autorização e supervisão da Área de *Compliance*.

11. 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.

12. 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.

13. 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 (f*orward*)", 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.

14. 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.

15. Armazenamento em Nuvem (Cloud)

A Gestora realizará o armazenamento das Informações 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.

16. 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.

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.

5. MONITORAMENTO E TESTES DE CONTINGÊNCIA

O monitoramento dos controles existentes e estabelecidos nessa Política serão realizados e executados pela Tecnoqualify, 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.

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:

<u>Empresa de TI Terceirizada (Sob Supervisão do *Compliance*):</u>

a) Verificação e Auditoria dos Logs;
b) Criação de laudo pericial 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 ou Jurídico Contratado:

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 Companhia.
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.

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 pelo Diretor 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

É considerada como informação privilegiada qualquer Informação Relevante (conforme definido abaixo) a respeito de alguma empresa, que não tenha sido publicada e que seja conseguida de maneira privilegiada, em consequência da ligação profissional ou pessoal mantida com um cliente, com colaboradores de empresas estudadas ou investidas ou com terceiros, ou em razão da condição de Colaborador.

Considera-se Informação Relevante, para os efeitos deste Manual de Compliance, qualquer informação, decisão, deliberação, ou qualquer outro ato ou fato de caráter político-administrativo, técnico, negocial ou econômico-financeiro ocorrido ou relacionado aos seus negócios da Gestora que possa influir de modo ponderável: (a) na rentabilidade dos valores

mobiliários administrados pela Gestora; (b) na decisão de Investidores de comprar, vender ou manter cotas de fundos de investimento administrados pela Gestora; e (c) na decisão dos Investidores de exercer quaisquer direitos inerentes à condição de titular de cotas de fundos de investimento administrados pela Gestora.

As informações privilegiadas precisam ser mantidas em sigilo por todos que a acessarem, seja em função da prática da atividade profissional ou do relacionamento pessoal.

Em caso do Colaborador tiver acesso a uma informação privilegiada que não deveria ter, deverá transmiti-la rapidamente ao Diretor de Compliance, não podendo comunicá-la a ninguém, nem mesmo a outros membros da Gestora, profissionais de mercado, amigos e parentes, e nem a usar, seja em seu próprio benefício ou de terceiros. Se não houver certeza quanto ao caráter privilegiado da informação, deve-se, igualmente, relatar o ocorrido ao Diretor de Compliance.

- *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

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 terceiro;

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.

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.

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 dados@milescapital.com, por meio do qual o seu 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).

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.

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.

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.

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.

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.

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

Esta política será revisada anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.

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 **Miles Capital Ltda.** em agosto de 2021. 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 **Miles Capital Ltda.**, inscrita no CNPJ/MF sob o n.º 23.303.230/0001-25. ("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:

a) 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.

b) 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.

2. 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.

2.1 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.

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

2.3 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.

3 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.

3.1 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.

3.2 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.

3.3 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.

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

4. O Colaborador reconhece e toma ciência que:

a) Todos os documentos relacionados direta ou indiretamente com as Informações Confidenciais, inclusive contratos, minutas de contrato, cartas, fac-símiles, 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;

b) 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;

c) 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;

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

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.

5. 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.

5.1 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.

5.2 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.

6. 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.

6.1 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 pelo Diretor de *Compliance*, conforme descrito no Código.

6.2 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]

_____

MILES CAPITAL LTDA.