Política de Privacidade e Proteção de Dados

1. Introdução

O Instituto Basta trata diariamente informações extremamente sensíveis relacionadas à proteção, prevenção e atendimento de vítimas de violência sexual, exploração e tráfico de pessoas. Nesse contexto, a privacidade e a segurança dos dados não são apenas exigências legais, mas constituem um compromisso ético e institucional fundamental para garantir a dignidade, a segurança e o bem-estar de todas as pessoas atendidas, colaboradoras, voluntárias e parceiras.

A Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018) estabelece regras claras para o tratamento de dados pessoais e sensíveis, especialmente aqueles que, se expostos indevidamente, podem causar danos emocionais, físicos, morais e sociais aos titulares. Como organização social, o Instituto Basta adota medidas proporcionais firmes o suficiente para assegurar que toda informação seja tratada com rigor, responsabilidade e transparência.

Esta Política de Privacidade e Proteção de Dados estabelece os princípios, responsabilidades e procedimentos que orientam a coleta, o uso, o

armazenamento, o compartilhamento e o descarte de dados, garantindo conformidade com a legislação, segurança na operação institucional e confiança por parte das pessoas atendidas e da sociedade. Ao fortalecer práticas de governança e proteção de dados, o Instituto Basta reafirma seu compromisso com a integridade, a ética e a proteção integral das vítimas, pilares essenciais para sua missão.

2. Objetivos

Estabelecer diretrizes para **coleta, armazenamento, tratamento, uso, compartilhamento, segurança e descarte** de dados pessoais e sensíveis tratados pelo Instituto Basta, assegurando:

- Privacidade e sigilo das informações;
- Proteção reforçada a vítimas de violência sexual e tráfico humano;
- Conformidade com a **Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018)** e demais normas nacionais e internacionais aplicáveis.

3. Definições Essenciais

- **Dados pessoais:** informação que permite identificar uma pessoa (ex.: nome, endereço, telefone).
- **Dado pessoal sensível:** informações sobre saúde, vida sexual, dados sociais, religiosos, étnicos, biométricos ou qualquer dado que, se exposto, possa gerar risco ao titular.
- **Titular:** pessoa a quem os dados se referem.
- **Tratamento:** qualquer uso do dado (coletar, armazenar, acessar, compartilhar, analisar, excluir etc.).
- **Controlador:** Instituto Basta (quem decide como os dados são utilizados).

- **Operador:** pessoa ou organização que realiza algum tratamento em nome do Instituto.
- **Incidente de Segurança:** acessos não autorizados, vazamentos, perda ou uso inadequado.
- **Núcleo de Acolhimento:** onde estão os profissionais especializados no atendimento e proteção das vítimas.

4. Princípios Orientadores

O tratamento de dados pelo Instituto Basta seguirá os princípios da LGPD:

4.1 Finalidade

Uso dos dados apenas para propósitos legítimos, específicos e informados.

4.2 Adequação

O tratamento deve ser compatível com a finalidade declarada.

4.3 Necessidade

Coleta mínima indispensável, evitando excessos.

4.4 Transparência

Informações claras, acessíveis e atualizadas aos titulares.

4.5 Segurança

Medidas técnicas e administrativas proporcionais ao porte do Instituto Basta, incluindo:

- criptografia de documentos digitais;
- controles de acesso;
- uso de senhas fortes;
- armazenamento seguro físico e digital;
- backup periódico.

4.6 Prevenção

Adoção de práticas que reduzam risco de incidentes de segurança.

4.7 Não Discriminação

Proibição de uso discriminatório dos dados.

4.7 Responsabilização e Prestação de Contas

Registro e demonstração das medidas adotadas para proteção dos dados.

5. Dados Tratados pelo Instituto Basta

5.1 Dados Pessoais

- Nome completo
- Data de nascimento e idade
- Gênero (quando necessário para atendimento)
- Contatos (telefone, e-mail)
- Endereço
- Documentos pessoais (CPF, RG)

5.2 Dados Sensíveis

Tratados somente quando estritamente necessários e mediante consentimento ou base legal específica.

- Histórico de violência, exploração e vulnerabilidades
- Informações de saúde física e mental
- Dados sobre raça/etnia, religião ou convicção filosófica (somente quando houver relevância para o atendimento)
- Registros psicológicos e sociais

5.3 Dados Institucionais

- Relatórios de atendimento
- Laudos e avaliações técnicas
- Registros administrativos
- Comunicações internas e externas relacionadas ao atendimento

6. Base legal para o Tratamento

O Instituto Basta utiliza as hipóteses legais previstas nos arts. 7º e 11 da LGPD:

- Consentimento do titular
- Cumprimento de obrigação legal (ex.: comunicação obrigatória ao Conselho Tutelar)
- Execução de políticas públicas
- Proteção da vida ou integridade física do titular ou de terceiros
- Prevenção à fraude e segurança dos titulares
- Legítimo interesse, quando aplicável e mediante análise de risco

7. Armazenamento e Proteção de Dados

7.1 Medidas de Segurança Digital

- Computadores protegidos por senha individual
- Controle de acesso por níveis de permissão
- Armazenamento em nuvem com autenticação de dois fatores
- Criptografia de arquivos sensíveis (PDF protegido, pastas criptografadas ou sistema seguro)

7.2 Medidas de Segurança Física

- Armários trancados exclusivamente para documentos sensíveis
- Acesso restrito ao setor de atendimento

- Termos de confidencialidade assinados por toda equipe e voluntários
- PROIBIÇÃO de transportar documentos sensíveis fora da sede sem autorização formal

7.3 Prazo de Retenção

- Dados de atendimento: **até 10 anos**, considerando possíveis demandas judiciais
- Dados administrativos: de acordo com legislação específica
- Após o prazo, os dados são **descartados de forma segura**, mediante:
- fragmentação física;
- exclusão completa e irreversível;
- eliminação digital com a sobrescrição de arquivos.

8. Compartilhamento de Dados

O compartilhamento será mínimo, seguro e baseado em hipótese legal.

8.1 Possibilidades de Compartilhamento

- Órgãos públicos: Conselho Tutelar, Ministério Público, Delegacias especializadas
- Profissionais de saúde, assistência ou jurídico envolvidos no atendimento
- Instituições parceiras mediante termo de confidencialidade
- Plataformas de gestão necessárias à operação do Instituto.

8.2 Regras de Compartilhamento

- Só ocorrerá quando necessário e proporcional
- Sempre com justificativa e registro
- Com consentimento do titular, salvo exceções legais
- Parceiros devem adotar medidas de segurança compatíveis

9. Direitos dos Titulares

Conforme LGPD, os titulares podem solicitar:

- confirmação da existência de tratamento
- acesso facilitado aos dados
- correção de informações
- bloqueio ou anonimização
- eliminação de dados desnecessários
- portabilidade
- informação sobre compartilhamento
- revogação do consentimento
- contestação de decisões automatizadas

Canal de atendimento: institutobasta@gmail.com

10. Responsabilidades Internas

10.1 Da Diretoria Executiva

- Garantir recursos mínimos para implementação da política
- Aprovar revisões e assegurar conformidade institucional

10.2 Da Gerência Institucional

- Manter inventário de dados
- Executar planos de segurança
- Monitorar incidentes
- Criar relatórios e indicadores anuais de conformidade

10.3 Coordenação de Projetos e Atendimentos

- Garantir que apenas dados essenciais sejam coletados

- Orientar equipe e voluntários
- Assegurar sigilo no contato com vítimas

10.4 Equipe e Voluntários

- Cumprir as diretrizes desta Política
- Assinar Termo de Confidencialidade
- Reportar incidentes imediatamente

11. Gestão de Incidentes

Qualquer suspeita de vazamento deve ser comunicada imediatamente à Gerência Institucional.

Fluxo mínimo:

1. **Identificação**
2. **Registro do incidente**
3. **Análise de risco**
4. **Comunicação ao titular e à ANPD**, quando necessário
5. **Mitigação e correção**
6. **Relatório final**

12. Revisão e Atualização

Esta Política será avaliada **anualmente** ou sempre que houver:

- mudanças legais;
- novos sistemas;
- incidentes significativos;
- crescimento institucional que demande novos controles.

13. Vigência

Entra em vigor na data de sua publicação e deve ser amplamente divulgada a:

- equipe técnica;
- voluntários;
- parceiros;
- beneficiários (em versões simplificadas quando necessário).

Ruanda, 16 de Janeiro de 2026. gov.br Documento assinado digitalmente
THAIS ROCHA MUNSTERMANN
Data: 15/01/2026 20:04:30-0300
Verifique em https://validar.iti.gov.br

Aprovado por: _____

ANEXO I - REGISTRO DE INCIDENTE DE SEGURANÇA

Objetivo

Este formulário deve ser utilizado sempre que houver suspeita, indício ou confirmação de incidente envolvendo dados pessoais ou sensíveis relacionados a beneficiários, colaboradores, voluntários, parceiros ou qualquer pessoa atendida pelo Instituto Basta.

1. Identificação do Incidente

- Número do Registro:
- Data e horário da ocorrência:
- Data e horário da detecção:
- Responsável pelo registro: (nome / função / setor)

2. Tipo de Incidente

( ) Vazamento de dados
( ) Acesso não autorizado
( ) Perda ou extravio de documento
( ) Compartilhamento indevido
( ) Ataque ou violação de sistema
( ) Destruição ou modificação de dados
( ) Outro: _____

3. Descrição Detalhada do Incidente

- O que aconteceu?
- Como o incidente foi identificado?
- Quais sistemas, documentos ou arquivos foram afetados?

4. Dados Envolvidos

Assinale os tipos de dados potencialmente comprometidos:

Dados pessoais:

( ) Nome
( ) Contato
( ) Documentos
( ) Endereço

Dados sensíveis:

( ) Histórico de violência
( ) Registros psicológicos
( ) Informações de saúde
( ) Origem racial/étnica
( ) Religião ou convicção

Quantidade aproximada de titulares afetados:
Perfis afetados: (beneficiários, colaboradores, voluntários, parceiros etc.)

5. Impacto e Riscos Identificados

- Possíveis danos à vítima:
  ( ) Exposição pública
  ( ) Risco físico
  ( ) Risco emocional
  ( ) Ameaça à privacidade
  ( ) Discriminação
  ( ) Fraude / golpe
  ( ) Outros: _____

- Avaliação de gravidade (conforme matriz — inserir pontuação):
  Baixo / Moderado / Alto / Crítico

6. Ações Imediatas Adotadas

- Medidas de contenção aplicadas
- Pessoas responsáveis
- Sistemas isolados ou bloqueados
- Comunicação interna realizada

7. Ações Corretivas Implementadas

- Ajustes de segurança
- Responsáveis envolvidos
- Prazos de conclusão

8. Comunicação Externa

- O titular foi comunicado? ( ) Sim ( ) Não
- Autoridades foram notificadas? (ANPD / MP / Delegacia)
- Observações:

9. Encerramento do Incidente

- Data de encerramento
- Responsável pela revisão final
- Lições aprendidas
- Melhorias a implementar

ANEXO II - FLUXO DE TRATAMENTO DE DADOS DE BENEFICIÁRIOS

1. Coleta de Dados

A coleta ocorre somente quando necessária e autorizada, e pode acontecer:

- No acolhimento inicial
- Em atendimentos psicológicos, sociais ou jurídicos
- Em atividades de campo e missões humanitárias
- Por formulários seguros (digitais ou físicos)

Dados sensíveis só serão coletados quando indispensáveis, sempre mediante consentimento ou amparo legal (proteção da vida e segurança do titular).

2. Registro Seguro

Após a coleta:

- Dados são inseridos em plataforma protegida, com controle de acesso (apenas profissionais autorizados).
- Documentos físicos são guardados em armários trancados, dentro de sala restrita.
- Cada beneficiário recebe um **ID interno** (código), reduzindo o uso de nomes reais nos sistemas.

3. Uso dos Dados

Os dados poderão ser utilizados para:

- Atendimento especializado (acolhimento, assistência, encaminhamentos)

- Produção de relatórios técnicos (anonimizados sempre que possível)
- Ações intersetoriais com a rede de proteção
- Monitoramento e avaliação interna

A equipe só acessa **aquilo que é estritamente necessário** para sua atuação (princípio do "menor privilégio").

4. Compartilhamento Controlado

O compartilhamento ocorre **apenas** quando:

- Necessário para proteção da vítima (Conselho Tutelar, MP, CREAS, delegacias)
- Autorizado pelo titular/responsável legal
- Requerido por lei

Antes do envio:

- Avalia-se o mínimo necessário de dados
- Utiliza-se canais seguros (criptografados quando digitais)
- Registra-se o compartilhamento em sistema
- Reforça-se a confidencialidade com parceiros

5. Armazenamento e Proteção

Medidas aplicadas:

- Acesso por login individual e autenticação em dois fatores
- Criptografia
- Backups automáticos
- Monitoramento de acesso usados pela equipe

Documentos físicos recebem etiqueta “CONFIDENCIAL”.

6. Retenção e Descarte

O tempo de guarda segue:

- Prazo legal obrigatório (quando houver)
- Necessidade de continuidade do atendimento

Ao final da vigência:

- Dados físicos são triturados
- Dados digitais são apagados de forma definitiva, sem possibilidade de recuperação
- Registra-se o descarte no “Livro de Controle de Dados”

7. Resposta a Incidentes

Em caso de suspeita ou violação:

1. Registrar o incidente imediatamente (modelo acima)
2. Comunicar a Coordenação de Proteção de Dados
3. Acionar medidas de contenção
4. Avaliar risco e impacto
5. Comunicar titulares e autoridades, quando necessário
6. Implementar ações corretivas
7. Documentar o encerramento

8. Reavaliação Periódica

Todos os fluxos e medidas de proteção passam por revisão:

- Anual
- Ou quando houver mudanças no sistema, equipe ou legislação

Treinamentos obrigatórios são oferecidos a todos os colaboradores e voluntários.