POLÍTICA	**CÓDIGO:** PG|19.00|14 **EDIÇÃO:** 21/06/2024 **Nº DE PÁGINAS:** 18 **VERSÃO:** 4ª **ND:** 2

SEGURANÇA CIBERNÉTICA | SIGILO | LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

ÓRGÃO ELABORADOR: *Compliance*	**ÓRGÃO VALIDADOR:** Diretor Presidente

SUMÁRIO

1. OBJETIVO

A presente tem como objetivo estabelecer, implementar e supervisionar um conjunto de práticas que protegem a informação armazenada nos computadores, aparelhos de comunicação transmitidas através das redes de comunicações, incluindo internet e celulares, garantindo a disponibilidade, integridade, confidencialidade, legalidade e autenticidade delas.

Ademais, a Política aborda também as práticas de tratamento de informações da WISE ASSET, no que diz respeito a proteção e sigilo, com base na Lei Gera de Proteção de Dados Pessoais – Lei nº Lei 13.790/18 (“LGPD”).

2. ABRANGÊNCIA

Este documento é aplicável a todos os colaboradores da empresa, os quais estão obrigados a observar, cumprir e fazer cumprir os termos e condições deste sistema.

3. DEFINIÇÕES, CONCEITOS E SIGLAS

TERMO	DEFINIÇÃO
ALTA ADMINISTRAÇÃO	Estrutura organizacional compreendida a partir da Diretoria Estatutária e Conselho de Administração.
ANEXOS	Tabelas, formulários, dados, imagens ou figuras gráficas incorporadas às últimas páginas de uma IN, para ilustrar ou facilitar o entendimento e aplicação do seu conteúdo.
COLABORADORES	Órgãos de membros estatutários, funcionários e estagiários.
DIRETRIZES	Conjunto de padrões para gestão, estrutura organizacional, processos, procedimentos e recursos necessários à gestão.
POLÍTICA	Descrevem a visão, missão e valores da empresa, os quais devem ser incorporados a todos os documentos legais elaborados internamente.

PRINCÍPIOS	Preceitos elementares ou requisitos que a gestora deve observar na realização de suas atividades, buscando uma conduta exigida nos relacionamentos, operações e serviços, em seu ambiente interno ou externo.
RESPONSABILIDADE	Consiste na obrigação de responder corporativa ou localmente por determinadas atribuições.

4. BASES NORMATIVAS

4.1. Documentos de Referência

- **Resolução CVM nº 35, de 26 de maio de 2021**: estabelece normas e procedimentos a serem observados na intermediação de operações realizadas com valores mobiliários em mercados regulamentados de valores mobiliários e revoga a Deliberação CVM nº 105, de 22 de janeiro de 1991, e as Instruções CVM nº 51, de 9 de junho de 1986, CVM nº 333, de 6 de abril de 2000, CVM nº 505, de 27 de setembro de 2011, Instrução CVM nº 526, de 21 de setembro de 2012; Instrução CVM nº 581, de 29 de setembro de 2016; Instrução CVM nº 612, de 21 de agosto de 2019; e Instrução CVM nº 618, de 28 de janeiro de 2020;
- **Lei nº 13.790/18:** dispõe sobre a proteção dos dados pessoais

4.2. Documentos Complementares

- Código de Ética e Conduta.

5. DETALHAMENTO

5.1. Princípios

a) *Comprometimento*: os colaboradores da Gestora, independentemente de sua função exercida, devem estar comprometidos em seguir as políticas, práticas e controles internos necessários ao cumprimento desta Política;

b) Compliance: esta Política deve estar em conformidade com as Regras e Procedimentos da ANBIMA, bem como as metodologias e procedimentos adotados devem ser passíveis de verificação pelos administradores fiduciários dos fundos sob gestão da Gestora e da área de Supervisão da ANBIMA;

c) *Consistência:* as informações a serem utilizados no processo de gestão de risco de liquidez devem ser obtidos de fontes externas independentes e seguir o princípio da Equidade. Quando da impossibilidade de os dados serem obtidos de fontes externas independentes, a metodologia e premissas devem ser únicas para todos os fundos. Os dados privados devem seguir metodologia devidamente documentada para a captura dos mesmos e deve ser passível de verificação por terceiros;

d) *Ética e Legalidade*: atuar em conformidade com a legislação e regulação vigentes, com padrões de ética e conduta;

e) *Formalismo*: o processo aqui descrito deve ser seguido pela área de gestão de risco e todos os documentos referentes às suas decisões devem ser guardados e passíveis de serem auditáveis;

f) *Melhoria contínua*: compromisso em aperfeiçoar os padrões de ética e conduta, aplicação de medidas corretivas, adequados níveis de segurança, qualidade dos produtos ofertados e eficiência dos serviços;

g) *Melhores Práticas*: o processo e a metodologia desta Política devem seguir as melhores práticas de mercado;

h) *Transparência*: disponibilização, a qualquer tempo, de informações relativas as atividades e decisões sobre o processo alinhado a estratégia da **WISE ASSET**.

5.2. Diretrizes

5.2.1. Segurança

Todas as Informações sigilosas constituem ativos de valor para a gestora, e, por conseguinte, precisam ser adequadamente protegidas contra ameaças e ações que possam causar danos e prejuízos para a empresa, clientes, fundos e colaboradores.

As informações sigilosas podem ser armazenadas e transmitidas de diversas maneiras, como, por exemplo, arquivos eletrônicos, mensagens eletrônicas, sites de internet, bancos de dados, meio impresso, mídias de áudio e de vídeo dentre outras.

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

Assim, por princípio, a guarda e segurança das informações sigilosas devem abranger três aspectos básicos destacados a seguir:

- Acesso: Somente pessoas devidamente autorizadas pela WISE ASSET devem ter acesso às Informações sigilosas;
- Integridade: Somente alterações, supressões e adições autorizadas pela gestora devem ser realizadas às Informações sigilosas;
- Disponibilidade: As informações sigilosas devem estar disponíveis para os colaboradores autorizados sempre que necessário ou for demandado.

As informações sigilosas devem ser adequadamente gerenciadas e protegidas contra furto, fraude, espionagem, perda não intencional, acidentes e outras ameaças.

A gestora deve seguir os seguintes procedimentos para garantir a segurança cibernética:

Identificação e avaliação de riscos ("*risk assessment*")

Os seguintes itens devem ser observados:

- Confidencialidade: garantia de que a informação é acessível somente às pessoas autorizadas;
- Integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento;
- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;
- Riscos Cibernéticos: riscos de ataques cibernéticos, oriundos de *malware*, técnicas de engenharia social, invasões, ataques de rede (DDoS e *Botnets*), fraudes externas, desprotegendo dados, redes e sistemas da empresa, causando danos financeiros e de reputação consideráveis.
- Malwares:
    - Vírus: software que causa danos à máquina, rede, *softwares* e banco de dados;
    - Cavalo de Tróia: 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;
- *Ransomware*: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido;

- Engenharia Social:
  - *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.
- Fraudes Externas e Invasões: Realização de operações por fraudadores, utilizando-se de ataques em contas bancárias, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico;
- Ataques DDoS e *Botnets*: Ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos *Botnets*, o ataque vem de muitos computadores infectados utilizados para criar e enviar "spam" ou vírus ou inundar uma rede com mensagens, resultando na negação de serviços.

Ações de prevenção e proteção

A gestora adota regras para concessão de senhas de acesso a dispositivos corporativos, sistemas e rede, em função da relevância para acesso à sede e à rede, incluindo aos servidores.

Os eventos de login e alteração de senhas são auditáveis e rastreáveis, e o acesso remoto a arquivos e sistemas internos ou na nuvem têm controles adequados.

Ao incluir novos equipamentos e sistemas em produção, a gestora deverá garantir que sejam feitas configurações seguras de seus recursos. Devem ser feitos testes em ambiente de homologação e de prova de conceito antes do envio à produção.

A gestora conta com recursos *anti-malware* em estações e servidores de rede como antivírus e *firewalls* pessoais.

A gestora realiza também, "*backup*" das informações e dos diversos ativos da instituição, conforme o plano de contingência e de continuidade do negócio.

Monitoramento e testes

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

Periodicamente, a WISE ASSET realiza testes de segurança no seu sistema de segurança da informação e proteção de dados. Seguem abaixo algumas dessas medidas:

- Verificação dos logs dos colaboradores;
- Alteração periódica de senha de acesso dos colaboradores;
- Segregação de acessos;
- Manutenção trimestral de todos os *hardwares*;
- "*Backup*" diário, realizado na nuvem.

O "*backup*" de todas as informações armazenadas nos servidores será realizado na forma descrita no plano de contingência e continuidade de negócios da gestora, com vistas a evitar a perda de informações, e viabilizando sua recuperação em situações de contingência.

As rotinas de "*backup*" são periodicamente monitoradas.

Plano de resposta

Havendo indícios ou de suspeita fundamentada, a WISE ASSET deverá ser acionada para realizar os procedimentos necessários de modo a identificar o evento ocorrido. Os procedimentos a serem aplicados poderão variar de acordo com a natureza e o tipo do evento.

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

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

A responsabilidade de implantação e monitoramento desses procedimentos é da área de gestão de Risco e *Compliance*.

Segurança quanto às pessoas

Este tópico trata da segurança quanto às pessoas e tem como finalidade reduzir os riscos de erros humanos, roubo, fraude ou uso inadequado de informações e recursos da WISE ASSET.

Identificação das Pessoas: Todas as pessoas com acesso aos sistemas e informações, pertencentes ou em posse da WISE ASSET, deverão ter uma identificação (login). As exceções deverão ser devidamente documentadas e aprovadas pela Diretoria.

Normas Para Controle de Acesso a Computadores, Redes e Sistemas: Este item trata do controle de acesso aos sistemas e às informações pertencentes ou de posse da WISE ASSET. Um sistema efetivo de controle de acesso deve ser utilizado para autenticar os usuários. As principais características desse controle são:

- O acesso a computadores e redes deve ser protegido por senha;
- As senhas devem ser individuais e intransferíveis. A senha é de uso exclusivo, pessoal e intransferível, sendo o compartilhamento proibido em quaisquer circunstâncias;
- As senhas não devem ser triviais e previsíveis;
    - Os tipos de caracteres utilizados para a formação da senha devem ser:

1. Letras maiúsculas;

2. Letras minúsculas;

3. Números; e

4. Sinais ou símbolos especiais (Ex: @ # $ % & * - + = “ ´ ` ^ ~ { } [ ] / | \ ? !).

As senhas deverão ter um tamanho mínimo de 06 (seis) caracteres, sendo obrigatória a utilização de no mínimo três dos quatro tipos de caracteres acima definidos, sendo mandatário o uso de no mínimo um sinal ou símbolo especial;

As senhas devem ser alteradas no prazo de no máximo 5 (cinco) meses.

a) Monitorar o enquadramento dos fundos em cada limite atribuído;

b) Assegurar a identificação, a mitigação e o gerenciamento contínuo dos riscos, em consonância com as diretrizes internas e órgãos reguladores;

c) Ter metodologias de gestão de riscos que suportem os processos, os negócios e a tomada de decisão;

d) Estabelecer e revisar periodicamente limites, políticas e procedimentos específicos;

e) Assegurar que a estrutura está sendo implementada de acordo com os padrões mínimos definidos.

5.2.2. Sigilo

O tratamento das informações de uma empresa, de seus associados, de clientes e de provedores é parte crítica na administração desta empresa.

No setor financeiro, a confidencialidade de qualquer informação que não é de domínio público, tem caráter especial de grande impacto, o que exige maior cuidado.

Com o acesso e a integração de diversos meios de comunicação e informática é necessária a formação de uma política de segurança baseada em três pilares:

- Elaboração de procedimentos operacionais relacionadas à infraestrutura (*Software* e *Hardware*);
- Capacitação de pessoal (Treinamento);
- Criação de compromisso (Acordos de Confidencialidade).

5.2.2.1. Elaboração de Procedimento Operacionais

Entre os procedimentos operacionais destacamos:

- <u>O uso de software e do acesso de usuários</u>
    - A utilização do correio eletrônico (e-mail) ou qualquer outro meio de comunicação via internet (Skype, Email entre outros) deve ser de uso profissional. É proibida a divulgação de mensagens com conteúdo religioso, racial, pornográfico ou político. A utilização de webmail deve ser controlada por um administrador. Todo cuidado deve ser tomado ao receber arquivos suspeitos de se conter vírus;
    - Criação de filtros nos mecanismos eletrônicos de comunicação;
    - Criptografia na transmissão de arquivos de computador;
    - Proteção contra vírus existentes com o uso de softwares de prevenção que devem ser usados no servidor de rede. Periodicamente serão verificados todos os discos de armazenamento de dados ("*hard-disks*") de todos os computadores;
    - Controle de acesso em que todo usuário terá uma chave de acesso à rede (login) exclusiva que identifica claramente seu detentor, acompanhada de senha de acesso controlada pela área de Informática. O supervisor da rede será o único autorizado a atribuir chaves e senhas de acesso para os usuários da rede. O perfil do usuário determinará o nível de acesso;
    - Troca periódica de senhas de acesso;
    - Segurança de arquivos: diariamente serão realizados backups de todos os arquivos de dados salvos na rede (base de dados, planilhas, textos entre outros).

- Hardware – Proteção e Segurança

  - Local de instalação de hardware deve possuir proteção dos raios solares, de altas temperaturas e de incidência de poeira;
  - Instalação elétrica: é necessária a presença de "*no-breaks*" corretamente dimensionados para a falta de energia elétrica (para salvamento de dados e desligamento correto) e manutenção de uniformidade de tensão de rede;
  - Servidor: sala do servidor deverá possuir acesso restrito às pessoas autorizadas;
  - "*Backup*" externo: os arquivos de *backup* e a documentação dos sistemas devem ser armazenados em lugar diferente ao do escritório, em lugar seguro e de acesso restrito a funcionários autorizados;
  - Telefonia – gravações digitais ou em CDs de ligações telefônicas originadas ou recebidas em mesas de operações para consulta;
  - Internet – presença de mais de um provedor em meios diferentes (*wireless* e cabo);
  - Uso de equipamentos de impressão aprovados pela WISE ASSET, máquinas de fotocópia e de mecanismos eletrônicos de disseminação de informações, tais como e-mails da companhia e pessoais, internet, mensagens eletrônicas e rede de relacionamentos entre outros, no sentido de que as informações sejam expostas ou reproduzidas somente em equipamentos de acesso restrito e que sejam transmitidas somente por mecanismos eletrônicos autorizados, devidamente protegidos de possíveis invasões externas, de forma a evitar a disseminação irrestrita de informações.

5.2.2.2. Capacitação Pessoal e Treinamento

O treinamento acima referido deve ser dado aos empregados da companhia que, em virtude do cargo ou da função que ocupam, tenham acesso a informações privilegiadas, neles compreendidos não apenas os que participem de processos técnicos,

operacionais ou decisórios, mas também aqueles que atuem em procedimentos auxiliares.

5.2.2.3. Adoção de Comportamento Seguro

As informações sigilosas podem ser encontradas na sede da Gestora e fazem parte do ambiente de trabalho de todos os colaboradores. Portanto, é fundamental para a proteção delas que os colaboradores adotem comportamento seguro e consistente, com destaque para os seguintes itens:

- A atitude proativa e engajada dos colaboradores no que diz respeito à proteção das informações sigilosas;
- Compreensão que as ameaças externas podem afetar a segurança das informações sigilosas, tais como vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos, bem como fraudes destinadas a roubar senhas de acesso aos sistemas de tecnologia da informação em uso e aos servidores;
- Assuntos relacionados ao desempenho de atividades e funções na WISE ASSET não devem ser discutidos em ambientes públicos ou em áreas expostas como: meios de transporte, locais públicos, encontros sociais;
- As senhas de acesso do colaborador aos sistemas da WISE ASSET são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive a outros colaboradores), anotadas em papel ou em sistema visível ou de acesso não protegido;
- Os computadores devem ser bloqueados sempre que o colaborador se ausentar de sua estação de trabalho;
- Arquivos eletrônicos de origem desconhecida não devem ser abertos e/ou executados nos computadores da empresa;
- Mensagens eletrônicas e seus anexos são para uso exclusivo do remetente e destinatário e podem conter informações sigilosas;
- O acesso remoto à rede, às informações sigilosas e sistemas da gestora somente será permitido mediante autorização da área de Compliance e Risco;

- Documentos impressos e arquivos contendo informações sigilosas devem ser adequadamente armazenados e protegidos, sendo vedada a retirada da sede da gestora sem a autorização prévia.

5.2.2.4. Gestão de Acesso a Sistemas de Informação e a Ambientes Lógicos

Todo acesso às informações sigilosas, aos ambientes lógicos deve ser controlado, de forma a garantir acesso apenas às pessoas expressamente autorizadas pela Área de Risco e de Compliance.

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

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

5.2.2.5. Utilização de Internet

O uso da Internet deve restringir-se às atividades relacionadas aos negócios e serviços da WISE ASSET e para a obtenção de informações e dados necessários ao desempenho dos trabalhos.

5.2.2.6. Sites da Internet

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

5.2.3. Lei Geral de Proteção de Dados Pessoais ("LGPD")

Além de todos os procedimentos já adotados no que se refere ao sigilo, a WISE ASSET também possui preocupação com os dados pessoais que trata.

Neste sentido, a empresa tem o objetivo de assegurar a segurança das informações, ao tempo que não impeçam e/ou dificultem o processo do negócio, mas que garantam:

- A confiabilidade das informações através da preservação da confidencialidade, integridade e disponibilidade dos dados;
- O compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda de acordo com a legalidade e as boas práticas mundiais, a fim de mitigar riscos técnicos e jurídicos;
- A definição de procedimentos específicos de Segurança da Informação e a implementação de controles e processos para o atendimento de seus requisitos;
- A participação e cumprimento por todos os colaboradores em todo o processo.

Logo, é prática obrigatória na WISE ASSET:

- Utilização dos equipamentos de informática, de comunicação, os sistemas e as informações devem ser utilizados para a realização de atividades profissionais, com senso de responsabilidade e preceitos éticos, dentro da legalidade;
- Respeito à privacidade dos usuários, agindo de forma ética e atendendo aos princípios da Lei Geral de Proteção de Dados Pessoais;
- Atuação com transparência, prestando informações confiáveis, relevantes e tempestivas à sociedade, garantindo o sigilo das informações e dados imprescindíveis à segurança dos indivíduos, bem como a inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas.

Por isso, a WISE ASSET reserva-se o direito de monitorar e registrar todo e qualquer uso das informações geradas, armazenadas ou veiculadas na instituição. Para tanto, são criados e implantados controles apropriados, registros de atividades em todos os pontos e sistemas julgados necessários para reduzir os riscos, pautando-se na ética e na legalidade.

5.2.3.1. Normas para Tratamento da Informação

Devem ser definidas regras claras para proteção da informação contra perda, alteração e acesso por pessoas não autorizadas, seja qual for o meio em que vier a ser armazenada (magnético, correspondências, relatórios, manuscritos etc.).

Os usuários (empresas, áreas, pessoas etc.) das informações precisam ser claramente definidos, isto é, os direitos que cada um tem para acessá-las e os procedimentos para protegê-las do acesso por pessoas não-autorizadas, independentemente da forma como estiver disponível.

Toda informação deve ser utilizada apenas para fins de interesse exclusivo da WISE ASSET.

Toda informação relevante deve ter pelo menos uma cópia reserva ou outro procedimento eficiente para pronta recuperação em caso de perda.

Nenhuma informação deve ser acessada, divulgada ou disponibilizada, sob qualquer pretexto, sem a devida autorização.

É proibida a transmissão a terceiros, por qualquer meio, bem como sua divulgação, reprodução, cópia, utilização ou exploração de conhecimentos, dados e informações de propriedade da Instituição, sem a prévia e expressa autorização da Diretoria responsável, estendendo-se tal vedação ao período após o término do contrato de trabalho, sem prejuízo das ações de natureza penal aplicáveis ao assunto.

5.2.3.2. Recomendações para o Tratamento de Informações

A pessoa que receber indevidamente uma informação deve procurar imediatamente o remetente e alertá-lo sobre o equívoco.

As informações disponíveis na Internet somente deverão ser acessadas para fins de execução das atividades de interesse exclusivo da WISE ASSET.

Toda informação em papel, mídia removível ou qualquer outro meio de armazenamento deve ser destruída após o uso, ou guardada de forma a não estar disponível para pessoas não autorizadas.

As manutenções em equipamentos que armazenem informações devem ser acompanhadas por um representante da área sempre que esse equipamento estiver em

uso ou logado com a credencial do funcionário que necessita do suporte. Quando forem vendidos, devolvidos ao fabricante, enviados para manutenção ou deslocados para outros usuários, as informações neles contidas deverão ser destruídas antes da liberação do equipamento.

5.2.3.3. Proteção de Dados Pessoais

A WISE ASSET em atendimento e respeito à Lei Geral de Proteção de Dados Pessoais deverá garantir a disponibilidade, integridade e confidencialidade dos dados pessoais, em todo seu ciclo de vida, sendo esta categoria de dados tratados de forma permanente como dados confidenciais.

Todo tratamento de dados pessoais deverá estar atrelado a uma finalidade específica, informada ao titular e devidamente atrelada a uma ou mais bases legais previstas nos artigos 7º e 11º da Lei Geral de Proteção de Dados Pessoais, atentando-se aos princípios da necessidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e prestação de contas.

O detalhamento dos requisitos e regras para tratamento de dados pessoais serão disponibilizados em norma específica, sendo necessário que todos os colaboradores e prestadores de serviços tomem ciência e sejam sensibilizados sobre o tema e a respectiva norma.

Toda e qualquer alteração ou criação de sistemas, serviços ou produtos que envolvam tratamento de dados pessoais deverão aplicar o “Privacy by Design / Privacidade desde a concepção”.

6. PENALIDADES

Os membros da estrutura organizacional que não observarem as diretrizes e as obrigações dessa política, bem como as normas e procedimentos correlatos, por negligência, culpa ou dolo, estão sujeitos a ações disciplinares, além das penalidades previstas em lei.

7. VIGÊNCIA

Essa norma entra em vigor na data de sua publicação e vigorará por prazo indeterminado, devendo ser atualizada sempre que a área responsável entender necessário ou quando da ocorrência de alteração da regulação ou legislação pertinente.

8. HISTÓRICO DE REVISÕES

VERSÃO	DATA DE REVISÃO	DESCRIÇÃO
1	12/2020	Atualização de fim de exercício
2	12/2021	Atualização de fim de exercício
3	12/2022	Atualização de fim de exercício

9. APROVAÇÕES

MEMBRO	ASSINATURA
André Luis Sartori Ribeiro	
Rhuan Rosa	

PG - 20.06.2024 - Segurança cibernética, Sigilo e LGPD.pdf

Documento número #a5367584-40fc-42b5-b370-1a3426e953be

Hash do documento original (SHA256): 377cf2099242ea889e67a5422f7c6e57254b124fc30d19d1370405648933fa40

Assinaturas

André Luis Sartori Ribeiro
CPF: 009.434.400-09
Assinou como diretor(a) em 02 jul 2024 às 12:23:16

Rhuan Rosa
CPF: 346.770.538-39
Assinou como diretor(a) em 27 jun 2024 às 11:26:34

Log

27 jun 2024, 10:44:32	Operador com email compliance@wiseasset.com.br na Conta e6c16605-ac06-45d7-b33c-1337523099e1 criou este documento número a5367584-40fc-42b5-b370-1a3426e953be. Data limite para assinatura do documento: 27 de julho de 2024 (10:40). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
27 jun 2024, 10:44:33	Operador com email compliance@wiseasset.com.br na Conta e6c16605-ac06-45d7-b33c-1337523099e1 adicionou à Lista de Assinatura: andre.ribeiro@wiseasset.com.br para assinar como diretor(a), via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo André Luis Sartori Ribeiro e CPF 009.434.400-09.
27 jun 2024, 10:44:33	Operador com email compliance@wiseasset.com.br na Conta e6c16605-ac06-45d7-b33c-1337523099e1 adicionou à Lista de Assinatura: rhuan.rosa@wiseasset.com.br para assinar como diretor(a), via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Rhuan Rosa e CPF 346.770.538-39.
27 jun 2024, 11:26:34	Rhuan Rosa assinou como diretor(a). Pontos de autenticação: Token via E-mail rhuan.rosa@wiseasset.com.br. CPF informado: 346.770.538-39. IP: 200.233.244.17. Componente de assinatura versão 1.898.1 disponibilizado em https://app.clicksign.com.
02 jul 2024, 12:23:17	André Luis Sartori Ribeiro assinou como diretor(a). Pontos de autenticação: Token via E-mail andre.ribeiro@wiseasset.com.br. CPF informado: 009.434.400-09. IP: 170.246.128.254. Localização compartilhada pelo dispositivo eletrônico: latitude -28.6728535 e longitude -49.3754793. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.900.2 disponibilizado em https://app.clicksign.com.

02 jul 2024, 12:23:17	Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número a5367584-40fc-42b5-b370-1a3426e953be.

Documento assinado com validade jurídica.
Para conferir a validade, acesse https://www.clicksign.com/validador e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº a5367584-40fc-42b5-b370-1a3426e953be, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.