POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, CIBERNÉTICA E PROTEÇÃO DE DADOS

Versão	Atualizada em	Responsável:
4	Setembro /2026	Diretoria de Compliance, Risco e PLD

Sumário

1. APLICABILIDADE 3
2. OBJETIVO 3
3. PREMISSAS E DEFINIÇÕES 3
4. PROGRAMA DE SEGURANÇA DA SONATA 3
4.1 Princípios de Segurança da Informação 3
4.2 Princípios de Segurança Cibernética e Identificação de Riscos 4
4.3 Classificação da Informação 4
4.4 Ações de Prevenção e Proteção 4
4.5 Estrutura de TI 5
4.6 Disponibilização e uso 5
4.7 Softwares 5
4.8 Registros 5
4.9 Responsabilidades do usuário 6
4.10 Outras Proteções aos Computadores 6
4.11 Regras e responsabilidades do uso da Internet 6
4.12 Bloqueio de endereços de Internet 6
4.13 Uso de correio eletrônico particular 6
4.14 Endereço eletrônico de programas ou de comunicação corporativa 6
4.15 Acesso à distância ao e-mail 6
4.16 Responsabilidades e forma de uso de Correio Eletrônico 7
4.17 Cópias de segurança do Correio Eletrônico 7
4.18 Armazenamento em Nuvem (Cloud) 7
4.19 Contratação de Terceiros para Serviços de Armazenamento na Nuvem 7
4.20 Uso de IA 7
4.21 Dispositivos Pessoais 8
5. MONITORAMENTO E TESTES DE CONTINGÊNCIA 8
6. PLANO DE RESPOSTA 8
7. CONFIDENCIALIDADE 9
7.1 Informação Privilegiada e Insider Trading 9
7.2 Divulgação Privilegiada 9
7.3 Front Running 9
8. PROTEÇÃO DE DADOS PESSOAIS 9
8.1 Escopo e Abrangência: 9
8.2 Princípios Norteadores: 10
8.3 Direitos 10
8.4 Período de Armazenamento dos Dados Pessoais: 11
8.5 Cooperação com Autoridades: 11
8.6 Governança: 11

8.7 Obrigação de Reporte:.....11
8.8 Registro de Eventos:.....12
8.9 Treinamento:.....12
9. VIGÊNCIA E ATUALIZAÇÃO.....12
10. DIVULGAÇÃO.....12
11. MANUTENÇÃO DOS ARQUIVOS.....12
ANEXO I - TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, CIBERNÉTICA E PROTEÇÃO DE DADOS.....13
ANEXO II - TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE.....14

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 Sonata, ou que acessem informações a ela pertencentes. Todo e qualquer usuário de recursos computadorizados disponibilizados pela Sonata 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 Ltda.** ("Sonata ou Gestora"), estabelece os mecanismos de segurança da informação, segurança cibernética e proteção de dados com a finalidade de assegurar a confidencialidade, a integridade, disponibilidade, legalidade, autenticidade e auditabilidade dos dados e dos sistemas de informação utilizados, no suporte às atividades de gestão de recursos e gestão de patrimônio, em atenção aos dispositivos da Resolução CVM n.º 21/21, da Resolução CVM n.º 175/22 e alterações consolidadas, do Código ANBIMA de Administração e gestão de Recursos de Terceiros, das Regras e Procedimentos de Deveres Básicos da ANBIMA (arts. 9º a 17), do Guia ANBIMA de Cibersegurança (4ª edição), da Lei n.º 13.709/18 - Lei Geral de Proteção de Dados Pessoais (LGPD) e das Resoluções CD/ANPD n.º 15/24 e 18/24.

3. PREMISSAS E DEFINIÇÕES

Adiante, a Sonata abordará os principais mecanismos e procedimentos de prevenção às ameaças ao patrimônio, à imagem e, principalmente, aos seus negócios.

Todas as diretrizes aqui dispostas são de responsabilidade da Diretoria de Compliance, Risco e PLD da Sonata, sob a direção do Comitê de Compliance.

4. PROGRAMA DE SEGURANÇA DA SONATA

4.1 Princípios de Segurança da Informação

O Programa de Segurança da Informação da Sonata, rege direitos e deveres dos Colaboradores e de terceiros que possuam acesso aos ativos de informação da instituição. Os princípios fundamentais que regem este programa compreendem:

- **Confidencialidade**: garantia de que o acesso à informação seja restrito e obtido somente por pessoas expressamente autorizadas;
- **Integridade**: garantia de que as informações, dados, e sistemas estejam protegidos

contra alterações não autorizadas, perdas acidentais ou fraudes, mantendo-se íntegros e completos;

- **Disponibilidade**: garantia de que os usuários autorizados tenham acesso à informação e aos ativos de processamento sempre que necessário para o desempenho de suas atividades;
- **Legalidade**: conformidade plena com o ordenamento jurídico, as instruções e normas editadas pela Comissão de Valores Mobiliários (CVM), pelo Banco Central do Brasil (BCB), pela Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (ANBIMA) e pela Autoridade nacional de Proteção de Dados (ANPD);
- **Autenticidade**: garantia de veracidade da origem e do emissor da informação;
- **Auditabilidade**: rastreabilidade completa e inalterável de todos os acessos, transações, alterações e eventos de processamento efetuados nos sistemas da Sonata.

4.2 Princípios de Segurança Cibernética e Identificação de Riscos

A segurança cibernética compreende a proteção dos ativos de informação contra ataques maliciosos, acessos não autorizados, interceptações, adulterações ou indisponibilidade operacional. Não se limitando aos riscos citados acima, a Sonata relaciona todos os processos e ativos relevantes, bem como a avaliação contínua dos riscos cibernéticos, conforme orientação da Diretoria de Compliance, Risco e PLD. A avaliação dos riscos e ações de prevenção inerentes às atividades desempenhadas pela Sonata estão descritas no Anexo III da presente Política.

4.3 Classificação da Informação

Todas as informações produzidas, transmitidas, processadas ou custodiadas pela Sonata são classificadas segundo seu grau de sensibilidade e criticidade operacional, o detalhamento consta da Política de Confidencialidade, Tratamento da Informação e Segregação de Atividades da Sonata

A supervisão do tratamento dos dados contemplará a classificação formal, a utilização de equipamentos homologados, os controles de armazenamento e computação em nuvem, a gestão de acessos e a capacitação continuada dos Colaboradores.

4.4 Ações de Prevenção e Proteção

Deste modo, a Sonata segrega as informações geradas, aperfeiçoando a implementação de processos e controles internos. A atuação preventiva adota sistema de graduação de criticidade:

- **Nível Ordinário**: operação regular, com monitoramento automatizado de logs e acessos;
- **Alerta Prévio**: identificação de inconformidades, tentativas incomuns de acesso ou movimentações anômalas, demandando averiguação imediata;
- **Incidente crítico**: comprovação da violação, invasão cibernética, vazamento de dados ou indisponibilidade sistêmica, demandando acionamento instantâneo do Plano de Resposta e comunicação às instâncias decisórias.

4.5 Estrutura de TI

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

- Rotinas de backup diário, automatizadas e com guarda em ambiente apartado e seguro;
- Computadores corporativos configurados e autorizados com acesso gerenciado à nuvem;
- Acesso restrito e autenticado ao sistema de informações de posição dos fundos e gerenciamento de riscos;
- *Firewall* redundante com controle rigoroso do tráfego de rede e portas;
- *Switches* Giga corporativo integrados à telefonia IP gerenciada;
- Correio eletrônico institucional provido de filtros *anti-spam* e antivírus em nível servidor;
- Sistema de Nobreak com autonomia adequada para salvaguarda de dados operacionais;
- Sistema de Proxy com registro detalhado de conexões e tráfego;
- Aplicação obrigatória do Questionário de Diligência de Cibersegurança da ANBIMA para contratação e manutenção de fornecedores de infraestrutura e serviços em nuvem.

4.6 Disponibilização e uso

Os recursos e equipamentos de Tecnologia da Informação são disponibilizados para o exercício estritamente profissional das funções atribuídas aos Colaboradores. A criação, alteração e exclusão de credenciais de acesso subordinam-se à prévia requisição e aprovação da Diretoria de Compliance, Risco e PLD.

Os parâmetros mandatórios de autenticação e senhas incluem: (a) extensão mínima de 12 (doze) caracteres contendo letras maiúsculas, minúsculas, números e caracteres especiais, com autenticação multifator (MFA) obrigatória para e-mail, sistemas em nuvem e sistemas de gestão; (b) ciclo de não reutilização das últimas 5 (cinco) senhas cadastradas; (c) bloqueio automático após no máximo 3 (três) tentativas consecutivas e incorretas de autenticação; e (d) validade máxima e expiração obrigatória em prazo de 180 (cento e oitenta) dias. Todos os eventos de autenticação e privilégios de administrador permanecem integralmente auditáveis.

4.7 Softwares

É vetado aos usuários implantar novos programas ou alterar configurações sem a permissão formalizada da Diretoria de Compliance, Risco e PLD. É vedado a usuário implantar ou alterar componentes físicos em seus computadores.

Apenas softwares devidamente licenciados, inventariados e homologados pela Área de TI serão instalados nos computadores corporativos da Sonata.

4.8 Registros

Os registros eletrônicos (*logs*) de acesso, operações, autenticações e tráfego de dados serão

armazenados de forma segura e inalterável pelo prazo mínimo de 5 (cinco) anos, em estrita observância à Resolução CVM n.º 21/21 e demais exigências regulatórias aplicáveis, garantindo sua plena integridade, autenticidade e auditabilidade perante os órgãos fiscalizadores.

4.9 Responsabilidades do usuário

Constitui responsabilidade indelegável de todo Colaborador zelar pela integridade física e lógica dos equipamentos corporativos sob sua guarda, manter o sigilo absoluto de suas senhas individuais, bloquear a estação de trabalho sempre que se ausentar e reportar imediatamente qualquer anomalia à Diretoria de Compliance, Risco e PLD.

4.10 Outras Proteções aos Computadores

Os computadores corporativos devem manter ativas as soluções antivírus e de proteção contra códigos maliciosos homologadas, as quais receberão atualizações automáticas de assinaturas e varreduras periódicas. É vedada a desativação voluntária de ferramentas de proteção.

4.11 Regras e responsabilidades do uso da Internet

A conexão à rede mundial de computadores é fornecida para o exercício das atividades profissionais. É estritamente proibida a navegação em sítios eletrônicos que contenham material pornográfico, preconceituoso, ilícito, de apostas ou jogos de azar, ou que promovam atividades lesivas ou ilegais

4.12 Bloqueio de endereços de Internet

A Sonata mantém controle de filtragem e bloqueio ativo de sítios e aplicações que ofereçam riscos à segurança da rede corporativa ou que não guardem relação com o escopo operacional da Gestora, cabendo revisão técnica mediante solicitação formal e justificada à Diretoria de Compliance, Risco e PLD.

4.13 Uso de correio eletrônico particular

É vedado o uso de contas de correio eletrônico particular para a condução de negócios, remessa de dados confidenciais ou tratamento de informações corporativas da Sonata e de seus clientes.

4.14 Endereço eletrônico de programas ou de comunicação corporativa

As comunicações oficiais da Sonata serão realizadas por meio dos endereços e domínios institucionais (@sonatainvest.com.br ou correlatos homologados). Nenhum Colaborador poderá vincular canais de atendimento ou ordens de clientes a contas privadas.

4.15 Acesso à distância ao e-mail

O acesso remoto ao correio corporativo e aos sistemas em nuvem exige a utilização de múltiplos fatores de autenticação (MFA) e equipamentos com proteções de segurança ativas, submetendo-se aos mesmos rigores e deveres de sigilo das instalações físicas.

4.16 Responsabilidades e forma de uso de Correio Eletrônico

O e-mail institucional é ferramenta corporativa de propriedade da Sonata. É terminantemente proibido o envio de mensagens contendo conteúdo difamatório, assediador, discriminatório ou a transmissão não autorizada de dados protegidos e arquivos executáveis suspeitos.

4.17 Cópias de segurança do Correio Eletrônico

Todas as comunicações eletrônicas trafegadas no âmbito corporativo são objeto de custódia e cópias de segurança em ambiente resiliente. O e-mail corporativo da Sonata fica na nuvem contratado junto a um reconhecido provedor desse tipo de serviço, qual seja, o Google Workspace (Gmail e Google Drive).

4.18 Armazenamento em Nuvem (Cloud)

Os dados corporativos alocados em infraestrutura de computação em nuvem devem observar elevados padrões de criptografia em trânsito e em repouso, políticas de controle de acesso fundamentadas no privilégio mínimo e replicação geográfica de salvaguarda.

4.19 Contratação de Terceiros para Serviços de Armazenamento na Nuvem

A contratação e a manutenção de prestadores de serviços de computação em nuvem submetem-se ao processo prévio e contínuo de diligência (*due diligence*), conforme definidos nas Regras de e Procedimentos de Deveres Básicos da ANBIMA, sendo verificado no mínimo:

- Garantia inequívoca de acesso irrestrito da Sonata aos seus dados a qualquer momento;
- Níveis de serviço contratuais (SLA) para confidencialidade, integridade, disponibilidade e tempo de recuperação de desastres;
- Aderência comprovada às certificações internacionais e normas de segurança reconhecidas (como ISO/IEC 27001 e SOC);
- Provimento regular de relatórios de auditoria e recursos de monitoramento;
- Identificação precisa dos locais de custódia e efetiva segregação lógica e física dos dados;
- Qualidade técnica dos controles de autenticação e de combate a acessos não autorizados.

O processo de contratação discriminará os modelos de serviço contratados (SaaS - Software as a Service, PaaS - Platform as a Service, IaaS - Infrastructure as a Service) e observará a possibilidade de dispensa ou simplificação nos casos taxativamente previstos na autorregulação vigente.

4.20 Uso de IA

O uso de Inteligência Artificial Generativa é restrito às ferramentas homologadas e listadas pela

Diretoria de Compliance, Risco e PLD, sendo vedada a inserção de informações confidenciais, privilegiadas ou de dados pessoais em ferramentas não homologadas e obrigatória a revisão humana de qualquer conteúdo gerado utilizado em análises, relatórios ou comunicações, observado o Guia ANBIMA de Governança de IA.

4.21 Dispositivos Pessoais

O acesso a e-mail e sistemas corporativos a partir de dispositivos pessoais somente será permitido mediante autorização da Diretoria de Compliance, Risco e PLD, com MFA, bloqueio de tela, criptografia do dispositivo, sistema operacional atualizado e possibilidade de remoção remota dos dados corporativos, sendo vedado o armazenamento local de informações confidenciais ou restritas.

5. MONITORAMENTO E TESTES DE CONTINGÊNCIA

A infraestrutura tecnológica e as rotinas cibernéticas da Sonata serão submetidas a monitoramento contínuo sob a supervisão da Diretoria de Compliance, Risco e PLD. Adicionalmente, serão executados testes periódicos de continuidade e recuperação, no mínimo anualmente, cujos procedimentos, métricas e cenários simulatórios de contingência operacional estão dispostos no Plano de Continuidade de Negócios da instituição.

Adicionalmente, serão realizados, no mínimo anualmente, teste de intrusão (pentest) e varredura de vulnerabilidades por empresa especializada e, no mínimo semestralmente, simulações de phishing, com registro dos resultados e dos planos de ação. As atualizações de segurança (patches) serão aplicadas mensalmente ou, em caso de vulnerabilidade crítica, em até 7 (sete) dias.

6. PLANO DE RESPOSTA

O Plano de Resposta a Incidentes Cibernéticos estabelece os fluxos obrigatórios de contenção e remediação

- **Empresa de TI Terceirizada**: atuação técnica imediata na contenção do ataque, isolamento dos perímetros afetados, restauração de sistemas e análise forense da vulnerabilidade;
- **Compliance, Risco e PLD:** elaboração de relatório circunstanciado, mensuração dos impactos operacionais e comunicação à ANPD e aos titulares afetados, quando o incidente puder acarretar risco ou dano relevante, no prazo de 3 (três) dias úteis contados do conhecimento de que o incidente afetou dados pessoais (arts. 6º e 9º da Resolução CD/ANPD n.º 15/24), e comunicação aos clientes, administradores fiduciários, CVM e ANBIMA, quando cabível;
- **Back Office e Gestão**: levantamento detalhado de perdas de dados e planejamento emergencial de contenção do risco de liquidez e continuidade das ordens pendentes;
- **Classificação**: graduação da severidade do incidente (baixa, média, alta ou crítica);

- **Registro**: inclusão obrigatória de todos os eventos no Relatório Anual de Controles Internos e Compliance;
- **Responsabilização**: avaliação de condutas e apuração de culpabilidade disciplinar nos termos estritos do Código de Ética e Conduta.

7. CONFIDENCIALIDADE

Toda informação relativa às estratégias, posições de carteira, operações financeiras e dados de clientes detida pela Sonata é de natureza estritamente confidencial. A referida informação 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 Diretoria de Compliance, Risco e PLD.

Quem tiver acesso a uma informação privilegiada deverá divulgá-la imediatamente a Diretoria de Compliance, Risco e PLD para adoção das salvaguardas institucionais pertinentes, conforme a Política de Confidencialidade, Tratamento de Informações e Segregação de Atividades.

7.1 Informação Privilegiada e Insider Trading

É expressamente vedada a utilização de informação relevante e privilegiada ainda não divulgada ao mercado para obter vantagem indevida, para si ou para outrem, mediante negociação de valores mobiliários (*insider trading*), sujeitando-se o infrator às sanções administrativas, civis e penais cabíveis. O detalhamento deste assunto está disponível na Política de Confidencialidade, Tratamento da Informação e Segregação de Atividades da Sonata.

7.2 Divulgação Privilegiada

Constitui infração grave repassar informação confidencial ou privilegiada a terceiros não autorizados (*tipping*), devendo os Colaboradores manter absoluta reserva sobre as operações em análise ou em curso na gestora.

7.3 Front Running

É terminantemente proibida a realização de operações com valores mobiliários para carteira própria ou de pessoas vinculadas quando se tenha conhecimento prévio de ordens a serem executadas em nome dos veículos e fundos geridos pela Sonata (*front running*).

8. PROTEÇÃO DE DADOS PESSOAIS

8.1 Escopo e Abrangência:

As diretrizes de proteção de dados aplicam-se a todas as atividades de tratamento de dados pessoais realizadas pela Sonata, compreendendo a coleta, produção, recepção, classificação,

utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação.

8.2 Princípios Norteadores:

O tratamento de dados pessoais na Sonata fundamenta-se nos princípios do art. 6º da Lei n.º 13.709/18 (LGPD): finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

O controle dos dados pessoais tratados pela Sonata é mantido em inventário de dados pessoais (registro das operações de tratamento, art. 37 da LGPD), que identifica, para cada processo, o controlador e o operador, a base legal (arts. 7º e 11 da LGPD), a finalidade, a duração do tratamento, os compartilhamentos e os responsáveis.

8.3 Direitos

Em respeito aos direitos fundamentais de liberdade, de intimidade e de privacidade, e, ainda, ao disposto no art. 18, da Lei n.º 13.709/18, o titular dos dados pessoais pode exercer seus direitos ao solicitar à Sonata, seus dados, a qualquer momento e mediante requerimento expresso. Esses direitos estão exemplificados abaixo, todavia o seu exercício em face da Sonata 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 n.º 13.709/18;
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 Sonata 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 com o Aviso de Privacidade publicado em seu site. As requisições dos

titulares serão respondidas em até 15 (quinze) dias, nos termos do art. 19, II, da LGPD. 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 Sonata, 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 Sonata 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 Sonata 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 Sonata, serão notificados sobre tal divulgação, para que tomem as medidas apropriadas.

Adicionalmente, a Sonata 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 Compliance.

A Sonata manterá registro das operações de tratamento de dados pessoais (art. 37 da LGPD), revisado anualmente pelo Encarregado.

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 Sonata para a devida apuração. Caso o incidente possa acarretar risco ou dano relevante aos titulares, o Encarregado pelo Tratamento de Dados Pessoais comunicará a Autoridade Nacional de Proteção de Dados e os titulares no prazo de 3 (três) dias úteis, nos termos da Resolução CD/ANPD n.º 15/24.

8.8 Registro de Eventos:

Todos os incidentes de segurança envolvendo dados pessoais, inclusive os não comunicados à ANPD, serão registrados com as informações mínimas do art. 10 da Resolução CD/ANPD n.º 15/24 e mantidos pelo prazo mínimo de 5 (cinco) anos, sem prejuízo de sua inclusão no Relatório de Controles Internos e da atualização do Relatório de Impacto à Proteção de Dados Pessoais (art. 38 da LGPD), quando aplicável.

8.9 Treinamento:

A Sonata treinará seus Colaboradores sobre a proteção de dados pessoais e de dados sigilosos de acordo com as suas Políticas.

9. VIGÊNCIA E ATUALIZAÇÃO

Esta Política entra em vigor na data de sua aprovação e deverá ser revisada em até 12 (doze) meses, ou em prazo inferior se exigido por regulação específica. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.

10. DIVULGAÇÃO

Esta Política será divulgada a todos os Colaboradores e prestadores de serviços relevantes mediante entrega formal física ou eletrônica, ficando permanentemente disponível para consulta no repositório corporativo da Sonata.

11. MANUTENÇÃO DOS ARQUIVOS

A Sonata manterá armazenados eletronicamente, todos os arquivos, pertinentes ao processo de Compliance desta Política, pelo prazo mínimo de 5 (cinco) anos, conforme legislação vigente.

Sem prejuízo do prazo mínimo regulatório acima referido, documentos que possam servir como meio de prova em processos judiciais ou administrativos serão conservados pelo prazo prescricional aplicável, observando-se o limite de 10 (dez) anos previsto no art. 205 do Código Civil.

ANEXO I - TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, CIBERNÉTICA E PROTEÇÃO DE DADOS

Por meio do presente Termo, eu,_____, inscrito no CPF/MF sob o n.º _____, declaro que li e estou plenamente de acordo com as disposições da Política de Segurança da Informação, Cibernética e Proteção de Dados aprovados pela **Sonata**. Comprometo-me a cumprir com integralmente seus preceitos e diretrizes de confidencialidade, integridade e proteção de dados.

[Nome do Colaborador]

Data: ____ / ____ / _____

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. ("Sonata"), estabelecem o presente Termo de Responsabilidade e Confidencialidade sob as seguintes cláusulas:

1. **Definições**: são consideradas informações confidenciais todos os dados técnicos, estratégicos, mercadológicos, cadastrais, financeiros e societários a que o Colaborador tiver acesso em razão de suas atividades;
2. **Obrigações de Sigilo**: o Colaborador compromete-se a manter estrito e absoluto sigilo sobre qualquer informação confidencial, não a divulgando nem permitindo sua divulgação sem prévia anuência por escrito da Sonata;
3. **Propriedade**: todas as criações, bancos de dados, relatórios, códigos e informações geradas no âmbito da relação profissional pertencem exclusivamente à **Sonata Gestora de Recursos Ltda.**;
4. **Sanções**: o descumprimento das cláusulas sujeitará o infrator à rescisão contratual motivada por justa causa e responsabilização civil e criminal cabíveis;
5. **Dedução de Rendimentos**: a Sonata reserva-se o direito de reter e compensar eventuais prejuízos comprovados resultantes de ato doloso ou culposo grave;
6. **Notificação a Autoridades**: o dever de confidencialidade cessa exclusivamente mediante ordem judicial ou determinação legal formal de autoridade competente;
7. **Ciência**: o Colaborador declara ciência integral de todas as obrigações e penalidades previstas neste instrumento.

São Paulo, de de 20 .

_____

[COLABORADOR]

_____

Sonata Gestora de Recursos Ltda.

ANEXO III – MAPEAMENTO DE RISCOS

Categoria de Risco	Ameaça Identificada	Grau de Exposição	Ações de Prevenção e Proteção
Segurança de Rede e Infraestrutura	Ataques de Malware / Ransomware e Negação de Serviço (DDoS)	Médio a Alto	Implementação de antivírus corporativo com varredura em tempo real, firewall redundante, bloqueio perimetral de portas e testes anuais de contingência.
Contratação de Serviços em Nuvem	Invasões (Advanced Persistent Threats – APT) e vazamento de dados	Alto	Aplicação rigorosa do Questionário de Due Diligence de Cibersegurança da ANBIMA, autenticação multifator (MFA) obrigatória, criptografia de dados e backups automatizados.
Fator Humano e Acessos	Engenharia Social, Phishing e Acesso Indevido por credenciais vulneráveis	Médio	Treinamentos anuais obrigatórios sobre LGPD e cibersegurança, política estrita de senhas (180 dias e complexidade), logs auditáveis por 5 anos e Termos de Adesão.