

TERA4

POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS
Julho de 2026

REGISTRO DE ALTERAÇÕES			
Versão	Item Modificado	Modificação	Data
1	Versão original	-	01/2021
2	Adição de itens	Adição de novos temas	09/2022
3	Revisão geral	Revisão geral	07/2026

Sumário

1. Definições Gerais 1.1 Objetivo e Abrangências 1.2 Embasamento Regulatório 1.3 Principais Definições e Responsabilidades	4
2. Tratamento de Dados Pessoais pela Tera 2.1 Princípios Aplicados ao Tratamento de Dados Pessoais 2.2 Fontes de Obtenção dos Dados Pessoais 2.2.1. Dados Pessoais Recebidos de Forma Incidental ou Não Solicitado 2.3 Finalidades do Tratamento e Bases Legais de Tratamento de Dados Pessoais 2.3.1. Bases Legais Não Aplicáveis às Atividades da Tera 2.4 Requisitos Específicos Por Base Legal 2.4.1. Cumprimento de Obrigação Legal e/ou Regulatória (art. 7º, II, LGPD) 2.4.2. Execução de Contrato e Procedimentos Preliminares (Art. 7º, V, LGPD) 2.4.3. Exercício Regular de Direitos (art. 7º, VI, LGPD) 2.4.4. Legítimo Interesse (arts. 7º, IX, e 10, LGPD) 2.4.5. Consentimento (arts. 7º, I, e 8º, LGPD) 2.5 Uso Compartilhado de Dados, Operadores e Terceiros 2.6 Dados Pessoais Sensíveis 2.7 Gravação de Reuniões, Transcrição e Ferramentas de Inteligência Artificial 2.8 Retenção e Eliminação dos Dados Pessoais 2.9 Registro das Operações de Tratamento e Relatório de Impacto 2.10 Segurança do Tratamento	8
3. Direitos dos Titulares dos Dados Pessoais 3.1 Confirmação de Existência e Acesso aos Dados Pessoais 3.2 Correção de Dados Pessoais 3.3 Anonimização, Bloqueio ou Eliminação dos Dados Pessoais 3.4 Portabilidade dos Dados Pessoais 3.5 Eliminação dos Dados Pessoais Tratados com Consentimento 3.6 Informações Sobre o Compartilhamento de Dados Pessoais 3.7 Oposição ao Tratamento 3.8 Revisão de Decisões Automatizadas 3.9 Informações sobre a Negativa de Consentimento e Petição à ANPD 3.10 Forma de Solicitação e Prazo de Resposta	16
4. Respostas a Incidentes de Segurança 4.1 Objetivo	18

4.2 Prazo Aplicável	
4.3 Fluxo Interno de Resposta a Incidentes	
4.3.1. Visão Geral	
4.3.2. Etapas do Fluxo	
5. Transferência Internacional dos Dados	20
6. Penalidades	22
6.1. Governança, Aprovação, Treinamento e Revisão	
7. Anexos	
7.1. Modelos de Comunicação	
7.1.1. Modelo de Comunicação à ANPD	
7.1.2. Modelo de Comunicação aos Titulares	24

1. Definições Gerais

1.1 Objetivo e Abrangências:

A presente Política de Proteção de Dados Pessoais (“Política”) da Tera Investimentos Ltda. (“Gestora” ou “Tera”) visa a atender as diretrizes, as responsabilidades e os procedimentos aplicáveis ao tratamento de dados pessoais de acordo com a Lei nº 13.709/2018, conforme alterações (“Lei Geral de Proteção de Dados Pessoais” ou “LGPD”), no âmbito das atividades exercidas pela Gestora, sem prejuízo de outras providências que se façam necessárias para a integral conformidade com as normas de proteção de dados pessoais, tais como mapeamento de atividades de tratamento de dados pessoais e diagnóstico da maturidade da Gestora com relação à proteção de dados pessoais.

Para esse fim, esta Política define as regras aplicáveis ao mapeamento, à coleta, à utilização, ao compartilhamento, ao armazenamento e à eliminação de dados pessoais, bem como as medidas de governança necessárias para assegurar a conformidade da Tera com a legislação de proteção de dados, devendo ser observada por todos os Colaboradores¹ no desempenho de suas funções.

As regras descritas nesta Política aplicam-se a todo Tratamento de Dados Pessoais realizado pela Gestora, independentemente de os dados terem sido fornecidos pelo próprio Titular ou obtidos junto a terceiros, fontes públicas ou bases de consulta, e alcançam, dentre outros, investidores ou famílias com quem a Gestora possua relacionamento comercial direto (“Clientes” e “Potenciais Clientes”), pessoas naturais vinculadas a fornecedores, prestadores de serviços e contrapartes das operações das carteiras sob gestão (“Prestadores de Serviços e Contrapartes”), Colaboradores, ou pessoas naturais cujos dados sejam tratados no cumprimento de deveres legais e regulatórios de diligência, ainda que não mantenham qualquer relação com a Gestora.

1.2 Embasamento Regulatório

Esta Política tem por embasamento regulatório as normas e regulamentos abaixo indicados, sem prejuízo de outros cujo objeto se relacione à matéria aqui tratada:

- (i) Lei Geral de Proteção de Dados Pessoais;
- (ii) Resolução CVM nº 21/2021 (“RCVM 21”);
- (iii) Resolução CVM nº 50/2021 (“RCVM 50”);
- (iv) Resolução CVM nº 175/2022 (“RCVM 175”);
- (v) Lei nº 9.613/1998 e Lei nº 13.810/2019;
- (vi) Código ANBIMA de Regulação e Melhores Práticas para Administração e Gestão de Recursos de Terceiros;
- (vii) Regras e Procedimentos de Deveres Básicos da ANBIMA;
- (viii) Resolução CD/ANPD² nº 04/2023 (“RANPD 04”);
- (ix) Resolução CD/ANPD nº 15/2024 (“RANPD 15”); e
- (x) Resolução CD/ANPD nº 19/2024 (“RANPD 19”).
- (xi) Resolução CD/ANPD nº 32/2026, que reconhece a União Europeia como organismo internacional com grau de proteção de dados adequado; e

¹ Conforme definido no Manual de Compliance.

² Agência Nacional de Proteção de Dados.

(xii) Lei nº 12.965/2014 (Marco Civil da Internet);

1.3 Principais Definições e Responsabilidades

Os termos definidos empregados nesta Política deverão ser interpretados de acordo com as definições constantes deste documento, de outros manuais e políticas internas da Tera e, subsidiariamente, da legislação aplicável, em especial da LGPD.

Abaixo, as principais definições a serem observadas para aplicação da presente Política:

Consentimento³	Manifestação livre, informada e inequívoca pela qual o Titular concorda com o tratamento de seus dados pessoais para finalidade determinada. No contexto da Gestora, o Consentimento é base legal residual e excepcional, aplicável apenas às hipóteses e aos requisitos de validade do item 2.4.5 desta Política. É revogável a qualquer tempo, mediante procedimento gratuito e facilitado, sendo nulas as autorizações genéricas e cabendo à Tera o ônus de comprovar sua obtenção regular.
Dados Pessoais⁴	Toda informação relacionada a pessoa natural identificada ou identificável ⁵ . No contexto da Gestora, compreende os dados de identificação (ex: nome, RG, CPF etc.), de qualificação, patrimoniais, financeiros, de análise de perfil do investidor e de contato de Titulares, coletados no âmbito das atividades da Gestora, tais como, mas sem qualquer limitação, prospecção, cadastro, análise reputacional (<i>background check</i>) no contexto de KYC ⁶ , KYP ⁷ e KYE ⁸ , gestão de patrimônio e de recursos.
Dados Pessoais Sensíveis⁹	Dado Pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a pessoa natural.
Dado Anonimizado¹⁰	Dado relativo a Titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. No contexto da Gestora, aplica-se, por exemplo, a informações agregadas ou estatísticas extraídas de bases de clientes/investidores para fins de estudos internos, relatórios gerenciais ou envio de dados a bases setoriais (ex.: ANBIMA), quando não houver possibilidade de reidentificação do titular, hipótese em que o dado deixa de se sujeitar ao regime da LGPD.

³ Conforme definido no art. 5º, XII, da LGPD

⁴ Conforme definido no art. 5º, I, da LGPD.

⁵ Conforme definido no art. 5º, II, da LGPD.

⁶ Know Your Client (Conheça seu Cliente)

⁷ Know Your Partner (Conheça seu Parceiro)

⁸ Know Your Employee (Conheça seu Empregado)

⁹ Conforme definido no art. 5º, II, da LGPD.

¹⁰ Conforme definido no art. 5º, III, da LGPD.

Banco de Dados¹¹	Conjunto estruturado de Dados Pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico. No contexto da Gestora, correspondem aos sistemas de cadastro de clientes/investidores, plataformas de gerenciamento de obrigações regulatórias (sistemas de compliance), sistemas de gestão de carteiras e demais repositórios físicos ou eletrônicos que armazenem Dados Pessoais de Titulares.
Titular¹²	A pessoa natural a quem se referem os Dados Pessoais objeto de Tratamento (art. 5º, V, da LGPD). No contexto da Gestora, incluem-se, sem limitação: (i) Clientes e Potenciais Clientes: investidores e cotistas pessoa física dos fundos e veículos de investimento sob gestão, clientes de carteira administrada e dos serviços de gestão de patrimônio, e pessoas naturais em processo de cadastro ou prospecção, ainda que a relação não se concretize; quando o cliente for pessoa jurídica ou veículo, seus representantes legais, procuradores, administradores, sócios e beneficiários finais pessoa física; (ii) Integrantes de grupo familiar e beneficiários: integrantes do grupo familiar do Cliente e beneficiários de estruturas patrimoniais, sucessórias, securitárias ou previdenciárias, cujos dados sejam necessários à estruturação, revisão ou execução dessas soluções; (iii) Colaboradores e candidatos: sócios, empregados, estagiários e prestadores pessoa física da Gestora, bem como candidatos a vagas; e (iv) Prestadores de Serviços e contrapartes: pessoas naturais vinculadas a prestadores de serviços, fornecedores e contrapartes das carteiras sob gestão. (v) Terceiros submetidos a procedimentos de diligência: pessoas naturais cujos dados sejam tratados em rotinas de prevenção à lavagem de dinheiro, verificação de pessoas expostas politicamente, consulta a listas restritivas e demais diligências reputacionais, ainda que não mantenham relação com a Gestora; e (vi) Visitantes: pessoas naturais que acessem os canais digitais ou as dependências físicas da Gestora, inclusive por meio de controle de acesso e sistemas de monitoramento. Enquadram-se nesta definição ex-clientes, ex-colaboradores e demais titulares cujos dados permaneçam sob tratamento em razão de obrigação legal, regulatória ou de exercício regular de direitos. Dados relativos à pessoa jurídica não constituem Dados Pessoais, salvo quando permitam identificar, direta ou indiretamente, pessoa natural.
Controlador¹³	A pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento dos Dados Pessoais. No contexto da Gestora, a Tera atua como Controladora dos dados coletados diretamente de seus Clientes, Colaboradores e Prestadores de Serviços, uma vez que define a finalidade e os meios desse tratamento, incluindo, mas sem limitação, para fins de cadastro, processos de

¹¹ Conforme definido no art. 5º, IV, da LGPD.

¹² Conforme definido no artigo 5º, V, da LGPD.

¹³ Conforme definido no art. 5º, VI, da LGPD.

	<i>Know Your Client, Know Your Partner, Know Your Employee</i> , execução contratual e cumprimento de obrigações legais e regulatórias perante CVM e ANBIMA.
Operador¹⁴	A pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de Dados Pessoais em nome do Controlador . A atuação da Tera como Operadora é excepcional. Nas relações com o administrador fiduciário, o distribuidor, o custodiante e os demais participantes de mercado, a Tera e esses participantes atuam, em regra, como Controladores independentes, cada qual definindo as finalidades do Tratamento necessário ao cumprimento de suas próprias obrigações regulatórias.
Encarregado¹⁵	Colaborador da Gestora: Alan Lima (alan.lima@teracapital.com.br ou dpo@teracapital.com.br). Compete ao Encarregado aceitar reclamações e comunicações dos Titulares, prestar esclarecimentos e adotar providências, receber comunicações da ANPD, orientar os Colaboradores e executar as demais atribuições do artigo 41 da LGPD. A identidade e as informações de contato do Encarregado são divulgadas publicamente no sítio eletrônico da Gestora.
Agentes de Tratamento¹⁶	Expressão que designa, em conjunto, o Controlador e o Operador. No contexto da Gestora, qualificam-se como Agentes de Tratamento a própria Tera (nas hipóteses acima) e os terceiros contratados que tenham acesso a Dados Pessoais no exercício de suas atividades (ex. administrador fiduciário, custodiante, distribuidor, consultor especializado e demais prestadores de serviços), cabendo à Gestora formalizar contratualmente os papéis, responsabilidades e bases legais aplicáveis a cada relação.
Área de Compliance¹⁷	Área responsável por: (a) mapear e tratar os Dados Pessoais que a Tera recebe em suas interações com Titulares dos Dados Pessoais; (b) assegurar que o compartilhamento de Dados Pessoais com terceiros seja realizado de acordo com as regras estabelecidas na LGPD e nesta Política; (c) vedar o compartilhamento de Dados Pessoais nos casos em que não for possível o cumprimento das regras estabelecidas na LGPD e nesta Política; e (d) atualizar periodicamente a presente Política.
Tratamento¹⁸	Toda operação realizada com Dados Pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

¹⁴ Conforme definido no art. 5º, VII, da LGPD.

¹⁵ Conforme definido no art. 5º, VIII, da LGPD.

¹⁶ Conforme definido no art. 5º, IX, da LGPD.

¹⁷ Conforme definido no Manual de Compliance.

¹⁸ Conforme definido no art. 5º, X, da LGPD

Colaboradores	Sócios, administradores, empregados, estagiários, aprendizes e prestadores de serviço pessoa física que atuem em nome da Gestora, independentemente da natureza do vínculo, conforme definido no Manual de Compliance.
Uso Compartilhado de Dados	Comunicação, difusão, transferência internacional, interconexão ou tratamento compartilhado de Dados Pessoais por dois ou mais Agentes de Tratamento, observado o item 2.5 desta Política.
Transferência Internacional de Dados	Transferência de Dados Pessoais para país estrangeiro ou organismo internacional do qual o País seja membro, sujeita às hipóteses do artigo 33 da LGPD e à RANPD 19, na forma do Capítulo 5 desta Política.
Incidente de Segurança	Evento adverso, confirmado ou sob suspeita, relacionado a violação de segurança que provoque acesso não autorizado, destruição, perda, alteração, vazamento ou qualquer forma de Tratamento inadequado de Dados Pessoais, ainda que acidental, na forma do Capítulo 4 desta Política.
ANPD	Autoridade Nacional de Proteção de Dados, órgão da administração pública federal responsável por zelar pela proteção dos Dados Pessoais e por fiscalizar e aplicar sanções em caso de descumprimento da LGPD.

2. Tratamento de Dados Pessoais pela Tera

2.1. Princípios Aplicados ao Tratamento de Dados Pessoais

Todo Tratamento de Dados Pessoais realizado pela Tera observará a boa-fé e os princípios do artigo 6º da LGPD, aplicados da seguinte forma:

- (i) **Finalidade:** cada Tratamento tem finalidade determinada, sendo vedado o uso posterior incompatível com essa finalidade;
- (ii) **Adequação:** os dados tratados devem ser compatíveis com a finalidade informada ao Titular e com o contexto em que foram obtidos;
- (iii) **Necessidade:** coleta-se apenas o necessário para prestação dos serviços da Tera e atendimento à legislação e regulamentação vigente;
- (iv) **Livre Acesso:** o Titular tem consulta facilitada e gratuita sobre o Tratamento de seus dados, na forma do Capítulo 3 desta Política e LGPD;
- (v) **Qualidade dos Dados Pessoais:** os dados cadastrais são mantidos exatos e atualizados, em periodicidade compatível com a regulamentação aplicável;
- (vi) **Transparência:** as informações sobre o Tratamento são claras e acessíveis, observados os segredos comercial e industrial e o sigilo imposto pela regulamentação do mercado de capitais;
- (vii) **Segurança:** aplicam-se as medidas técnicas e administrativas estabelecidas nas políticas internas da Tera;
- (viii) **Prevenção:** a Tera atua preventivamente, e não apenas em resposta a incidentes, nos termos do Capítulo 4;
- (ix) **Não Discriminação:** é vedado o Tratamento para fins discriminatórios ilícitos ou abusivos;
- (x) **Responsabilização e prestação de contas:** a Tera mantém documentação apta a comprovar a adoção e a eficácia das medidas previstas nesta Política.

2.2. Fontes de Obtenção dos Dados Pessoais

Os Dados Pessoais tratados pela Tera são obtidos das seguintes fontes:

- (i) **Diretamente do Titular:** no preenchimento de ficha cadastral, questionário de análise de perfil do investidor, formulários fiscais (FATCA e CRS), contratos e demais documentos de pré e pós contratação, bem como no curso do relacionamento;
- (ii) **Prestadores de Serviços e Demais Participantes de Mercado:** administrador fiduciário, custodiante, escriturador, distribuidor, consultor especializado e demais participantes das operações e dos veículos sob gestão, no âmbito das respectivas atribuições regulamentares e contratuais;
- (iii) **Fontes Públicas e Bases de Terceiros:** listas restritivas nacionais e internacionais, bases de pessoas expostas politicamente, mídia negativa, publicações oficiais, tribunais, juntas comerciais e ferramentas contratadas de diligência reputacional;
- (iv) **Geradas Internamente pela Tera:** registros de atendimento, correspondência institucional, *logs* de acesso a sistemas e, quando aplicável, gravações e transcrições de reuniões, nos termos do item 2.7;
- (v) **Recebidas de Forma Incidental ou Não Solicitada:** nos termos do item 2.2.1 infra.

2.2.1. Dados Pessoais Recebidos de Forma Incidental ou Não Solicitado

Caso a Tera, por meio de seus Colaboradores, receba Dados Pessoais de forma incidental ou não solicitada (ie. copiada em mensagem eletrônica que contenha informações pessoais de terceiros), tais dados não serão utilizados para nenhuma finalidade própria da Gestora, não serão incorporados às suas bases de dados nem repassados a terceiros, devendo permanecer restritos ao contexto em que foram recebidos.

A comunicação ao Encarregado é exigida apenas quando o recebimento: (i) envolver Dados Pessoais Sensíveis, na forma do item 2.6; (ii) abranger volume relevante de Titulares; (iii) resultar na incorporação dos dados a sistema ou base da Gestora; ou (iv) indicar a ocorrência de Incidente de Segurança, próprio ou de terceiro, hipótese em que se aplica o Capítulo 4.

2.3. Finalidades do Tratamento e Bases Legais de Tratamento de Dados Pessoais

A Tera trata Dados Pessoais para as finalidades indicadas no quadro abaixo, com fundamento nas bases legais existentes. O quadro abaixo cumpre o requisito previsto no artigo 9º, inciso V, das Regras e Procedimentos de Deveres Básicos da ANBIMA, que prevê a obrigação de especificar o controle de privacidade de Dados Pessoais a que as instituições participantes tenham acesso:

#	Finalidade	Titulares	Base legal	Guarda	Responsável
1	Cadastro, identificação, qualificação e atualização cadastral de Clientes, inclusive procedimentos de conhecimento do cliente (KYC)	Clientes e representantes	Obrigação legal ou regulatória (art. 7º, II, LGPD); RCV 50 e RCV 21	Mín. 5 (cinco) anos do cadastro ou da última atualização (RCV 50, art. 26, § 2º)	Compliance
2	Diligências de prevenção à lavagem de dinheiro e ao financiamento do terrorismo: consulta a listas restritivas, verificação de pessoa exposta politicamente, mídia negativa,	Clientes, Colaboradores, Prestadores de Serviços	Art. 7º, II, LGPD; Lei nº 9.613/1998; Lei nº 13.810/2019; RCV 50	Mín. 5 (cinco) anos, prorrogável por determinação da CVM (RCV 50, art. 26)	Compliance

#	Finalidade	Titulares	Base legal	Guarda	Responsável
	monitoramento de operações e comunicações ao COAF				
3	Análise de perfil do investidor	Clientes	Art. 7º, II, LGPD para os serviços regulados	Mín. 5 (cinco) anos (RCVM 21, art. 34)	Gestão e Compliance
4	Execução dos contratos de gestão de carteira administrada, de gestão de patrimônio e de consolidação de investimentos	Clientes	Execução de contrato (art. 7º, V, LGPD)	Vigência do contrato + 5 (cinco) anos	Compliance e Gestão
5	Gestão dos fundos e veículos de investimento e relacionamento com cotistas, inclusive atendimento a assembleias e prestação de informações	Clientes	Art. 7º, II e V, LGPD; RCVM 175; RCVM 21	Mín. 5 (cinco) anos (RCVM 175, art. 130; RCVM 21, art. 34)	Compliance e Gestão
6	Prestação de informações a reguladores e autorreguladores (CVM, ANBIMA, BACEN, COAF) e a autoridades fiscais, inclusive no âmbito de CRS e FATCA	Clientes, Colaboradores e Prestadores de Serviços	Art. 7º, II, LGPD	Mín. 5 (cinco) anos (RCVM 21, art. 34)	Compliance
7	Exercício regular de direitos da Tera em processo judicial, administrativo ou arbitral e atendimento a fiscalizações e requisições de autoridade competente	Todos	Exercício regular de direitos (art. 7º, VI, LGPD)	Até o trânsito em julgado	Jurídico e Compliance
8	Atendimento a requisições de Titulares no exercício dos direitos do artigo 18 da LGPD	Todos	Art. 7º, II, 18 e 19, LGPD	5 (cinco) anos do encerramento da solicitação	Compliance e Encarregado
9	Segurança da informação e cibernética, controle de acesso a sistemas e ambientes, monitoramento de recursos corporativos e prevenção a fraudes	Clientes, Colaboradores e terceiros com acesso	Legítimo interesse (art. 7º, IX, LGPD)	12 (doze) meses para logs	Tecnologia e Compliance
10	Recrutamento e seleção de Colaboradores	Colaboradores e candidatos	Procedimentos preliminares (art. 7º, V, LGPD); banco de talentos mediante legítimo interesse (art. 7º, IX, LGPD)	12 (doze) meses após o processo.	Recursos Humanos e Compliance
11	Diligência reputacional de Colaboradores, candidatos, Prestadores de Serviços e contrapartes (KYE/KYP)	Colaboradores, candidatos, Prestadores de Serviços	Art. 7º, II, LGPD quando exigida pela regulamentação; no que exceder, legítimo interesse (art. 7º, IX, LGPD)	Mín. 5 (cinco) anos (RCVM 21, art. 34)	Compliance
12	Gravação e transcrição de reuniões e uso de ferramentas de apoio baseadas em inteligência artificial	Clientes, Colaboradores, Prestadores de Serviços	Legítimo interesse (art. 7º, IX, LGPD); Consentimento quando exigido pelo item 2.4.5	12 (doze) meses	Encarregado e Tecnologia

#	Finalidade	Titulares	Base legal	Guarda	Responsável
13	Cumprimento das políticas e manuais internos da Gestora, apuração de descumprimentos e resposta a incidentes de segurança	Todos	Art. 7º, II e IX, LGPD	Mín. 5 (cinco) anos	Compliance e Encarregado
14	Administração da relação de trabalho: folha de pagamento, benefícios, jornada, saúde e segurança do trabalho e demais obrigações trabalhistas e previdenciárias	Colaboradores e respectivos dependentes	Execução de contrato (art. 7º, V, LGPD) e obrigação legal ou regulatória (art. 7º, II); dados de saúde na forma do art. 11, II, “a”	Prazos da legislação trabalhista e previdenciária, observado o mínimo de 5 (cinco) anos após o término do vínculo	Recursos Humanos e Compliance
15	Controle de acesso físico às dependências da Gestora e monitoramento por sistema de imagem	Colaboradores, Prestadores de Serviços e visitantes	Legítimo interesse (art. 7º, IX, LGPD); Consentimento específico para dado biométrico (art. 11, I), na forma do item 2.6	Até 90 (noventa) dias para imagens e registros de acesso	Tecnologia e Compliance
16	Estruturação e acompanhamento de soluções de planejamento patrimonial e sucessório, inclusive por meio de veículos constituídos no exterior	Clientes, integrantes de grupo familiar e beneficiários	Execução de contrato (art. 7º, V, LGPD); quanto a integrantes de grupo familiar e beneficiários, legítimo interesse (art. 7º, IX), mediante teste de balanceamento	Vigência do contrato + 5 (cinco) anos	Gestão e Compliance
17	Comunicações institucionais, envio de materiais e relacionamento não relacionado à execução dos contratos	Clientes e potenciais Clientes	Legítimo interesse (art. 7º, IX, LGPD), assegurada a oposição; Consentimento quando exigido pelo item 2.4.5	Até a manifestação de oposição do Titular	Gestão e Compliance

2.3.1. Bases Legais Não Aplicáveis às Atividades da Tera

A Tera declara que não realiza Tratamento de Dados Pessoais com fundamento nas seguintes hipóteses do artigo 7º da LGPD, por não guardarem relação com suas atividades:

- (i) tratamento e uso compartilhado por administração pública para execução de políticas públicas;
- (ii) realização de estudos por órgão de pesquisa;
- (iii) tutela da saúde em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- (iv) proteção do crédito.

A hipótese do inciso VII do artigo 7º (proteção da vida ou da incolumidade física do Titular ou de terceiro) não constitui base legal ordinária de nenhuma atividade da Tera, podendo ser invocada apenas em situação concreta de emergência, com registro imediato pelo Encarregado.

2.4. Requisitos Específicos Por Base Legal

2.4.1. Cumprimento de Obrigação Legal e/ou Regulatória (art. 7º, II, LGPD)

Aplica-se sempre que o Tratamento for necessário ao cumprimento de obrigação estabelecida em lei, decreto, resolução, instrução, ofício, deliberação de autorregulação ou outro ato normativo aplicável às atividades da Tera, incluindo as obrigações de cadastro e atualização cadastral, de prevenção à lavagem de dinheiro e ao financiamento do terrorismo, de verificação do perfil do investidor, de guarda de documentos e registros, de prestação de informações a reguladores, autorreguladores e autoridades fiscais, inclusive no âmbito do CRS e do FATCA, e de atendimento a requisições de autoridade competente.

2.4.2. Execução de Contrato e Procedimentos Preliminares (Art. 7º, V, LGPD)

Aplica-se quando o Tratamento for necessário à execução de contrato do qual o Titular seja parte ou à adoção de procedimentos preliminares relacionados a contrato, a pedido do próprio Titular (ie. contratos de gestão de carteira administrada, de gestão de patrimônio e de consolidação de ativos financeiros e não financeiros, bem como propostas, simulações e etapas de *onboarding* solicitadas pelo Titular antes da contratação).

As obrigações decorrentes da regulamentação ou da autorregulação aplicáveis às atividades da Tera não se enquadram nesta base legal, ainda que executadas no contexto de um contrato. Tais obrigações têm fundamento no item 2.4.1 supra. Tal distinção se faz relevante uma vez que, encerrado o contrato, o dever de guarda regulatório subsiste.

2.4.3. Exercício Regular de Direitos (art. 7º, VI, LGPD)

Aplica-se ao Tratamento necessário à defesa dos interesses da Tera em processo judicial, administrativo ou arbitral (Lei nº 9.307/1996), bem como ao atendimento de fiscalizações e requisições de autoridade competente. O Tratamento limita-se aos dados pertinentes ao objeto da controvérsia ou da requisição e cessa com o trânsito em julgado ou o encerramento do procedimento, ressalvados os prazos prescricionais e de guarda aplicáveis.

2.4.4. Legítimo Interesse (arts. 7º, IX, e 10, LGPD)

O Tratamento fundado no legítimo interesse da Tera ou de terceiro exige atenção especial, de modo a assegurar o equilíbrio entre (a) o interesse legítimo invocado; e (b) a proteção dos direitos, das liberdades fundamentais e das legítimas expectativas do Titular. Nessa hipótese, somente podem ser tratados os Dados Pessoais estritamente necessários à finalidade pretendida.

Antes do início de qualquer Tratamento fundado no legítimo interesse, o Encarregado, com apoio da Área de Compliance, elaborará e arquivará teste de balanceamento (também referido como teste de proporcionalidade ou avaliação de legítimo interesse), contemplando, no mínimo:

- (i) **Legitimidade do interesse:** a finalidade deve ser legítima, específica e compatível com as atividades da Tera, não podendo ser vedada por lei nem fundada em hipótese meramente futura ou abstrata;
- (ii) **Necessidade:** deve-se demonstrar que a finalidade não pode ser atingida com menos dados e avaliar se outra base legal é mais adequada;
- (iii) **Balanceamento:** devem ser analisados os impactos sobre os direitos e as legítimas expectativas do Titular, verificando-se se o interesse invocado prevalece;
- (iv) **Salvaguardas:** devem ser adotadas medidas de mitigação, como transparência prévia, limitação

de acesso, minimização, pseudonimização ou anonimização e, quando cabível, a possibilidade de oposição pelo Titular, medidas que não se confundem com a obtenção de Consentimento.

O registro das operações fundadas em legítimo interesse é obrigatório, nos termos do artigo 37 da LGPD, e a Tera poderá ser instada pela ANPD a apresentar relatório de impacto à proteção de dados pessoais, na forma do artigo 10, § 3º, da LGPD.

2.4.5. Consentimento (arts. 7º, I, e 8º, LGPD)

O Consentimento é base legal residual e excepcional no contexto da Tera. Deve-se evitar invocá-lo quando houver outra base legal aplicável, em especial nas hipóteses de cumprimento de obrigação legal ou regulatória e de execução de contrato.

Na hipótese de o Consentimento ser a base legal adequada, deverá observar cumulativamente os seguintes requisitos de validade:

- (i) **Informado:** o Titular deve ser previamente informado da finalidade do Tratamento, dos dados envolvidos, do compartilhamento pretendido e de seus direitos;
- (ii) **Livre:** o Titular deve ter efetivo poder decisório; quando possível, a autorização será fragmentada por finalidade. Sendo determinada informação essencial à prestação do serviço, esse fato será informado de forma destacada;
- (iii) **Inequívoco:** é vedada qualquer forma de indução, manipulação ou obtenção precipitada da manifestação;
- (iv) **Específico:** o Consentimento refere-se a finalidades determinadas e a dados ou categorias de dados especificados, sendo nulas as autorizações genéricas;
- (v) **Destacado:** colhido por escrito, o Consentimento constará de instrumento apartado ou de cláusula destacada das demais cláusulas contratuais, sendo vedada sua inserção difusa no corpo do contrato de prestação de serviços.

O ônus de comprovar a obtenção regular do Consentimento é da Tera. O Titular pode revogá-lo a qualquer momento, por manifestação expressa encaminhada ao canal do Encarregado, mediante procedimento gratuito e facilitado, ficando ratificados os Tratamentos realizados sob o amparo do Consentimento anterior até a revogação. A revogação não afeta os Tratamentos fundados em outra base legal, notadamente as obrigações de guarda e de prestação de informações a reguladores.

Havendo alteração da finalidade incompatível com o Consentimento original, o Titular será previamente informado e poderá revogá-lo caso discorde.

No contexto da Tera, o Consentimento será utilizado, em especial: (i) no Tratamento de Dados Pessoais Sensíveis não amparado nas hipóteses do artigo 11, inciso II, da LGPD; (ii) no Tratamento de dados de crianças e adolescentes, hipótese em que será colhido de forma específica e em destaque de ao menos um dos pais ou do responsável legal, nos termos do artigo 14, § 1º, da LGPD; e (iii) em finalidades acessórias e não necessárias à prestação dos serviços, tais como comunicações institucionais e envio de materiais.

2.5. Uso Compartilhado de Dados, Operadores e Terceiros

O compartilhamento de Dados Pessoais é modalidade de Tratamento e, como tal, exige finalidade determinada e base legal próprias, que serão sempre as mesmas do Tratamento que o justifica, registradas no quadro do item 2.3 supra.

A Tera compartilha Dados Pessoais, no limite do necessário, com:

Terceiro	Finalidade	Papel
Administrador fiduciário, custodiante, escriturador e controlador de ativos e passivos	Operacionalização dos fundos e veículos sob gestão e das carteiras administradas	Controlador autônomo quanto às suas atribuições regulamentares
Distribuidor	Distribuição de cotas e relacionamento com o investidor	Controlador autônomo quanto às suas atribuições regulamentares
Consultor especializado e demais prestadores contratados no interesse das carteiras	Execução das atividades contratadas	Operador ou Controlador autônomo, conforme o contrato
Prestador terceirizado de recursos humanos e de folha de pagamento	Administração da relação de trabalho	Operador
Provedores de sistemas, de armazenamento e de computação em nuvem, inclusive ferramentas de gravação e transcrição	Suporte às atividades da Gestora	Operador
Auditores, assessores jurídicos e consultores externos	Auditoria, defesa de direitos e assessoria	Operador ou Controlador autônomo, conforme o caso
CVM, ANBIMA, BACEN, COAF, Receita Federal e demais autoridades	Cumprimento de obrigação legal ou regulatória e atendimento a requisições	Destinatário legal — não configura compartilhamento discricionário

São condições para o compartilhamento:

- (i) celebração de instrumento contratual que contenha cláusulas de proteção de dados pessoais, definindo o papel de cada parte, as finalidades autorizadas e demais condições aplicáveis;
- (ii) diligência prévia sobre a capacidade do terceiro de cumprir esta Política e a legislação de proteção de dados, na forma das regras de contratação de terceiros da Tera; e
- (iii) observância do Capítulo 5 desta Política, quando houver Transferência Internacional de Dados.

A eventual circulação de Dados Pessoais entre a Tera e outras entidades do mesmo grupo econômico constitui uso compartilhado de dados e, como tal, depende de finalidade determinada, base legal própria e informação ao Titular, não sendo autorizada pela mera identidade de grupo econômico.

2.6. Dados Pessoais Sensíveis

Como regra, a Tera não coleta nem solicita Dados Pessoais Sensíveis de Clientes, de seus representantes ou de integrantes de grupo familiar.

O Tratamento de Dados Pessoais Sensíveis pela Tera restringe-se, em regra, às seguintes hipóteses, observado o artigo 11 da LGPD:

- (i) Dados de saúde de Colaboradores estritamente necessários à administração de benefícios e ao cumprimento de obrigações trabalhistas, previdenciárias e de saúde e segurança do trabalho, com fundamento no artigo 11, inciso II, alínea "a", da LGPD;
- (ii) Dados sensíveis indispensáveis ao exercício regular de direitos em processo judicial, administrativo ou arbitral, com fundamento no artigo 11, inciso II, alínea "d", da LGPD; e
- (iii) Dado biométrico facial de Colaboradores, para a finalidade exclusiva de controle de acesso às dependências da Gestora, mediante Consentimento específico e destacado do Colaborador (artigo 11, inciso I, da LGPD), assegurada, em qualquer caso, alternativa de acesso não

biométrica, sem prejuízo ao Colaborador que não consentir.

Excepcionalmente, no âmbito na prestação de serviços de planejamento patrimonial e sucessório, a Gestora pode receber Dados Pessoais Sensíveis de Clientes, de integrantes de grupo familiar do Cliente e beneficiários, hipótese em que o Tratamento observará o artigo 11 da LGPD e o disposto neste item.

Caso a Tera, por meio de seus Colaboradores, receba Dados Pessoais de forma incidental ou não solicitada (ie. cópia em mensagem eletrônica que contenha informações pessoais de terceiros), tais dados não serão utilizados para nenhuma finalidade própria da Gestora, não serão incorporados às suas bases de dados nem repassados a terceiros, devendo permanecer restritos ao contexto em que foram recebidos.

A comunicação ao Encarregado é exigida apenas quando o recebimento incidental de Dados Pessoais Sensíveis: (i) abranger volume relevante de Titulares; (ii) resultar na incorporação dos dados a sistema ou base da Gestora; ou (iii) indicar a ocorrência de Incidente de Segurança, próprio ou de terceiro, hipótese em que se aplica o Capítulo 4.

A condição de pessoa exposta politicamente (PEP), tratada para fins de prevenção à lavagem de dinheiro, não constitui Dado Pessoal Sensível na acepção do artigo 5º, inciso II, da LGPD. Ainda assim, considerando seu potencial de revelar informação de natureza política, a Tera trata esse dado com acesso restrito e exclusivamente para a finalidade regulatória que o justifica.

2.7. Gravação de Reuniões, Transcrição e Ferramentas de Inteligência Artificial

A Tera pode gravar e transcrever reuniões e utilizar ferramentas de apoio baseadas em inteligência artificial no processamento de comunicações, documentos e registros que contenham Dados Pessoais, exclusivamente por meio de ferramentas previamente homologadas pela Área de Compliance e pela área responsável por tecnologia da informação e cibersegurança, e observadas as regras deste item.

Quando a gravação envolver reunião com Cliente e não houver base legal de execução de contrato ou de cumprimento de obrigação regulatória que a ampare, será obtido o Consentimento do Titular na forma do item 2.4.5, facultada a manifestação de oposição a qualquer momento.

É vedado inserir Dados Pessoais, Dados Pessoais Sensíveis ou informações confidenciais de Clientes, de Colaboradores ou das carteiras sob gestão em ferramentas de inteligência artificial de uso público, em contas particulares ou não homologadas pela Gestora, ainda que para fins de resumo, tradução, revisão ou análise.

2.8. Retenção e Eliminação dos Dados Pessoais

O Tratamento se encerra quando verificado o alcance da finalidade, quando os dados deixarem de ser necessários ou pertinentes à finalidade, ao fim do período de Tratamento, por comunicação do Titular ou por determinação da ANPD, nos termos do artigo 15 da LGPD.

Encerrado o Tratamento, os Dados Pessoais serão eliminados, autorizada a conservação, nos termos do artigo 16 da LGPD, para: (a) cumprimento de obrigação legal ou regulatória pela Tera; (b) transferência a terceiro, observados os requisitos da LGPD; ou (c) uso exclusivo da Tera, vedado o acesso por terceiro e desde que anonimizados os dados.

É vedada a eliminação de Dados Pessoais que sejam objeto de litígio, de procedimento administrativo, de fiscalização ou de requisição de autoridade em curso, ainda que vencido o prazo de guarda, até o encerramento definitivo do procedimento.

A eliminação será realizada por método que impeça a recuperação da informação, mediante registro da

operação, e alcançará as cópias existentes em ambientes de backup, na medida em que os limites técnicos das ferramentas utilizadas o permitirem.

2.9. Registro das Operações de Tratamento e Relatório de Impacto

A Tera mantém registro das operações de Tratamento de Dados Pessoais que realiza, nos termos do artigo 37 da LGPD, especialmente das fundadas em legítimo interesse. O registro é elaborado e mantido pela Área de Compliance, com apoio das áreas envolvidas.

O registro das operações de tratamento é revisto sempre que houver alteração relevante em atividades, contratos, sistemas ou fornecedores, e deve manter-se consistente com os quadros dos itens 2.3 e 2.4 supra.

A Tera elaborará relatório de impacto à proteção de Dados Pessoais, contendo a descrição dos tipos de dados coletados, a metodologia de coleta e de garantia da segurança e a análise das medidas, salvaguardas e mecanismos de mitigação de risco adotados, nas seguintes hipóteses: (a) quando determinado pela ANPD, nos termos do artigo 38 da LGPD; (b) quando o Tratamento se fundar em legítimo interesse e for solicitado pela ANPD, nos termos do artigo 10, § 3º; e (c) por deliberação do Encarregado, nas hipóteses de realização de Tratamento para nova finalidade que não estiver indicada no quadro do item 2.3.

2.10. Segurança do Tratamento

A Tera adota medidas de segurança 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 qualquer forma de Tratamento inadequado, nos termos do artigo 46 da LGPD. As medidas específicas, os controles de acesso, os testes periódicos e as regras de sigilo constam da política de segurança da informação e do manual de confidencialidade da Gestora, exigidos pelos artigos 24 e 28 da RCV 21 e pelos artigos 9º a 12 das Regras e Procedimentos de Deveres Básicos da ANBIMA.

Os incidentes de segurança envolvendo Dados Pessoais observam o fluxo do Capítulo 4 desta Política.

3. Direitos dos Titulares de Dados Pessoais

Os Titulares dos Dados Pessoais possuem diversos direitos com relação aos Dados Pessoais e Dados Pessoais Sensíveis. Foram mapeados os seguintes direitos:

3.1. Confirmação de Existência e Acesso aos Dados Pessoais: O Titular dos Dados Pessoais poderá requerer à Gestora a confirmação da existência e/ou de acesso a seus Dados Pessoais. A confirmação de existência ou o acesso serão providenciados imediatamente, em formato simplificado, ou, se assim requerido pelo Titular, por meio de declaração clara e completa, no prazo do item 3.10, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do Tratamento, nos termos do artigo 19, incisos I e II, da LGPD.

3.2. Correção de Dados Pessoais: O Titular dos Dados Pessoais poderá requerer à Tera a correção de dados incompletos, inexatos ou desatualizados.

3.3. Anonimização, Bloqueio ou Eliminação dos Dados Pessoais: O Titular dos Dados Pessoais poderá requerer a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD. O atendimento observa as hipóteses de conservação do artigo

16 da LGPD e não alcança os Dados Pessoais cuja guarda seja exigida por obrigação legal ou regulatória, notadamente pelos prazos indicados no quadro do item 2.3, nem os necessários ao exercício regular de direitos. Nessas hipóteses, a Tera informará ao Titular as razões de fato e de direito que impedem a adoção da providência, nos termos do artigo 18, § 4º, da LGPD.

Para fins de aplicação desta Política, por desnecessários e excessivos entendem-se os dados que não são mais úteis para a finalidade de Tratamento específica anteriormente desejada.

3.4. Portabilidade dos Dados Pessoais: O Titular poderá solicitar a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição formal expressa à Gestora, de acordo com a regulamentação da ANPD e LGPD. Nessa hipótese, deverão ser mantidos em sigilo os segredos comercial e industrial da Tera.

Ressalta-se que os dados que foram anonimizados pela Gestora não serão incluídos na portabilidade.

Por fim, importante destacar que, mesmo realizada a portabilidade, a Gestora deverá manter os Dados Pessoais para fins de cumprimento da regulamentação em vigor aplicável, conforme o(s) prazo(s) legal(is) ou contratual(is).

3.5. Eliminação dos Dados Pessoais Tratados com Consentimento: Considerando que o Consentimento pode ser revogado a qualquer momento mediante manifestação formal e expressa do Titular à Gestora, por meio de procedimento gratuito e facilitado, a eliminação dos Dados Pessoais deve ocorrer em prazo razoável após o recebimento do pedido.

No entanto, a Gestora está autorizada a realizar a conservação dos Dados Pessoais nas seguintes hipóteses:

- (i) Dados Pessoais obtidos para o cumprimento de obrigação legal ou regulatória pela Gestora;
- (ii) Para a transferência a terceiro, tal como para fins de Transferência Internacional de Dados e Uso Compartilhado de Dados, desde que respeitados os requisitos de tratamento de dados dispostos na LGPD; ou
- (iii) Para uso exclusivo da Gestora, vedado seu acesso por terceiro, e desde que anonimizados os dados.

3.6. Informação Sobre o Compartilhamento de Dados Pessoais: É direito do Titular dos Dados Pessoais ser informado de forma clara sobre o compartilhamento de seus dados com terceiros. A circulação de Dados Pessoais entre entidades do mesmo grupo econômico, ainda que com CNPJs distintos, constitui Uso Compartilhado de Dados e depende de finalidade determinada, base legal própria e informação ao Titular.

3.7. Oposição ao Tratamento: O Titular poderá opor-se a Tratamento realizado com fundamento em uma das hipóteses de dispensa de Consentimento, em caso de descumprimento da LGPD, nos termos do artigo 18, § 2º. A Gestora assegura, ainda, a possibilidade de oposição aos Tratamentos fundados em legítimo interesse, na forma do item 2.4.4.

3.8. Revisão de Decisões Automatizadas: O Titular poderá solicitar a revisão de decisões tomadas unicamente com base em Tratamento automatizado de seus Dados Pessoais que afetem seus interesses, nos termos do artigo 20 da LGPD. A Gestora não adota, na data desta Política, decisões unicamente automatizadas com tais efeitos; caso venha a adotá-las, informará previamente os Titulares e os critérios utilizados, observado o item 2.7.

3.9. Informação sobre a Negativa de Consentimento e Petição à ANPD: O Titular tem direito de ser informado sobre a possibilidade de não fornecer Consentimento e sobre as consequências da negativa, bem como de peticionar em face da Gestora perante a ANPD, nos termos do artigo 18, incisos VI e VII, da LGPD.

3.10. Forma de Solicitação e Prazo de Resposta: Na hipótese de o Titular desejar exercer quaisquer dos direitos indicados nos itens 3.1 a 3.9 supra, deverá encaminhar a referida solicitação à Gestora por meio do e-mail dpo@teracapital.com.br. O Encarregado confirmará a identidade do requerente antes de prestar qualquer informação e, tratando-se de solicitação apresentada por representante legal, procurador, herdeiro ou inventariante, exigirá a comprovação documental dos poderes.

A Tera responderá a cada solicitação no prazo máximo de 15 (quinze) dias, contado do recebimento, conforme prazo previsto no artigo 19, inciso II, da LGPD para a declaração de confirmação e acesso e adotado pela Gestora, por padronização, para os demais direitos. Não sendo possível atender à solicitação, a Tera comunicará ao Titular, no mesmo prazo, as razões de fato ou de direito que impedem a adoção imediata da providência.

4. Respostas a Incidentes de Segurança

4.1. Objetivo

Esta seção estabelece o procedimento e prazo aplicável para a comunicação de incidentes de segurança que envolvam Dados Pessoais tratados pela Gestora, em conformidade com a Lei Geral de Proteção de Dados Pessoais e com a regulamentação editada pela ANPD.

4.2. Prazo Aplicável

Nos termos da LGPD e da RANPD 15, incidentes de segurança que possam acarretar risco ou dano relevante aos Titulares de Dados Pessoais devem ser comunicados à ANPD e aos Titulares afetados no prazo de 3 (três) dias úteis, contado a partir da data em que Gestora tomar conhecimento do incidente.

A comunicação à ANPD é apresentada por meio do formulário eletrônico disponibilizado pela Autoridade. Não sendo possível reunir, no prazo, todas as informações exigidas, a Gestora realizará a comunicação com os elementos disponíveis, justificando a ausência dos demais, e a complementará em até 20 (vinte) dias úteis, nos termos da RANPD 15.

Quando a Tera atuar como Operadora, comunicará o incidente ao Controlador imediatamente após dele tomar conhecimento, cabendo a este a comunicação à ANPD e aos Titulares. Os contratos celebrados com Operadores da Gestora deverão prever a comunicação imediata de incidentes à Tera.

4.3. Fluxo Interno de Resposta a Incidentes

4.3.1 Visão Geral

A Gestora adota fluxo estruturado em 6 (seis) etapas para identificação, avaliação, contenção, e, quando aplicável, notificação de incidentes de segurança envolvendo Dados Pessoais dos Titulares, conforme detalhado a seguir.

4.3.2 Etapas do Fluxo

- (a) **Deteção e Registro:** Todo Colaborador que identificar ou suspeitar da ocorrência de um incidente de segurança (tal como vazamento de dados, acesso indevido, perda ou furto de dispositivo, ou envio de e-mail a destinatário incorreto) deve comunicar o fato imediatamente ao Encarregado, por meio do canal único e institucional disponibilizado para esse fim (dpo@teracapital.com.br).

O registro preciso do horário da detecção é elemento crítico do processo, uma vez que o prazo legal de comunicação, referido na Seção 4.2, é contado a partir do conhecimento do incidente pela Tera, e não de sua ocorrência.

- (b) **Triagem e Classificação de Risco:** Cabe ao Encarregado avaliar a natureza do incidente reportado e classificar o nível de risco associado (baixo, médio ou alto) no prazo de até 24 (vinte e quatro) horas contadas do recebimento da comunicação, considerando, entre outros, os seguintes critérios:
- (i) Tipo de Dado Pessoal envolvido;
 - (ii) Volume e categoria de Titulares potencialmente afetados;
 - (iii) Ocorrência de efetiva exposição das informações a terceiros; e
 - (iv) Potencial de dano aos Titulares de dados.

A classificação de risco determina a necessidade de escalonamento do incidente às Áreas de Tecnologia¹⁹, empresa de suporte tecnológico e cibersegurança da Gestora, jurídico interno ou externo e/ou qualquer área de negócio envolvida no incidente.

¹⁹ Conforme definido no Manual de Compliance da Gestora.

- (c) **Contenção:** Identificado o incidente, devem ser adotadas imediatamente as medidas necessárias à sua contenção, tais como revogação de acessos, isolamento de sistemas afetados, recuperação de comunicações enviadas indevidamente e notificação ao fornecedor ou operador envolvido. Nesta etapa, a prioridade é interromper a exposição dos dados, ainda que a apuração da causa raiz do incidente venha a ser concluída posteriormente;
- (d) **Análise e Decisão sobre Notificação:** Concluída a contenção, procede-se à apuração da causa raiz do incidente, à delimitação do escopo real de impacto (número de Titulares afetados e categorias de dados comprometidos) e à verificação das medidas técnicas de segurança já em vigor. Com base nesses elementos, compete ao Encarregado decidir se o incidente configura risco ou dano relevante aos Titulares, critério que determina a obrigatoriedade de notificação à ANPD e aos Titulares afetados nos termos dos modelos de comunicação previstos no Anexo I desta Política;
- (e) **Notificação:** Constatada a obrigatoriedade de notificação, esta deve ser realizada às seguintes interessadas:
 - (i) **ANPD:** comunicação contendo a natureza dos Dados Pessoais afetados, os Titulares envolvidos, as medidas técnicas e de segurança utilizadas para a proteção dos dados, os riscos relacionados ao incidente e as medidas que foram ou serão adotadas para reverter ou mitigar seus efeitos; e
 - (ii) **Titulares afetados:** comunicação em linguagem clara e acessível, descrevendo o que ocorreu, quais dados foram impactados, as providências adotadas pela Tera e as medidas que o Titular pode adotar para se resguardar; e
 - (iii) **Administrador fiduciário, distribuidor e demais Agentes de Tratamento afetados, bem como CVM e ANBIMA, quando o incidente atingir dados ou sistemas relacionados aos veículos sob gestão ou quando houver dever de reporte decorrente da regulamentação, da autorregulação ou dos contratos celebrados.**
- (f) **Remediação e Registro Histórico:** Após a contenção do incidente, a Tera deve revisar o controle que originou a falha e atualizar as políticas, processos e/ou sistemas pertinentes, de modo a prevenir sua recorrência. Todos os incidentes, inclusive aqueles não notificados à ANPD, devem ser integralmente documentados e conservados pelo prazo mínimo de 5 (cinco) anos, de modo a evidenciar o cumprimento do princípio da responsabilização e prestação de contas em eventual procedimento fiscalizatório.

5. Transferência Internacional De Dados

A Transferência Internacional de Dados somente será realizada quando presente uma das hipóteses do artigo 33 da LGPD e observado o Regulamento de Transferência Internacional de Dados (RANPD 19). A transferência fundada em decisão de adequação depende de reconhecimento formal, pela ANPD, do país ou organismo internacional de destino, não cabendo à Gestora avaliar autonomamente a equivalência da legislação estrangeira. Até a data desta Política, a ANPD reconheceu como adequada apenas a União Europeia, por meio da Resolução CD/ANPD nº 32/2026.²⁰

²⁰ Conforme definido no art. 5º, XV, da LGPD.

A transferência pode acontecer quando (i) for necessária a cooperação entre órgãos públicos de inteligência de diferentes países para fins de investigação e processamento penal; (ii) quando a transferência for necessária para cumprimento de determinação legal ou regulatória pelo Controlador; (iii) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato; (iv) para o exercício regular de direitos em processo judicial, administrativo ou arbitral; ou (v) para a execução de políticas públicas ou demandas legais do serviço público.

Além disso, a Transferência Internacional de Dados também poderá ocorrer quando o Controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do Titular e do regime de proteção de dados previstos na LGPD, na forma de:

- (a) cláusulas contratuais específicas para determinada transferência;
- (b) cláusulas-padrão contratuais;
- (c) normas corporativas globais; e
- (d) selos, certificados e códigos de conduta regularmente emitidos.
- (e) Constitui hipótese autônoma, e não forma de garantia, a transferência autorizada por Consentimento específico e em destaque do Titular, precedido de informação sobre o caráter internacional da operação e com distinção clara desta de outras finalidades (artigo 33, inciso VIII, da LGPD).

Dessa forma, a Gestora tem o dever de assegurar o cumprimento desses princípios por meio de cláusulas contratuais, certificados e outras comprovações reconhecidas.

As cláusulas-padrão contratuais aprovadas pela ANPD devem ser adotadas na íntegra, sem alteração de seu conteúdo, admitidos ajustes apenas nos campos expressamente destinados ao preenchimento das particularidades da operação, sob pena de invalidade, e independem de aprovação prévia da Autoridade. As cláusulas contratuais específicas e as normas corporativas globais, ao contrário, dependem de aprovação prévia da ANPD.

No contexto da Gestora, são realizadas Transferências Internacionais de Dados, entre outras hipóteses, para: (i) veículos de investimento e estruturas constituídos no exterior, inclusive trusts e private investment companies, e respectivos trustees, administradores e agentes; (ii) instituições financeiras, custodiantes e corretoras estrangeiras; (iii) assessores jurídicos e tributários estrangeiros; (iv) provedores de sistemas, de armazenamento em nuvem e de ferramentas de gravação, transcrição e inteligência artificial cujo processamento ocorra fora do território nacional; e (v) autoridades fiscais estrangeiras, por intermédio da Secretaria Especial da Receita Federal do Brasil, no âmbito do CRS e do FATCA.

A título exemplificativo, mencione-se o pedido de identificação da *Ultimate Beneficial Ownership* (UBO) por parte de autoridade pública estrangeira, bem como o preenchimento de formulários no âmbito do CRS (*Common Reporting Standard*) e do W-8 (FATCA). Em todos esses casos, a Transferência Internacional de Dados estaria autorizada pela própria LGPD, conforme seu art. 33, inciso IX.

6. Penalidades

A LGPD estabelece que as sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios, dentre outros:

- (a) a gravidade e a natureza das infrações e dos direitos pessoais afetados;
- (b) boa-fé do infrator;
- (c) grau do dano;
- (d) cooperação do infrator;
- (e) existência de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados; e
- (f) adoção de política de boas práticas e governança.

As penalidades aos Agentes de Tratamento que não seguirem as disposições da LGPD podem ser as seguintes:

- (i) advertência, com indicação de prazo para adoção de medidas corretivas;
- (ii) multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos e limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- (iii) multa diária limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- (iv) publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- (v) bloqueio dos Dados Pessoais a que se refere a infração até a sua regularização;
- (vi) eliminação dos Dados Pessoais a que se refere a infração;
- (vii) suspensão parcial do funcionamento do Banco de Dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo Controlador; ou
- (viii) suspensão do exercício da atividade de tratamento dos Dados Pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período.
- (ix) As sanções administrativas previstas neste Capítulo não excluem a responsabilidade civil da Gestora perante os Titulares, nos termos dos artigos 42 a 45 da LGPD, nem as sanções aplicáveis pela CVM e pela ANBIMA em razão do descumprimento da regulamentação e da autorregulação.
- (x) O descumprimento desta Política por Colaborador sujeita-o às medidas disciplinares previstas nas políticas internas da Gestora, proporcionais à gravidade da conduta, sem prejuízo das responsabilidades civil e criminal cabíveis.

6.1. Governança, Aprovação, Treinamento e Revisão

Esta Política é aprovada pela diretoria da Gestora, competindo à Área de Compliance, com apoio do Encarregado, sua elaboração, atualização e divulgação interna.

A Política será revista sempre que houver alteração legislativa ou regulatória relevante, ou mudança significativa nas atividades, nos sistemas ou nos prestadores de serviços da Gestora, e, em qualquer hipótese, em prazo não superior a 24 (vinte e quatro) meses, nos termos do artigo 4º, parágrafo único, das Regras e Procedimentos de Deveres Básicos da ANBIMA.

Os Colaboradores recebem treinamento sobre proteção de dados pessoais no momento da contratação e, no mínimo, anualmente, mantendo a Área de Compliance o registro de participação.

Os Colaboradores firmam termo de ciência desta Política e de confidencialidade, nos termos do artigo 12 das Regras e Procedimentos de Deveres Básicos da ANBIMA.

7. Anexos

5.1. Modelos de Comunicação

7.1.1. Modelo de Comunicação à ANPD

COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA — LGPD

À Autoridade Nacional de Proteção de Dados (ANPD)

1. IDENTIFICAÇÃO DO CONTROLADOR

Razão social: Tera Investimentos Ltda.

CNPJ: 30.782.926/0001-47

Endereço: [endereço completo]

2. IDENTIFICAÇÃO DO ENCARREGADO (DPO)

Nome: [nome do Encarregado]

E-mail: [e-mail de contato]

Telefone: [telefone de contato]

3. DATAS RELEVANTES

Data e hora do conhecimento do incidente pela Gestora: [dd/mm/aaaa, hh:mm]

Data e hora estimada de ocorrência do incidente: [dd/mm/aaaa, hh:mm ou "em apuração"]

Data desta comunicação: [dd/mm/aaaa]

4. DESCRIÇÃO DA NATUREZA DOS DADOS PESSOAIS AFETADOS

Categorias de dados envolvidos: [ex.: nome, CPF, e-mail, dados cadastrais / dados sensíveis, se houver]

Volume estimado de registros afetados: [quantidade ou "em apuração"]

5. INFORMAÇÕES SOBRE OS TITULARES ENVOLVIDOS

Categoria de titulares: [clientes / colaboradores / contrapartes / candidatos à vaga]

Quantidade estimada de titulares afetados: [número ou "em apuração"]

6. MEDIDAS TÉCNICAS E DE SEGURANÇA UTILIZADAS

Descrição das medidas técnicas e administrativas de proteção vigentes à época do incidente: [ex.: criptografia, controle de acesso, segmentação de rede, backup], observados os segredos comercial e industrial da Gestora.

7. RISCOS RELACIONADOS AO INCIDENTE

Descrição dos riscos e potenciais danos aos Titulares decorrentes do incidente: [ex.: risco de fraude, uso indevido de dados, exposição financeira].

8. MOTIVO DA DEMORA [(se aplicável)]

[Preencher apenas se a comunicação não ocorreu de forma imediata ao conhecimento do incidente; descrever os motivos objetivos da demora]

9. MEDIDAS ADOTADAS OU A SEREM ADOTADAS

Medidas de contenção já implementadas: [ex.: revogação de acessos, isolamento de sistemas, notificação a fornecedores envolvidos]

Medidas corretivas planejadas para mitigar efeitos e evitar recorrência: [descrever]

10. RESPONSÁVEL PELA COMUNICAÇÃO

Nome: [nome do Encarregado ou responsável]

Assinatura/cargo: [Encarregado de Dados Pessoais ou Tera Investimentos Ltda.]

7.1.2. Modelo de Comunicação aos Titulares

Assunto: Comunicado importante sobre a segurança dos seus dados pessoais

Prezado(a) [nome do Titular],

Estamos entrando em contato para informar sobre um incidente de segurança que pode ter afetado alguns dos seus dados pessoais tratados pela Tera Investimentos Ltda.

Descrição da ocorrência:

[Descrever de forma simples e direta o que ocorreu, evitando termos técnicos — ex.: "identificamos um acesso não autorizado a um de nossos sistemas" ou "um e-mail contendo seus dados foi enviado indevidamente a um destinatário incorreto"]

Quando ocorreu e quando identificamos: O incidente ocorreu em [data ou período estimado] e foi identificado por nossa equipe em [data].

Quais dados foram envolvidos:

[Listar de forma objetiva, ex.: nome completo, CPF, e-mail. Caso envolva dado sensível, destacar isso claramente]

O que já fizemos:

Assim que identificamos o incidente, adotamos as seguintes medidas:

[ex.: "bloqueamos o acesso afetado", "notificamos as autoridades competentes", "reforçamos os controles de segurança do sistema envolvido"].

O que recomendamos que você faça:

[Orientações práticas e proporcionais ao risco, ex.: "fique atento a mensagens ou ligações suspeitas em seu nome", "evite compartilhar informações adicionais caso seja contatado por terceiros não identificados",

"altere sua senha de acesso ao nosso portal, por precaução"]

Em caso de dúvidas:

Nosso Encarregado de Dados Pessoais está à disposição para esclarecimentos pelo e-mail [e-mail do Encarregado] ou telefone [telefone e e-mail do Encarregado].

Reforçamos nosso compromisso com a proteção dos seus dados pessoais e lamentamos qualquer transtorno causado por este incidente.

Atenciosamente,

Tera Investimentos Ltda.

[Nome do Encarregado]

Encarregado de Dados Pessoais (DPO)

Observações:

- Preencher e enviar a comunicação aos Titulares somente após (ou simultaneamente a) a comunicação à ANPD, mantendo consistência entre as duas versões quanto aos fatos descritos.
- Guardar cópia de ambas as comunicações, com data e hora de envio, no registro de incidentes mantido pelo Encarregado (mínimo de 5 anos), conforme já previsto no fluxo interno de resposta a incidentes.
- A comunicação à ANPD deve ser apresentada por meio do formulário eletrônico disponibilizado pela Autoridade em seu sítio na internet. Este modelo destina-se à organização prévia das informações e ao registro documental da ocorrência.