



MARRUA GESTORA DE RECURSOS LTDA.

POLÍTICA DE SEGURANÇA CIBERNÉTICA, PRIVACIDADE E PROTEÇÃO DE DADOS

("Política")

Data da Aprovação	Fevereiro/2026
Área responsável	Compliance
Elaborado por	Área de Compliance
Escopo	Todos os Colaboradores e Pessoas Ligadas da Marrua, conforme aplicável

Versão 1 — Fevereiro de 2026

Esta Política é propriedade da Marrua Gestora de Recursos Ltda. e não está autorizada a cópia, uso ou distribuição deste documento e seu conteúdo sob nenhuma hipótese.

SUMÁRIO

Capítulo 1 — Disposições Preliminares	3
1.1. Objetivo.....	3
1.2. Base Legal.....	3
1.3. Princípios Gerais	4
Capítulo 2 — Coleta, Tratamento e Compartilhamento de Dados	4
2.1. Meios de Coleta.....	4
2.2. Dados Pessoais Coletados	5
2.3. Dados Pessoais Sensíveis	5
2.4. Dados de Crianças e Adolescentes.....	5
2.5. Finalidades do Tratamento	6
2.6. Consentimento.....	6
2.7. Compartilhamento de Dados.....	6
2.8. Transferência Internacional de Dados.....	7
2.9. Armazenamento e Período de Retenção.....	7
2.10. Direitos dos Titulares	7
2.11. Encarregado pelo Tratamento de Dados Pessoais.....	8
Capítulo 3 — Segurança Cibernética e da Informação.....	8
3.1. Objetivo e Escopo	8
3.2. Classificação da Informação	9
3.3. Controles de Acesso	9
3.4. Proteção de Dados e Sistemas	9
3.5. Backup e Continuidade	10
3.6. Segurança no Compartilhamento com a BFL	10
3.7. Utilização de Recursos Tecnológicos	10
Capítulo 4 — Resposta a Incidentes de Segurança.....	11
4.1. Identificação e Comunicação	11
4.2. Avaliação e Contenção.....	11
4.3. Comunicação à ANPD e aos Titulares	11
4.4. Registro de Incidentes	11
4.5. Lições Aprendidas.....	12
Capítulo 5 — Treinamento e Conscientização	12
Capítulo 6 — Aviso Legal	12
Capítulo 7 — Disposições Gerais	13
Capítulo 8 — Histórico de Versões	13
Capítulo 9 — Responsáveis pelo Documento e Aprovação	13

Capítulo 1 — Disposições Preliminares

1.1. Objetivo

A presente Política consolida as diretrizes de segurança cibernética, privacidade e proteção de dados pessoais adotadas pela Marrua Gestora de Recursos Ltda. (“Marrua” ou “Gestora”), CNPJ 30.946.485/0001-71, reafirmando o compromisso institucional com a salvaguarda das informações e a observância da legislação de proteção de dados.

Esta Política complementa as disposições de confidencialidade contidas no Código de Ética e Conduta e no Manual de Controles Internos da Gestora, que permanecem como documentos norteadores dos princípios éticos e operacionais.

O documento aplica-se a todas as pessoas físicas que mantenham relacionamento com a Marrua, incluindo: investidores dos Fundos de Investimento em Direitos Creditórios (FIDC), Fundos de Investimento em Participações (FIP) e Fundos de Investimento Multimercado (FIM) sob gestão; cotistas em potencial; cedentes e sacados de operações de crédito dos FIDC; prestadores de serviços; colaboradores; candidatos a vagas de emprego; representantes de contrapartes; e demais terceiros que interajam com a Gestora.

A Marrua atua exclusivamente como gestora de recursos de terceiros. As atividades de administração fiduciária são exercidas pela BFL Administradora de Títulos e Valores Mobiliários Ltda. (“BFL”), integrante do mesmo grupo econômico. As atividades de custódia e escrituração são exercidas por instituições terceiras habilitadas.

1.2. Base Legal

Esta Política encontra fundamento nas seguintes normas:

- (i) Lei Federal nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (“LGPD”);
- (ii) Resolução CVM nº 21, de 25 de fevereiro de 2021, conforme alterada (“RCVM 21”);
- (iii) Resolução CVM nº 175, de 23 de dezembro de 2022, conforme alterada (“RCVM 175”);
- (iv) Resolução CVM nº 50, de 31 de agosto de 2021, conforme alterada (“RCVM 50”);
- (v) Código ANBIMA de Administração e Gestão de Recursos de Terceiros (“Código AGRT”), em especial o artigo 49;
- (vi) Código ANBIMA de Ética; e
- (vii) demais leis e regulamentações que impõem obrigações de identificação, cadastro e manutenção de informações.

1.3. Princípios Gerais

A Marrua reconhece a privacidade como direito fundamental de todos os titulares de dados pessoais, comprometendo-se a adotar medidas técnicas e organizacionais proporcionais ao seu porte e à natureza de suas atividades para assegurar a proteção das informações coletadas e tratadas.

Todas as informações pessoais são tratadas em conformidade com os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização.

A Gestora mantém procedimentos de treinamento periódico junto aos seus colaboradores sobre a importância da proteção de dados pessoais e as práticas adequadas para sua salvaguarda.

Capítulo 2 — Coleta, Tratamento e Compartilhamento de Dados

2.1. Meios de Coleta

A Marrua pode coletar dados pessoais por diferentes meios:

- a) fornecimento direto pelo titular, por meio de formulários, questionários, correspondências eletrônicas, contratos e documentos;
- b) cadastro junto a prestadores de serviços, incluindo a BFL (administradora fiduciária), distribuidores e plataformas de investimento;
- c) fontes públicas, registros oficiais e bases de dados disponibilizadas por órgãos competentes; e
- d) terceiros autorizados, inclusive cedentes de direitos creditórios no âmbito dos FIDC.

2.2. Dados Pessoais Coletados

No exercício de suas atividades, a Gestora poderá coletar:

- a) dados cadastrais e de identificação: nome completo, CPF, RG, data de nascimento, nacionalidade, estado civil, profissão, endereço, telefone, e-mail, informações sobre representantes legais e procuradores;
- b) dados financeiros e patrimoniais: informações sobre renda, patrimônio, origem dos recursos, declarações fiscais, extratos e comprovantes necessários aos processos de KYC;
- c) dados profissionais: histórico profissional, vínculo empregatício, cargo, experiência em investimentos, qualificação como investidor;
- d) dados de cedentes e sacados: no âmbito dos FIDC, informações cadastrais e financeiras de cedentes de direitos creditórios e de sacados/devedores dos créditos adquiridos, necessárias à análise de crédito e ao monitoramento da carteira; e
- e) dados de identificação digital: endereço IP, dados de navegação, registros de acesso aos sistemas, quando aplicável e no âmbito de sistemas próprios ou plataformas sob controle da Gestora.

2.3. Dados Pessoais Sensíveis

A Marrua não coleta dados pessoais sensíveis (origem racial, convicção religiosa, opinião política, dados de saúde, dados genéticos ou biométricos) para a prestação de seus serviços de gestão de recursos. Excepcionalmente, tais dados poderão ser coletados em processos seletivos para vagas de emprego, mediante consentimento específico, ou quando necessário para cumprimento de obrigação legal.

2.4. Dados de Crianças e Adolescentes

Os serviços prestados pela Marrua são destinados a pessoas maiores de idade. A Gestora não coleta intencionalmente dados pessoais de crianças ou adolescentes.

2.5. Finalidades do Tratamento

A Marrua realiza o tratamento de dados pessoais para finalidades lícitas, específicas e informadas aos titulares:

- a) cumprimento de obrigações regulatórias e legais perante CVM, ANBIMA, Receita Federal, COAF e demais órgãos, incluindo PLD/FTP, identificação de beneficiários finais e KYC;
- b) execução de contratos e prestação de serviços de gestão de carteiras, incluindo comunicação com cotistas, envio de informes e relatórios;
- c) processo de cadastro e verificação de identidade para estabelecimento de relacionamento;
- d) análise de crédito no âmbito dos FIDC, incluindo avaliação de cedentes, sacados e direitos creditórios;
- e) análise de adequação (suitability), quando aplicável;
- f) comunicações institucionais, com base no consentimento ou no legítimo interesse;
- g) prevenção a fraudes e segurança dos sistemas e operações; e
- h) exercício regular de direitos em processos judiciais, administrativos ou arbitrais.

2.6. Consentimento

Quando a base legal for o consentimento, este será obtido de forma livre, informada, inequívoca e específica. O consentimento poderá ser revogado a qualquer momento, sem prejuízo da legalidade do tratamento anterior. A revogação não afeta tratamentos fundamentados em outras bases legais.

2.7. Compartilhamento de Dados

A Marrua poderá compartilhar dados pessoais nas seguintes hipóteses:

- a) BFL (administradora fiduciária do grupo): para cumprimento de obrigações contratuais, regulatórias e operacionais relativas aos Fundos, observados os princípios de segregação e confidencialidade previstos na Política de Prevenção a Conflitos de Interesse;
- b) custodiantes e escrituradores: para fins de cumprimento das obrigações operacionais dos Fundos;

-
- c) órgãos reguladores e autorreguladores: CVM, ANBIMA, Banco Central, COAF e Receita Federal, em cumprimento de obrigações legais;
 - d) autoridades judiciais, policiais ou administrativas: mediante ordem judicial ou requisição formal;
 - e) prestadores de serviços contratados: auditores, consultores jurídicos, consultores especializados dos FIDC, empresas de tecnologia e agentes de cobrança;
 - f) contrapartes em operações de investimento: quando necessário para execução de operações dos Fundos; e
 - g) distribuidores e plataformas de investimento: para fins de distribuição das cotas e cumprimento de suitability.

A Marrua exige de seus prestadores de serviços e parceiros compromisso contratual com a proteção de dados pessoais e o cumprimento da legislação aplicável.

2.8. Transferência Internacional de Dados

O tratamento de dados pessoais é realizado predominantemente em território nacional. Eventualmente, poderá haver transferência internacional para países que proporcionem grau de proteção adequado ou mediante adoção de cláusulas contratuais específicas, conforme previsto na LGPD.

2.9. Armazenamento e Período de Retenção

Os dados pessoais serão armazenados pelo período necessário ao cumprimento das finalidades para as quais foram coletados, observados os prazos de guarda estabelecidos na legislação e regulamentação aplicáveis ao mercado de capitais.

Após o término do tratamento, os dados serão eliminados, ressalvada a conservação para: (a) cumprimento de obrigação legal; (b) estudo por órgão de pesquisa, garantida a anonimização; (c) transferência a terceiro nos termos da lei; ou (d) uso exclusivo do controlador, vedado acesso por terceiro e desde que anonimizados.

2.10. Direitos dos Titulares

Em conformidade com a LGPD, os titulares têm os seguintes direitos, exercíveis mediante requisição à Marrua:

- a) confirmação da existência de tratamento;
- b) acesso aos dados pessoais tratados;
- c) correção de dados incompletos, inexatos ou desatualizados;
- d) anonimização, bloqueio ou eliminação de dados desnecessários ou excessivos;
- e) portabilidade dos dados a outro fornecedor;
- f) eliminação dos dados tratados com base no consentimento;
- g) informação sobre entidades com as quais os dados foram compartilhados;
- h) informação sobre a possibilidade de não fornecer consentimento e suas consequências; e
- i) revogação do consentimento.

2.11. Encarregado pelo Tratamento de Dados Pessoais

A Marrua designou o Diretor de Compliance como Encarregado pelo Tratamento de Dados Pessoais (Data Protection Officer — DPO), responsável por atuar como canal de comunicação entre a Gestora, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Para esclarecimentos, dúvidas ou solicitações relacionadas ao tratamento de dados pessoais: compliance@marruagestora.com.br.

Capítulo 3 — Segurança Cibernética e da Informação

3.1. Objetivo e Escopo

Este capítulo estabelece as diretrizes de segurança cibernética e da informação da Marrua, proporcionais ao porte da Gestora e à criticidade das informações sob seu controle. As medidas aqui descritas visam prevenir, detectar e responder a ameaças que possam comprometer a confidencialidade, integridade e disponibilidade dos dados e sistemas.

Este capítulo aplica-se a todos os colaboradores, diretores, estagiários e prestadores de serviços que acessem os sistemas, redes ou informações da Gestora.

3.2. Classificação da Informação

As informações sob responsabilidade da Marrua são classificadas nos seguintes níveis:

- a) **Confidencial:** informações cuja divulgação não autorizada pode causar dano relevante à Gestora, aos Fundos ou aos investidores. Incluem: estratégias de investimento, dados de carteira, informações privilegiadas, dados pessoais de investidores e de cedentes/sacados dos FIDC;
- b) **Interna:** informações de uso restrito aos colaboradores e prestadores de serviços autorizados. Incluem: políticas internas, relatórios gerenciais, atas de comitês; e
- c) **Pública:** informações destinadas à divulgação ao público em geral. Incluem: materiais de divulgação, informes publicados e políticas disponibilizadas no website.

3.3. Controles de Acesso

A Gestora adota os seguintes controles de acesso:

- a) credenciais individuais e intransferíveis para acesso aos sistemas, com senhas complexas renovadas a cada 90 dias;
- b) princípio do menor privilégio: cada colaborador acessa apenas os sistemas e informações estritamente necessários ao exercício de suas funções;
- c) revisão periódica de acessos, com remoção imediata de credenciais de colaboradores desligados;
- d) autenticação em dois fatores (2FA) para acesso remoto a sistemas críticos; e
- e) registro de logs de acesso aos sistemas que contenham informações confidenciais.

3.4. Proteção de Dados e Sistemas

As medidas de proteção incluem:

- a) criptografia de dados sensíveis em trânsito e em repouso, quando aplicável;
- b) utilização de software antivírus e anti-malware com atualização automática em todos os dispositivos;
- c) firewalls e controles de rede para proteção do perímetro;
- d) atualização periódica de sistemas operacionais e aplicações (patch management);

-
- e) vedação ao uso de dispositivos pessoais não autorizados para acesso a dados dos Fundos; e
 - f) bloqueio automático de estações de trabalho após período de inatividade.

3.5. Backup e Continuidade

A Marrua mantém rotina de backup dos dados críticos, observando:

- a) backup diário em nuvem (OneDrive ou solução equivalente) dos arquivos de trabalho;
- b) cópia redundante em dispositivo físico (HD externo), armazenado em local seguro e segregado;
- c) testes periódicos de restauração para validação da integridade dos backups; e
- d) procedimentos de recuperação detalhados no Plano de Continuidade de Negócios da Gestora.

3.6. Segurança no Compartilhamento com a BFL

O compartilhamento de informações entre a Marrua e a BFL (administradora fiduciária do grupo) observará:

- a) limitação ao estritamente necessário para o cumprimento de obrigações regulatórias e operacionais;
- b) transmissão por canais seguros e criptografados;
- c) vedação ao compartilhamento de informações sobre estratégias de investimento, ordens pendentes ou quaisquer dados que possam comprometer a segregação funcional; e
- d) registro das transferências de dados realizadas, para fins de auditoria e rastreabilidade.

3.7. Utilização de Recursos Tecnológicos

Os recursos tecnológicos disponibilizados pela Marrua (computadores, e-mail, internet, sistemas de gestão) destinam-se exclusivamente ao exercício das atividades profissionais. São vedados:

- a) instalação de softwares não autorizados;
- b) acesso a conteúdos ilícitos, ofensivos ou não relacionados às atividades da Gestora;

-
- c) utilização de e-mail pessoal para envio ou recebimento de informações confidenciais; e
 - d) transferência de arquivos corporativos para dispositivos ou contas pessoais sem autorização do Compliance.

Capítulo 4 — Resposta a Incidentes de Segurança

4.1. Identificação e Comunicação

Qualquer colaborador que identifique ou suspeite de incidente de segurança — incluindo acesso não autorizado, vazamento de dados, malware, phishing ou perda de dispositivos — deve comunicar imediatamente ao Diretor de Compliance.

4.2. Avaliação e Contenção

O Diretor de Compliance, em conjunto com o Analista de TI e a Diretoria, avaliará:

- a) a natureza, a categoria e a quantidade de titulares potencialmente afetados;
- b) os riscos envolvidos e o potencial de dano;
- c) as medidas de contenção imediata e de mitigação; e
- d) a necessidade de comunicação à ANPD e aos titulares afetados.

4.3. Comunicação à ANPD e aos Titulares

Caso o incidente possa acarretar risco ou dano relevante aos titulares, a Gestora comunicará à ANPD e aos titulares afetados em prazo razoável, nos termos do artigo 48 da LGPD, informando, no mínimo:

- a) descrição da natureza dos dados pessoais afetados;
- b) informações sobre os titulares envolvidos;
- c) medidas técnicas e de segurança adotadas para proteção dos dados;
- d) riscos relacionados ao incidente; e
- e) medidas adotadas ou a serem adotadas para reverter ou mitigar os efeitos.

4.4. Registro de Incidentes

Todos os incidentes de segurança, independentemente de gravidade, serão registrados em documento interno contendo: descrição do evento, avaliação de impacto, medidas adotadas e decisão fundamentada quanto à comunicação ou não à ANPD. Os procedimentos operacionais detalhados encontram-se no Manual de Controles Internos.

4.5. Lições Aprendidas

Após a resolução de cada incidente, o Diretor de Compliance elaborará relatório de lições aprendidas, identificando vulnerabilidades exploradas e recomendando ajustes nos controles. As recomendações serão implementadas pelo Analista de TI e validadas pela Diretoria.

Capítulo 5 — Treinamento e Conscientização

A Marrua promoverá treinamento anual de todos os colaboradores sobre segurança da informação e proteção de dados pessoais, abrangendo:

- a) conceitos fundamentais da LGPD e responsabilidades dos colaboradores;
- b) boas práticas de segurança cibernética (senhas, phishing, engenharia social);
- c) procedimentos de resposta a incidentes; e
- d) atualizações regulatórias relevantes.

Novos colaboradores receberão treinamento específico no processo de integração. Os registros de participação serão mantidos pelo Compliance pelo período mínimo de 5 anos.

Capítulo 6 — Aviso Legal

A Marrua não será responsável pelo uso indevido ou perda de dados pessoais sobre os quais não possua controle ou acesso. Também não se responsabiliza por eventual uso ilícito de informações decorrente de conduta culposa ou dolosa dos próprios titulares ou de terceiros não vinculados à Gestora.

Cabe aos titulares adotar medidas adequadas para proteção de suas credenciais, comunicando imediatamente à Gestora qualquer uso não autorizado ou violação de segurança, ressalvadas as hipóteses de falha nos controles sob responsabilidade da Marrua.

Esta Política não se aplica a websites, aplicativos, plataformas ou serviços de terceiros acessíveis por meio dos canais da Gestora.

Capítulo 7 — Disposições Gerais

Esta Política, após aprovação pela Diretoria, deve ser registrada na ANBIMA em sua versão integral e atualizada, nos termos do artigo 49 do Código AGRT e do artigo 50 do mesmo Código, e encontra-se disponível para consulta no website da Marrua.

Nos termos do artigo 49 do Código AGRT, na eventual hipótese de compartilhamento de dados pessoais com a ANBIMA, a Marrua garantirá a atualização das informações e a transparência para com os titulares envolvidos.

A revisão desta Política ocorrerá com periodicidade mínima anual, ou sempre que houver alteração legal ou regulatória relevante. Alterações serão comunicadas aos interessados pelos canais apropriados.

Exceções a esta Política devem ser pré-aprovadas pelo Diretor de Compliance e registradas por escrito.

Capítulo 8 — Histórico de Versões

Data	Descrição
Fev/2026	Versão inicial

Capítulo 9 — Responsáveis pelo Documento e Aprovação

Responsável	Departamento
Elaboração / Revisão	Diretor de Compliance
Aprovação	Diretoria