Política de Privacidade e Proteção de dados

2ª versão

Dezembro de 2025

Rua Ó de Almeida, 1083 | CEP: 66053-190 | Belém, Pará, Brasil
F +55 91 3222 6000 | peabiru@peabiru.org.br | www.peabiru.org.br

Créditos

Período do trabalho
Dezembro de 2025

Elaboração da política
Hermógenes Sá

Revisão
João Meirelles
Maíra Parente
Swellen Barbosa

Endereço do Instituto Peabiru
Rua Ó de Almeida, 1083. Reduto.
Belém. Pará. 66.053-190
Tel: (91) 3222.6000

www.peabiru.org.br

Controle de Versões			
Versão	***Data***	***Elaborado por***	***Notas da Revisão***
01	30/11/2021	Hermógenes Sá	
02	30/09/2025	Maíra Parente	Atualização da Política de Privacidade e Proteção de Dados, com fortalecimento das medidas de confidencialidade, segurança da informação, controle de acesso, proteção de dados e procedimentos relacionados à gestão de incidentes, em atendimento às recomendações de auditoria do UNICEF.
02	15/12/2025	João Meirelles	revisado

Sumário

1 Apresentação 5

2 Aplicabilidade e Abrangência 5

3 Definições 5

3.1. Lei Geral de Proteção de Dados (Lei n° 13.709/2018) 5

3.2. Titular de Dados Pessoais 6

3.3. Dados Pessoais 6

3.4. Tratamento de Dados 6

4. Como coletamos seus Dados? 6

5. Quais dados são tratados? 7

5.1. De beneficiários 7

5.2. Visitantes de nosso site e de nossas redes sociais 7

5.3. Participantes em eventos 7

5.4. Pessoas que interagem via demais canais 7

6. Qual a finalidade da coleta e tratamento de seus dados? 8

7. Como funciona o acesso e o compartilhamento de seus dados? 8

8. Quais são os seus direitos e como você pode exercê-los? 9

9. Como seus dados são armazenados e protegidos? 10

9.1. Confidencialidade das Informações 11

9.2. Comunicação de Incidentes 11

9.3. Proteção de Dados Financeiros 11

9.4. Infraestrutura de Armazenamento e Compartilhamento 12

10. Alterações em nossa política de privacidade 12

1 Apresentação

Com o presente documento, queremos tornar públicos nossos processos relacionados à privacidade e à proteção de dados pessoais e assim garantir aos titulares dos dados o direito de saber como tratamos seus dados pessoais em nossas atividades administrativas e de projetos.

Este documento também estabelece as diretrizes internas de segurança da informação do Instituto Peabiru, abrangendo a confidencialidade, a integridade e a disponibilidade dos dados e informações institucionais, incluindo dados financeiros, em conformidade com as melhores práticas e recomendações de auditoria.

Nossa Política de Privacidade e Proteção de Dados Pessoais (Política) tem como princípios fundamentais:

1. o respeito aos seus direitos enquanto titular de dados pessoais;
2. a transparência e a prestação de contas sobre o tratamento de seus dados pessoais;
3. a busca constante de meios seguros para proteger os seus dados tratados por nós e manter a privacidade dos mesmos.

2 Aplicabilidade e Abrangência

Esta Política aplica-se a todos os colaboradores e demais pessoas que representem o Instituto Peabiru. Abrange associados, conselheiros, diretores, funcionários, estagiários, bolsistas, pesquisadores, voluntários, consultores, parceiros, prestadores de serviços, fornecedores, autônomos, bem como terceiros não integrantes dos grupos mencionados, mas que mantenham qualquer forma de relacionamento institucional com o Peabiru.

3 Definições

3.1. Lei Geral de Proteção de Dados (Lei nº 13.709/2018)

Como hoje os dados pessoais são muito importantes para os negócios e são

considerados direitos fundamentais das pessoas, essa lei veio para regular as atividades de tratamento de dados realizadas pelas diversas organizações.

Ela é a regra do jogo! Por um lado, ela determina os deveres e obrigações das entidades que realizam tratamento de dados pessoais, e, por outro,

define quais os direitos dos chamados titulares de dados, ou seja, você. A lei estabelece quais são os seus direitos em relação aos seus dados pessoais.

3.2. Titular de Dados Pessoais

Pessoa física a quem se referem os dados pessoais que são tratados.

3.3. Dados Pessoais

Qualquer informação que possa ser utilizada, individualmente ou em conjunto com outras informações, para identificar uma pessoa natural (pessoa física).

Por exemplo: nome, data de nascimento, gênero, RG, CPF, CNH, endereço, e-mail, número de telefone, profissão, escolaridade, raça/etnia, condições de saúde, convicções religiosas ou políticas, entre outras.

3.4. Tratamento de Dados

Qualquer atividade que seja realizada com a utilização de dados pessoais, como coleta, armazenamento, arquivamento, transferência, processamento, compartilhamento, utilização, acesso, transmissão, difusão, eliminação, entre outras.

4. Como coletamos seus Dados?

Nós coletamos seus dados de algumas formas:

- Se você é beneficiário ou beneficiária de algum de nossos projetos, coletamos seus dados de identificação e socioeconômicos através de nossas pesquisas de campo para diagnóstico e avaliação de seu perfil social, com o objetivo de planejar melhor nossas ações em sua comunidade/município e para gerar estudos que contribuam para a melhoria das condições de vida nesses locais. Algumas vezes, os dados são coletados em reuniões comunitárias através de listas de frequência.
- Se você visita nosso site um “cookie” é inserido em seu navegador por meio de programas de computador do tipo Google Analytics, entre outros. Basicamente, esses programas coletam, de forma anônima, o número de vezes que vocês nos visitaram, seu endereço IP, localização geográfica, tipo de navegador, duração da visita e páginas visitadas.
- Se você visita nossos perfis em sites de mídias sociais, como Instagram, Facebook, LinkedIn e Twitter, através destes sites

armazenamos dados de visitação referentes a gênero, faixa etária e localização de acessos.

- Se você participou de algum evento organizado ou apoiado pelo Instituto Peabiru e preencheu o formulário de inscrição e/ou de avaliação, provavelmente seus dados foram coletados e armazenados por nós para futuros convites.
- Se você nos enviar um e-mail ou entrar em contato por algum outro canal, como por exemplo o WhatsApp, fornecendo seus dados, nós armazenamos essas informações para manter o histórico da relação e agilizar futuras interações com o Instituto Peabiru.

5. Quais dados são tratados?

5.1. De beneficiários

Dados de identificação (nome, data de nascimento, local de nascimento), demográficos (idade, gênero, nível de escolaridade, renda aproximada, informações sobre a família), de localização (endereço, comunidade, município, localização georreferenciada), relacionados à produção (área em produção, atividades agrícolas, mão de obra, entre outras) e de acesso a políticas públicas.

5.2. Visitantes de nosso site e de nossas redes sociais

Em nosso site, são coletadas informações sobre preferências, páginas acessadas e conteúdos consumidos, tais como vídeos assistidos e/ou arquivos baixados.

Em nossas redes sociais, são coletadas informações referentes ao perfil do usuário, como nome e link de suas redes sociais. De forma não identificada são coletados dados referentes a gênero, faixa etária e localização dos perfis visitantes.

5.3. Participantes em eventos

Informações fornecidas no cadastro e/ou nas avaliações, tais como nome, telefone, e-mail, número de WhatsApp, endereço, idade e local de origem.

5.4. Pessoas que interagem via demais canais

Podem ser coletados e armazenados dados e documentos fornecidos no histórico de relacionamento ao contatar o atendimento ao público, o setor administrativo, financeiro, de recursos humanos ou de projetos.

6. Qual a finalidade da coleta e tratamento de seus dados?

Os dados coletados em pesquisas de campo servem para mensurar os impactos de nosso trabalho junto aos beneficiários e comunicar às demais partes interessadas sobre o progresso dessa dinâmica de transformação social. Na maioria das vezes, esses dados são agregados e essas informações anonimizadas e então publicados em forma de estudos e pesquisas para serem debatidos pela sociedade em geral.

Os dados coletados nos demais canais de relacionamento são usados para aprimorar a comunicação para o engajamento e mobilização social de nossos parceiros, públicos e demais partes interessadas em nossas atividades.

7. Como funciona o acesso e o compartilhamento de seus dados?

Na grande maioria das vezes, apenas nossos colaboradores e terceiros que prestam serviços em nosso nome terão acesso aos seus dados e informações pessoais. No entanto, em situações nas quais a coleta de seus dados ocorra em eventos ou projetos realizados em parceria, seus dados poderão ser compartilhados com financiadores ou parceiros explicitamente identificados.

Nessas situações, exigiremos a observância à LGPD e à nossa política de privacidade e proteção de dados, bem como o cumprimento de acordos de confidencialidade celebrados entre as Partes.

Contudo, nunca venderemos, alugaremos ou repassaremos seus dados pessoais para terceiros fora desses contextos, a não ser em casos em que essas informações sejam exigidas judicialmente ou pelo Poder Público.

O acesso aos dados pessoais e informações institucionais será restrito aos colaboradores, parceiros e prestadores de serviço que necessitem dessas informações para execução de suas atividades, observando os princípios da necessidade, finalidade, confidencialidade e segurança da informação.

Todos os terceiros que tenham acesso a dados pessoais ou informações institucionais deverão atuar em conformidade com esta Política, com a Lei Geral de Proteção de Dados (LGPD) e com eventuais acordos de confidencialidade firmados com o Instituto Peabiru.

Para operacionalizar esses princípios, o acesso ao ambiente de armazenamento em nuvem do Instituto Peabiru (Google Drive) é estruturado conforme a matriz de permissões abaixo, que define os níveis de acesso de acordo com o cargo e a necessidade funcional de cada colaborador:

Matriz de acesso Google Drive

Cargo/Função	***Nível de Permissão no Google Drive***	***O que pode fazer na prática?***	***Pastas que deve ter acesso***
Gestor / Diretor	***Administrador*** (Manager)	Gerencia membros do Drive, exclui arquivos permanentemente, cria novas pastas raiz e altera configurações.	***Acesso Total:*** Finanças, RH, Governança, Captação e Projetos.
Gerente	***Gerenciador de conteúdo*** (Content Manager)	Adiciona, edita, move e exclui arquivos dentro das pastas. Não pode remover membros nem deletar o Drive Compartilhado.	***Acesso Setorial:*** Pastas da sua área de atuação (ex: Projetos e Captação) + Leitura em Finanças.
Analista	***Colaborador*** (Contributor)	Pode criar e editar arquivos, mas ***não pode mover ou excluir arquivos/pastas*** (isso evita que apaguem coisas sem querer).	***Acesso Técnico:*** Pastas específicas de trabalho (ex: "Fotos de Eventos", "Relatórios Técnicos").
Auxiliar	***Comentarista*** ou ***Colaborador*** (depende da pasta)	Faz lançamentos e atualizações pontuais. Em pastas de prestação de contas, apenas comenta para validação do analista.	***Acesso Operacional:*** Pasta de "Triagem", "Entradas/Notas Fiscais" e "Logística".
Voluntário	***Leitor*** (Viewer) ou Acesso Individual por Link	Apenas visualiza documentos necessários para a ação (escalas, manuais). ***Nunca*** tem acesso à pasta raiz do Drive.	***Acesso Pontual:*** Apenas a arquivos específicos compartilhados diretamente com o e-mail dele.

8. Quais são os seus direitos e como você pode exercê-los?

Nós garantimos, de forma gratuita, aos titulares de dados, mediante requisição, o exercício de seus direitos de:

1. saberem da existência de tratamento de seus dados pessoais em nossa organização;
2. conhecerem quais dados pessoais seus são tratados;

3. terem seus dados pessoais corrigidos e/ou atualizados em nosso banco de dados;
4. serem informados sobre com quais organizações seus dados são compartilhados;
5. revogarem o consentimento fornecido anteriormente;
6. se oporem ao tratamento de seus dados pessoais.

As solicitações e requisições deverão ser encaminhadas por escrito para o e-mail ***meusdados@peabiru.org.br*.**

9. Como seus dados são armazenados e protegidos?

Todos os dados e informações pessoais coletados em nossos processos institucionais serão tratados em conformidade com a Lei Geral de Proteção de Dados (LGPD) e demais normativas aplicáveis.

O Instituto Peabiru adota medidas técnicas e administrativas destinadas à proteção dos dados pessoais e informações institucionais contra acessos não autorizados, perda, destruição, alteração, divulgação, compartilhamento indevido ou qualquer forma de tratamento inadequado ou ilícito.

Entre as medidas adotadas estão:

- controle de acesso aos sistemas e documentos conforme perfil e necessidade funcional;
- utilização de senhas individuais e restrição de acessos;
- armazenamento de informações em ambientes físicos e digitais seguros;
- realização de backups periódicos;
- utilização de ferramentas e sistemas com mecanismos de segurança;
- manutenção de histórico automático de acessos e alterações em documentos críticos, especialmente financeiros, permitindo identificar quem acessou, quando e o que foi modificado, como forma de garantir a integridade das informações e rastrear eventuais irregularidades;
- adoção de plano de continuidade operacional para garantir a disponibilidade de dados e sistemas críticos em caso de falhas técnicas, sinistros ou outros eventos disruptivos;
- preservação da confidencialidade das informações por colaboradores, parceiros e prestadores de serviço;
- descarte seguro de documentos físicos e digitais que contenham dados pessoais ou informações sensíveis.

O Instituto Peabiru também adota procedimentos internos para identificação, comunicação e tratamento de incidentes de segurança que possam comprometer a confidencialidade, integridade ou disponibilidade dos dados pessoais tratados pela instituição.

Ainda que sejam adotadas medidas adequadas de segurança da informação, o Instituto Peabiru reconhece que nenhum sistema é integralmente livre de riscos, inclusive decorrentes de atos de terceiros ou eventos externos imprevisíveis.

9.1. Confidencialidade das Informações

Todos os colaboradores, parceiros, consultores, fornecedores e prestadores de serviço que tenham acesso a dados pessoais ou informações institucionais deverão manter sigilo e confidencialidade sobre as informações acessadas, sendo vedada sua utilização, compartilhamento ou divulgação para finalidades distintas das autorizadas pelo Instituto Peabiru ou previstas em lei, conforme Termo de Confidencialidade e Sigilo (Anexo I).

9.2. Comunicação de Incidentes

Qualquer incidente de segurança envolvendo dados pessoais ou informações institucionais, incluindo perda, acesso indevido, vazamento, destruição ou compartilhamento não autorizado de informações, deverá ser comunicado imediatamente à gestão responsável para adoção das medidas cabíveis de contenção, mitigação, apuração e eventual comunicação às autoridades competentes e titulares dos dados, quando aplicável.

9.3. Proteção de Dados Financeiros

Os dados financeiros do Instituto Peabiru — incluindo registros contábeis, relatórios de prestação de contas, informações bancárias, planilhas orçamentárias, notas fiscais e documentos correlatos — são considerados informações de caráter sensível e estão sujeitos a salvaguardas específicas, em linha com as recomendações de boas práticas de auditoria e com os requisitos dos financiadores e parceiros institucionais.

Para garantir a confidencialidade, a integridade e a disponibilidade dos dados financeiros, o Instituto Peabiru adota as seguintes medidas:

- Confidencialidade: acesso restrito aos colaboradores do setor financeiro e gestão, conforme matriz de acesso definida nesta Política; proibição de compartilhamento com terceiros sem autorização prévia da diretoria; e assinatura de termo de sigilo por todos os envolvidos no manuseio dessas informações.
- Integridade: manutenção de histórico de versões e registros de auditoria de alterações em documentos financeiros; procedimentos de conferência periódica dos registros; e proibição de exclusão ou modificação de documentos sem autorização formal.

- Disponibilidade: realização de backups periódicos dos documentos financeiros com verificação de restauração; armazenamento em ambiente de nuvem seguro com redundância (Google Workspace Nonprofit); e definição de procedimentos para recuperação em caso de perda ou indisponibilidade dos dados.

9.4. Infraestrutura de Armazenamento e Compartilhamento

O Instituto Peabiru utiliza o ***Google Workspace Nonprofit*** (Google Drive) como plataforma principal de armazenamento e compartilhamento de documentos institucionais, por meio da estrutura de ***Drives Compartilhados*** (***Shared Drives***), que permite controle centralizado de permissões e rastreabilidade de acessos.

As seguintes configurações de segurança estão ativas na plataforma:

- ***Restrição de acesso para contas externas:*** voluntários e colaboradores eventuais têm acesso limitado a arquivos específicos compartilhados individualmente, sem acesso às pastas raiz ou a documentos institucionais sensíveis, como dados financeiros, de beneficiários ou de doadores.
- ***Bloqueio de download e cópia:*** arquivos que contenham dados de doadores, beneficiários ou informações financeiras têm o download e a cópia desativados, impedindo que o conteúdo seja extraído para dispositivos ou contas pessoais.
- ***Gerenciamento centralizado de permissões:*** o acesso é concedido e revogado pela gestão, conforme a matriz de permissões definida na seção 7 desta Política, garantindo que apenas colaboradores autorizados acessem cada conjunto de informações.

10. Alterações em nossa política de privacidade

Entendemos que é um desafio constante manter um ambiente organizacional que respeite os princípios da LGPD e, com isso, os direitos de você, titular de dados pessoais. Sendo assim, estaremos em aprimoramento constante de nossos processos de tratamento de dados, o que poderá eventualmente resultar em ajustes e alterações da presente política de privacidade.

Esta Política poderá ser revisada e atualizada periodicamente em razão de alterações legislativas, recomendações de auditoria, aprimoramento dos processos internos e atualização das medidas de segurança e proteção de dados adotadas pelo Instituto Peabiru.

ANEXO I

Termo de Confidencialidade e Sigilo

Pelo presente instrumento, de um lado:

INSTITUTO PEABIRU, pessoa jurídica de direito privado, sem fins lucrativos, inscrita no CNPJ sob o nº 02.650.035/0001-00, com sede em Belém, Estado do Pará, doravante denominado simplesmente ***INSTITUTO***; e

De outro lado: ***[Nome Completo do Colaborador]***, ***[Nacionalidade]***, ***[Estado Civil]***, ***[Profissão]***, portador da cédula de identidade RG nº ***[Número]*** e inscrito no CPF sob o nº ***[Número]***, residente e domiciliado na ***[Endereço Completo]***, doravante denominado simplesmente ***COLABORADOR***.

As partes têm, entre si, justo e acordado o presente Termo, mediante as seguintes cláusulas e condições:

Cláusula 1ª – Do Objetivo

O presente termo tem por objetivo assegurar o sigilo, a proteção e a integridade de todas as ***Informações Confidenciais*** a que o COLABORADOR tiver acesso em razão de suas funções no INSTITUTO, regulamentando especificamente as normas de segurança para o acesso a arquivos armazenados em ***ambiente virtual/nuvem (Google Drive)*** e o manuseio de ***documentos físicos***.

Cláusula 2ª – Do Acesso e Uso de Dados em Nuvem (Google Drive e Servidores)

Com relação ao acesso aos arquivos digitais, bancos de dados, planilhas e pastas compartilhadas na nuvem do INSTITUTO, o COLABORADOR compromete-se a:

1. ***Acesso Pessoal e Intransferível:*** Utilizar estritamente o e-mail institucional ou a conta expressamente autorizada pelo INSTITUTO

para acessar o Google Drive/servidores. É terminantemente proibido compartilhar credenciais de acesso (usuários e senhas) com terceiros, inclusive com outros colaboradores não autorizados para aquela pasta específica.

2. ***Proibição de Cópias Não Autorizadas:*** Não realizar o ***download*** (baixar), exportação, duplicação ou transferência de arquivos, relatórios ou bases de dados da nuvem para dispositivos particulares (computadores pessoais, celulares, ***pendrives***) ou contas de e-mail pessoais, salvo quando estritamente necessário para o cumprimento de suas funções e com autorização prévia.
3. ***Dispositivos Seguros:*** Acessar o ambiente de nuvem do INSTITUTO preferencialmente a partir de hardware fornecido pela organização ou, caso utilize dispositivo próprio, garantir que este possua antivírus atualizado e sistemas de proteção ativos.
4. ***Revogação de Acesso:*** Reconhecer que o INSTITUTO poderá, a qualquer momento e a seu critério, alterar, limitar ou revogar as permissões de acesso a pastas, arquivos ou ferramentas na nuvem.

Cláusula 3ª – Do Manuseio e Guarda de Documentos Físicos

Com relação aos documentos impressos, relatórios físicos, questionários de pesquisa de campo, contratos e livros contábeis de propriedade do INSTITUTO, o COLABORADOR obriga-se a:

1. ***Restrição de Circulação:*** Não retirar das dependências do INSTITUTO, ou dos locais de pesquisa de campo validados, qualquer documento físico original ou cópia, sem a prévia e expressa autorização da coordenação ou diretoria.
2. ***Guarda Segura:*** Zelar pela integridade física dos documentos sob sua responsabilidade, mantendo-os guardados em locais apropriados (arquivos, armários ou gavetas), evitando a exposição visual a terceiros ou visitantes e prevenindo perdas, extravios ou danos.
3. ***Descarte Seguro:*** Não descartar documentos impressos que contenham informações confidenciais ou dados pessoais em lixo comum. Fragmentos ou descarte de rascunhos com dados sensíveis devem ser destruídos mecanicamente de forma a impedir sua leitura ou reconstrução.

Cláusula 4ª – Da Proteção de Dados Pessoais (LGPD) e Comunidades

O COLABORADOR declara estar ciente de que as bases de dados (virtuais ou físicas) do INSTITUTO contêm dados pessoais e sensíveis regulamentados pela Lei Geral de Proteção de Dados (LGPD), incluindo informações cadastrais de doadores e parceiros, dados financeiros e contábeis da instituição, dados da equipe, e dados socioeconômicos e culturais coletados junto a povos e comunidades tradicionais da Amazônia. Compromete-se a não expor, compartilhar ou utilizar de forma inadequada qualquer dessas informações, para finalidades distintas das autorizadas pelo INSTITUTO.

Cláusula 5ª – Da Devolução e Exclusão de Arquivos ao Término do Vínculo

No momento do encerramento de seu vínculo profissional ou prestação de serviços com o INSTITUTO, o COLABORADOR deverá, no prazo máximo de 5 (cinco) dias úteis:

- Entregar imediatamente todos os documentos físicos, pastas e relatórios que estejam sob sua posse;
- Excluir permanentemente de seus dispositivos particulares quaisquer arquivos, fotografias, planilhas ou PDFs baixados do Drive institucional, sendo vedada a retenção de cópias de salvaguarda (***backup***);
- Estar ciente de que seus acessos corporativos (e-mail institucional e permissões no Google Drive) serão sumariamente revogados.

Cláusula 6ª – Da Vigência

A obrigação de sigilo, confidencialidade e não utilização dos dados em nuvem ou físicos aqui estipulada entra em vigor na data de sua assinatura e permanecerá válida por um período de ***5 (cinco) anos*** após o término formal do vínculo do COLABORADOR com o INSTITUTO.

Cláusula 7ª – Das Penalidades

O descumprimento de qualquer das obrigações de segurança digitais ou físicas previstas neste termo constituirá infração grave, sujeitando o COLABORADOR a:

- Rescisão imediata do contrato de trabalho por justa causa, ou rescisão motivada do contrato de prestação de serviços;
- Responsabilização civil integral por perdas e danos, danos reputacionais causados ao INSTITUTO e multas decorrentes de incidentes com a LGPD;

- Notificação às autoridades competentes em caso de crime de violação de segredo profissional ou furto de dados (Código Penal Brasileiro).

Cláusula 8ª – Do Foro

Para dirimir quaisquer controvérsias oriundas do presente termo, as partes elegem o Foro da Comarca de ***Belém/PA***, com renúncia expressa a qualquer outro.

Belém/PA, ***[Dia]*** de ***[Mês]*** de ***[Ano]***.

INSTITUTO PEABIRU

COLABORADOR

[Nome Completo do Colaborador]