NORTE ASSET MANAGEMENT GESTÃO DE RECURSOS S.A.

POLÍTICA DA SEGURANÇA DA INFORMAÇÃO, PROTEÇÃO DE DADOS E SEGURANÇA CIBERNÉTICA

Novembro de 2023

Sumário

1. Introdução

A Política de Segurança da Informação, Proteção de Dados e Segurança Cibernética ("Política") da Norte Asset Management Gestão de Recursos S.A. ("Gestora") formaliza e esclarece as regras, os procedimentos e controles internos para fins de **Segurança da Informação, Proteção de Dados e Segurança Cibernética**. Aplica-se a todos os sócios, Colaboradores, prestadores de serviços e sistemas, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da Gestora, ou que acessem informações a ela pertencentes. Todo e qualquer usuário de recursos computadorizados da instituição tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática da Gestora.

Em linha com as principais discussões e preocupações do mercado, a Política tem como base princípios e procedimentos que asseguram a confidencialidade, a integridade e a disponibilidade dos dados e sistemas de informação utilizados pela Gestora.

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 a consecução de suas atividades.

Em atenção aos dispositivos da Resolução CVM nº 21/2021 e do Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros, assim como à Lei 13.709, de agosto de 2018 (Lei Geral de Proteção de Dados) 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.

Sendo assim, nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da Gestora, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

3. Abrangência

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

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

4. Segurança da Informação e Cibernética

Esta Política de Segurança da Informação, Proteção de Dados e Segurança Cibernética leva em consideração diversos riscos e possibilidades considerando o porte, perfil de risco, modelo de negócio e complexidade das atividades desenvolvidas pela Gestora.

A coordenação direta das atividades relacionadas a esta Política ficará a cargo do Diretor de Compliance, que será responsável inclusive por sua revisão, realização de testes e treinamento dos colaboradores da Gestora ("Colaboradores"), conforme aqui descrito.

5. Princípios básicos da segurança da informação

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 instituição trabalha para manter junto aos seus clientes, a Gestora utilizou como linha de estruturação de sua Política, o Guia de Cibersegurança, da ANBIMA.

Nesse sentido, os seguintes princípios básicos norteiam esta política:

- confidencialidade;
- treinamento e conscientização sobre segurança da informação para todos os Colaboradores; e
- testes periódicos dos sistemas de informação.

6. Confidencialidade e controle de acesso

O acesso aos sistemas é liberado com base no princípio da necessidade da informação para a execução da função do Colaborador (*need-to-know*/*need-to-have principle*). O controle é feito por meio dos perfis de acesso, que segregam as funções realizadas pelas diversas áreas. Cada área possui um conjunto de perfis relacionados às suas atividades, e a Gestora dispõe de controles internos para que o acesso seja liberado mediante aprovação da área de Compliance.

7. Treinamento e conscientização

A Gestora oferece treinamentos periódicos aos quais os Colaboradores são submetidos durante o ano, com o objetivo de conscientizá-los sobre confidencialidade das informações, *cyber* segurança, engenharia social, *phishing*, entre outras potenciais ameaças à integridade dos sistemas de informação.

8. Testes periódicos de segurança

A Gestora dispõe de tecnologias de defesa contra possíveis ataques aos seus sistemas de informação e realiza testes periódicos no sistema disponível na rede mundial de computadores.

Testes são realizados anualmente com os próprios Colaboradores, que são submetidos a uma simulação de *phishing*.

9. Identificação de Riscos (risk assessment)

No âmbito de suas atividades, a Gestora identificou os seguintes principais riscos internos e externos que precisam de proteção:

- **Dados e Informações:** as Informações Confidenciais, incluindo informações a respeito de investidores, clientes, Colaboradores e da própria Gestora, operações e ativos investidos pelas carteiras de valores mobiliários sob sua gestão, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);

- **Sistemas:** informações sobre os sistemas utilizados pela Gestora e as tecnologias desenvolvidas internamente e por terceiros;

- **Processos e Controles:** processos e controles internos que sejam parte da rotina das áreas de negócio e compliance da Gestora; e

- **Governança da Gestão de Risco:** a eficácia da gestão de risco pela Gestora quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

Ademais, no que se refere especificamente à segurança cibernética, a Gestora identificou as seguintes principais ameaças, em linha com o disposto no Guia de Cibersegurança da ANBIMA:

- **Malware:** softwares desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, Spyware e Ransomware);

- **Engenharia social:** métodos de manipulação para obter informações confidenciais (Pharming, Phishing, Vishing, Smishing, e Acesso Pessoal);

- **Ataques de DDoS (*distributed denial of services*) e botnets:** ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição;

- **Invasões (*advanced persistent threats*):** ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Com base no acima, a Gestora avalia e define o plano estratégico de prevenção e acompanhamento para a mitigação ou eliminação do risco, assim como as eventuais modificações necessárias e o plano de retomada das atividades normais e reestabelecimento da segurança devida.

10. Ações de Prevenção e Proteção

<u>Regras Gerais</u>

No tocante à segurança da informação, seguindo o princípio da confidencialidade e do controle de acesso mencionados acima, o acesso aos sistemas é liberado com base no princípio da necessidade da informação para a execução da função do Colaborador (*need-to-know/need-to-have principle),* aplicando-se referido

princípio, inclusive no que se refere às informações confidenciais, reservadas ou privilegiadas. O controle é feito por meio dos perfis de acesso, que segregam as funções realizadas pelas diversas áreas. Cada área possui um conjunto de perfis relacionados às suas atividades, e a Gestora dispõe de controles internos para que o acesso seja liberado mediante aprovação.

É proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da Gestora e circulem em ambientes externos à Gestora com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas como informações confidenciais. As exceções devem ser autorizadas pelo superior hierárquico ou pelo Diretor de Compliance.

A proibição acima referida também não se aplicará quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos forem indispensáveis e em prol da execução e do desenvolvimento dos negócios e dos interesses da Gestora. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade, providenciando sua eliminação após utilização.

Em consonância com as normas internas acima, os Colaboradores devem se abster de utilizar pen-drivers, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Gestora. É proibida a conexão de equipamentos na rede da Gestora que não estejam previamente autorizados pela área de informática (ainda que terceirizada) e pelo Diretor de Compliance.

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

O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam difamar a imagem e afetar a reputação da Gestora.

O recebimento de e-mails muitas vezes não depende do próprio Colaborador, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente. Na eventualidade do recebimento de mensagens com as características acima descritas, o Colaborador deve apagá-las imediatamente, de modo que estas permaneçam o menor tempo possível nos servidores e computadores da Gestora, bem como avisar prontamente o Diretor de Compliance.

A visualização de sites, blogs, fotologs, webmails, entre outros, que contenham conteúdo discriminatório, preconceituoso sobre origem, etnia, religião, classe social, opinião política, idade, sexo, ou deficiência física, obsceno, pornográfico ou ofensivo é terminantemente proibida.

A Gestora mantém por 5 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 armazenados, a Gestora consegue manter a integridade, autenticidade e auditabilidade das informações e sistemas, conforme Resolução CVM n.º 21/2021.

Acesso Escalonado ao Sistema

O acesso como “administrador” de área de desktop será limitado aos usuários aprovados pelo Diretor de Compliance e, com isso, serão determinados privilégios/credenciais e níveis de acesso de usuários apropriados para os Colaboradores.

A Gestora, ademais, mantém diferentes níveis de acesso a pastas e arquivos eletrônicos, notadamente aqueles que contemplem Informações Confidenciais, de acordo com as funções e responsabilidades dos Colaboradores e pode monitorar o acesso dos Colaboradores a tais pastas e arquivos com base na senha e login disponibilizados.

A implantação destes controles é projetada para limitar a vulnerabilidade dos sistemas da Gestora em caso de violação.

Senha e Login

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

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

Uso de Equipamentos e Sistemas

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

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

Acesso Remoto

A Gestora permite o acesso remoto pelos Colaboradores, de acordo com a seguinte regra: todos os acessos remotos são permitidos mediante pedido prévio e por e-mail ao Diretor de Compliance. Os acessos remotos darão permissões de acesso aos mesmos sistemas, pastase arquivos observados no escritório da gestora. O Diretor de Compliance, junto com a área de TI, serão responsáveis por validar tais acessos.

O acesso remoto será feito através de portal de serviço hospedado em Cloud e o acesso não permitirá a troca de dados fora do ambiente da rede da gestora.

Controle de Acesso

O acesso de pessoas estranhas à Gestora a áreas restritas somente é permitido com a autorização expressa de Colaborador autorizado pelo Diretor de Compliance sempre acompanhado, sendo certo que a Gestora

mantém sistema de acesso por código para o servidor de dados e Centro de Processamento de Dados ("CPD").

Somente os Diretores e os Colaboradores autorizados pelo Diretor de Compliance têm acesso ao CPD, ademais qualquer prestador de serviço só poderá entrar no CPD acompanhado por algum Colaborador da Gestora devidamente autorizado por um Diretor.

O acesso à rede de informações eletrônicas conta com a utilização de servidores exclusivos da Gestora e serviço de armazenamento de dados em nuvem, em conta dedicada, que não poderão ser compartilhados com outras empresas responsáveis por diferentes atividades no mercado financeiro e de capitais.

Tendo em vista que a utilização de computadores, telefones, internet, e-mail e demais aparelhos se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos Colaboradores, a Gestora monitora a utilização de tais meios.

Firewall, Software, Varreduras e Backup

A Gestora utilizará um hardware de firewall projetado para evitar e detectar conexões não autorizadas e incursões maliciosas. O Diretor de Compliance será responsável por determinar o uso apropriado de firewalls (por exemplo, perímetro da rede).

A Gestora manterá proteção atualizada contra malware nos seus dispositivos e software antivírus projetado para detectar, evitar e, quando possível, limpar programas conhecidos que afetem de forma maliciosa os sistemas da empresa (por exemplo, vírus, worms, spyware).

Como parte de suas rotinas regulares de verificação, a área de TI realiza um escaneamento completo dos sistemas da Gestora, ao menos 1 (uma) vez por semana, buscando identificar e eliminar as ameaças.

A Gestora também manterá e testará regularmente medidas de backup consideradas apropriadas pelo Diretor de Compliance. As informações da Gestora são atualmente objeto de backup diário com o uso de computação na nuvem.

Para maiores informações, vide Plano de Contingência e Continuidade, arquivado na sede da Gestora.

Observado disposto na presente Política e nas demais políticas da Gestora, as seguintes condutas devem ser observadas pelos Colaboradores da Gestora:

- é expressamente proibida a instalação de softwares não homologados pelo departamento de TI, bem como fazer downloads pela Internet;
- é expressamente proibida a instalação de qualquer hardware que não esteja homologado pelo departamento de TI (Ex.: scanner, câmera fotográfica etc.);
- não utilização de disquetes, CDs, pen drives ou quaisquer outras mídias, sem prévia autorização do Diretor de Compliance e quando necessário da devida verificação pelo departamento de TI;
- não abertura de e-mail de remetente duvidoso ou desconhecido, principalmente os que tiverem anexos ou executáveis;
- manutenção de sigilo das senhas de acesso à rede e Internet. Todo usuário terá uma pasta no servidor

da Gestora sempre na rede corporativa, onde devem ser gravados seus arquivos. Qualquer arquivo que não for salvo neste local, não terá garantia de backup (cópia de segurança); e

- comunicação ao departamento de TI, quando da instalação de softwares específicos.

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, é necessário adotar certos procedimentos que devem ser realizados previamente a contratação de Terceiros para serviços de Armazenamento na Nuvem.

Necessário iniciar um devido processo de Due diligence do Terceiro antes da contratação, devendo-se constatar se a organização segue políticas, programas e procedimentos formais relativos à segurança da informação e Cibersegurança.

Com isto em mente, a empresa objeto de contratação deverá enviar a Gestora:

(i) Documentos que atestem a existência dos respectivos procedimentos de Cibersegurança;
(ii) Último relatório de teste/auditoria periódica;
(iii) As certificações que possam comprovar a devida capacidade técnica do prestador de serviço.

Uma vez recebidos os respectivos documentos, a Área de Compliance analisará o Terceiro, podendo negar de imediato a contratação deste ou exigir remediações para que este se encaixe nos moldes de segurança a serem aplicados pela Gestora.

Somente após a aprovação pela Área de Compliance, o Terceiro poderá ser contratado para prestar serviços de Armazenamento na Nuvem.

Em caso de qualquer incidente constatado pelo Terceiro, este deverá de imediato enviar uma notificação relatando o ocorrido à Gestora, a qual, dependendo da situação, poderá reavaliar e inclusive rescindir de imediato o contrato do Terceiro.

Outros serviços com utilização da tecnologia em Nuvem também devem ser considerados para fins das regras aqui presentes, sendo necessário aplicar os mesmos procedimentos de Due Dilligence 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.

11. Treinamento e Conscientização dos Colaboradores

Conforme já disposto acima, a Gestora oferece treinamentos aos seus Colaboradores com o objetivo de conscientizá-los sobre a confidencialidade das informações, *cyber* segurança, proteção de dados, engenharia social, *phishing*, entre outras potenciais ameaças à integridade dos sistemas de informação. Referido treinamento é realizado anualmente.

12. Plano de Identificação e Resposta

Identificação de Suspeitas

Qualquer suspeita de violação, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da Gestora (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer Informações Confidenciais, mesmo que de forma involuntária, deverá ser informada ao Diretor de Compliance prontamente. O Diretor de Compliance determinará quais membros da administração da Gestora e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.

Ademais, o Diretor de Compliance determinará quais clientes ou investidores, se houver, deverão ser contatados com relação à violação. Caso o vazamento de informações envolva dados pessoais, além da notificação ao Diretor de Compliance, também deverá ser informada a situação ao Encarregado pelo Tratamento de Dados Pessoais, também conhecido como Data Protection Officer ("DPO"), para que este realize a devida apuração e tome as medidas cabíveis. Caso necessário, o Encarregado pelo Tratamento deDados Pessoais notificará, em prazo compatível com a severidade do evento, a Autoridade Nacional de Proteção de Dados.

Procedimentos de Resposta

O Diretor de Compliance responderá a qualquer informação de suspeita de violação, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da Gestora de acordo com os critérios abaixo:

(i) Avaliação do tipo de incidente ocorrido (por exemplo, infecção de malware, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;

(ii) Comunicação do incidente ao DPO caso haja suspeita ou indício que possa comprometer dados pessoais de posse da Gestora.

(iii) Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma desabilitados;

(iv) Determinação dos papéis e responsabilidades do pessoal apropriado;

(v) Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;

(vi) Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, administrador fiduciário, clientes ou investidores afetados, segurança pública);

(vii) Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, a fim de garantir a ampla disseminação e tratamento equânime da informação, se privilegiada; e

(viii) Determinação do responsável que arcará com as perdas decorrentes do incidente, a cargo do Comitê de Compliance, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

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 dependendo da seriedade do evento, inclusive de dados sensíveis, nos termos do artigo 38 da Lei Geral de Proteção de Dados.

13. 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 Geral de Proteção de Dados:

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 tem direito de solicitar à Gestora, em relação aos seus dados, a qualquer momento e mediante requerimento expresso. Esses direitos estão exemplificados abaixo, todavia o seu exercício em face da Gestora deve ser analisado em cada caso concreto.

a) confirmação de existência de tratamento;
b) acesso aos dados;

c) correção de dados incompletos, inexatos ou desatualizado;
d) anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei 13.709/2018;
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@norteasset.com.br, por meio do qual o seu DPO, o Sr. Edson Fujimori, 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 a sua Política de Privacidade. O 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.

Transferência Internacional de Dados Pessoais

Em certas situações a Gestora poderá realizar a transferência internacional de dados pessoais a partir do envio de informações e documentos, afim de possibilitar procedimentos junto à prestadores de serviços internacionais. Esta transferência é realizada segundo os parâmetros do artigo 33, II da Lei Geral de Proteção de Dados.

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.

14. Arquivamento de Informações

De acordo com o disposto nesta Política, os Colaboradores deverão manter arquivada toda e qualquer informação, bem como documentos e extratos que venham a ser necessários para a efetivação satisfatória de possível auditoria interna e/ou externa ou investigação de órgãos regulatórios em torno de possíveis atuações da Gestora, investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro (conforme política de lavagem de dinheiro da Gestora), em conformidade com o inciso IV do Artigo 18 da Resolução nº 21/2021 da CVM.

15. Propriedade Intelectual

A Lei de Propriedade Intelectual dispõe claramente que toda invenção e modelo de utilidade pertencem exclusivamente ao empregador, neste caso a Gestora, quando decorrerem de trabalho cuja execução se deu durante o período de vínculo do Colaborador com a Gestora.

Desta forma, todos os documentos e arquivos, incluindo, sem limitação, aqueles produzidos, modificados, adaptados ou obtidos pelos Colaboradores, relacionados, direta ou indiretamente, com suas atividades profissionais junto à Gestora, tais como minutas de contrato, memorandos, cartas, fac-símiles, apresentações a clientes, e-mails, correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, fórmulas, planos de ação, bem como modelos de avaliação, análise e gestão, em qualquer formato, são e permanecerão sendo propriedade exclusiva da Gestora, razão pela qual o Colaborador 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, sendo vedado ao Colaborador, inclusive, disseminar e retransmitir tais documentos, bem como apropriar-se de quaisquer desses documentos e arquivos após seu desligamento da Gestora, salvo se autorizado expressamente pelo Diretor de Compliance e ressalvado o disposto abaixo.

Caso um Colaborador, ao ser admitido, disponibilize à Gestora documentos, planilhas, arquivos, fórmulas, modelos de avaliação, análise e gestão ou ferramentas similares para fins de desempenho de sua atividade profissional junto à Gestora, o Colaborador deverá assinar declaração nos termos do Anexo I à presente Política, confirmando que: (i) a utilização ou disponibilização de tais documentos e arquivos não infringe quaisquer contratos, acordos ou compromissos de confidencialidade, bem como não viola quaisquer direitos de propriedade intelectual de terceiros; e (ii) quaisquer alterações, adaptações, atualizações ou modificações, de qualquer forma ou espécie, em tais documentos e arquivos, serão de propriedade exclusiva da Gestora, sendo que o Colaborador não poderá apropriar-se ou fazer uso de tais documentos e arquivos alterados, adaptados, atualizados ou modificados após seu desligamento da Gestora, exceto se aprovado expressamente pelo Diretor de Compliance.

Ademais, nenhum Colaborador da Gestora será remunerado além da remuneração previamente acordada, por qualquer trabalho que constitua invenção ou modelo de utilidade, quando no desenvolvimento de suas

atividades na Gestora.

16. Revisão desta Política

O Diretor de Compliance deverá realizar uma revisão da Política de Segurança da Informação e Cibernética a cada 12 (doze) meses, no mínimo, para avaliar a eficácia da sua implantação, identificar novos riscos, ativos e processos e reavaliando os riscos residuais, incluindo no relatório anual de compliance eventuais deficiências encontradas.

A finalidade de tal revisão será assegurar que os dispositivos aqui previstos permaneçam consistentes com as operações comerciais da Gestora e acontecimentos regulatórios relevantes.

CONTROLE DE VERSÕES	DATA	MODIFICADO POR	DESCRIÇÃO DA MUDANÇA
1	Agosto/20	Compliance	Versão inicial
2	Novembro/21	RRZ Consultoria	Adequação LGPD
3	Dezembro/22	Compliance	Revisão periódica
4	Novembro/23	RRZ Consultoria	Revisão periódica

ANEXO I - TERMO DE PROPRIEDADE INTELECTUAL

Por meio deste instrumento eu,_____, inscrito no CPF sob o nº _____("Colaborador"), DECLARO para os devidos fins:

(i) que a disponibilização pelo Colaborador à **NORTE ASSET MANAGEMENT GESTÃO DE RECURSOS S.A.**, inscrita no CNPJ/ME sob o nº 36.633.625/0001-38 ("Gestora"), nesta data, dos documentos contidos no *pen drive* da marca_____, número de série_____("Documentos"), bem como sua futura utilização pela GESTORA, não infringe quaisquer contratos, acordos ou compromissos de confidencialidade que o Colaborador tenha firmado ou que seja de seu conhecimento, bem como não viola quaisquer direitos de propriedade intelectual de terceiros;
(ii) ciência e concordância de que quaisquer alterações, adaptações, atualizações ou modificações, de qualquer forma ou espécie, nos Documentos, serão de propriedade exclusiva da GESTORA, sendo que o Colaborador não poderá apropriar-se ou fazer uso de tais documentos e arquivos alterados, adaptados, atualizados ou modificados após seu desligamento da GESTORA, exceto se aprovado expressamente pela GESTORA.

Para os devidos fins, o Colaborador atesta que os Documentos foram duplicados no pen drive da marca _____, número de série_____, que ficará com a GESTORA e cujo conteúdo é idêntico ao *pen drive* disponibilizado pelo Colaborador.

Os *pen drives* fazem parte integrante do presente termo, para todos os fins e efeitos de direito. A lista de arquivos constantes dos *pen drives* se encontra no Apêndice ao presente termo.

_____,____de_____de_____.

_____
Colaborador:
CPF: