1. OBJETIVO

A presente Política Corporativa tem como objetivo estabelecer diretrizes para assegurar a privacidade e a proteção dos dados pessoais de forma eficiente, segura e transparente, garantindo a disponibilidade, integridade, autenticidade, confidencialidade e o tratamento adequado das informações, em conformidade com a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) e com os normativos internos da FINDES e de suas entidades.

2. ABRANGÊNCIA

Esta Política aplica-se aos titulares de dados pessoais que mantenham qualquer relação com as entidades que compõem a FINDES, quais sejam: FINDES, CINDES, SESI-ES, SENAI-ES, IEL-ES, IDEIES e CONEF, doravante denominadas, em conjunto, "FINDES", incluindo usuários dos sites institucionais, clientes, parceiros, candidatos em processos seletivos, prestadores de serviços, representantes legais de empresas parceiras, contratantes ou contratadas, empregados, colaboradores e demais titulares cujos dados pessoais sejam tratados pela FINDES.

3. DOCUMENTOS COMPLEMENTARES

- Lei nº 13.709/2018 – LGPD - Lei Geral de Proteção de Dados.
- Lei nº 12.527/2011 de Acesso à Informação (LAI).
- Lei nº 12.965/2014 - Marco Civil da Internet.
- ABNT NBR ISO/IEC 27001 – Tecnologia da Informação – Técnicas de segurança – Sistemas de Gestão de Segurança da Informação – Requisitos.
- ABNT NBR ISO/IEC 27002 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação.
- ABNT NBR ISO/IEC 27701 – Tecnologia da Informação – Técnicas de segurança – gestão da privacidade da informação — Requisitos e diretrizes.
- Código de Ética e Conduta da FINDES.
- POL-FINDES-008 - Gestão de Consequências e Medidas Disciplinares.
- POL-FINDES-005 - Política de Segurança da Informação.
- NOR-FINDES-025 - Uso dos Recursos de Tecnologia da Informação e Comunicação.
- NOR-FINDES-037 – Gestão de documentos.
- Política de Privacidade Externa.
- PRO-GETI-001 - Procedimento de Descarte de Mídia
- PRO-GETI - Procedimento de incidentes de segurança.
- PRO-GECOMP - Plano de Resposta a incidentes com dados pessoais.
- PRO-GECOMP – Procedimento de Plano de Resposta a Incidentes
- PRO-GECOMP-007 – Inventário de dados (revisar e elaborar processos).

4. DEFINIÇÕES

Para a compreensão deste documento adotam-se os seguintes termos e definições:

- **Anonimização:** é o processo pelo qual são utilizados meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

- **Autoridade Nacional de Proteção de Dados – ANPD:** autarquia de natureza especial responsável por zelar pela proteção dos dados pessoais e por regulamentar, implementar e fiscalizar o cumprimento da LGPD, no âmbito de suas competências legais.
- **Ciclo de vida da informação**: para efeito desta política, será considerado o seguinte ciclo de vida da informação: coleta -> retenção -> processamento -> compartilhamento ->eliminação.
- **Consentimento**: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.
- **Dado pessoal:** informação relacionada a pessoa natural identificada ou identificável.
- **Dado pessoal sensível:** 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 uma pessoa natural.
- **Encarregado de Proteção de Dados, Encarregado ou Data Protection Officer ("DPO"):** pessoa indicada, formalmente, pela FINDES para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD. As informações sobre o nosso Encarregado estão disponíveis na página https://findes.com.br/lgpd/encarregadao-de-dados-dpo/.
- **Informação:** conjunto de dados, imagens, textos e quaisquer outras formas de representação, dotadas de significado dentro de um contexto.
- **Incidente de segurança:** qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais.
- **LGPD:** Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais.
- **Pseudoanonimização:** é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.
- **Privacidade de dados:** conjunto de princípios, diretrizes e procedimentos destinados a assegurar o tratamento adequado dos dados pessoais ao longo de seu ciclo de vida, em conformidade com a legislação e os normativos aplicáveis.
- **Proteção de dados pessoais:** para fins desta Política, considera-se a Proteção de Dados Pessoais como uma combinação de dois pilares: segurança da informação e privacidade de dados.
- **Segurança da Informação:** conjunto de medidas técnicas, administrativas e organizacionais adotadas para proteger os dados pessoais e demais informações contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, assegurando, quando aplicável, sua confidencialidade, integridade e disponibilidade.
- **Titular de Dados:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
- **Tratamento de Dados Pessoais ou Tratamento:** 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.

- **Terceiro ou Parceiro:** qualquer pessoa, física ou jurídica, que atue em nome, no interesse ou para o benefício da Findes, preste serviços ou forneça outros bens, assim como Parceiros comerciais que prestem serviços à Findes, diretamente relacionados à obtenção, retenção ou facilitação de negócios, ou para a condução de assuntos da Findes, incluindo, sem limitação, quaisquer distribuidores, agentes, corretores, despachantes, intermediários, Parceiros de cadeia de suprimentos, consultores, revendedores, contratados e outros prestadores de serviços profissionais.
- **RIPD – Relatório de Impacto à Proteção de Dados Pessoais: Documento** elaborado pelo controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais dos titulares, bem como a identificação, avaliação e definição de medidas, salvaguardas e mecanismos de mitigação desses riscos, visando assegurar a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente com seu art. 5º, inciso XVII.
- **Sandbox (Ambiente de Testes Controlado**): Ambiente tecnológico isolado e controlado, utilizado para desenvolvimento, testes, simulações e validação de sistemas, aplicações e soluções tecnológicas, sem comprometer os ambientes de produção. Quando envolver o tratamento de dados pessoais, deve observar os princípios e requisitos da Lei Geral de Proteção de Dados Pessoais (LGPD), incluindo a adoção de medidas técnicas e administrativas de segurança, controle de acesso e, sempre que possível, utilização de dados fictícios, anonimizados ou sintéticos, visando prevenir acessos não autorizados, vazamentos e outros riscos à privacidade e à proteção de dados.
- **Datasets (Conjuntos de Dados):** Coleções organizadas e estruturadas ou não estruturadas de dados, utilizadas para armazenamento, processamento, análise, compartilhamento, desenvolvimento de sistemas e treinamento de modelos de inteligência artificial. Quando contiverem dados pessoais, seu tratamento deverá observar os princípios e requisitos da Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente quanto à finalidade, necessidade, adequação, segurança e prevenção, assegurando a adoção de medidas de proteção, controle de acesso e, sempre que possível, anonimização ou utilização de dados sintéticos, visando minimizar riscos à privacidade e aos direitos dos titulares.
- **LIA – Legitimate Interest Assessment (Avaliação de Legítimo Interesse):** Procedimento documentado de avaliação da possibilidade de utilização do legítimo interesse como base legal para o tratamento de dados pessoais, nos termos do art. 7º, inciso IX, e do art. 10 da Lei Geral de Proteção de Dados Pessoais (LGPD). Consiste na análise da finalidade legítima, da necessidade do tratamento e do balanceamento entre os interesses do controlador ou de terceiros e os direitos e liberdades fundamentais dos titulares, considerando suas legítimas expectativas e os riscos envolvidos. Tem como objetivo fundamentar a utilização dessa hipótese legal e identificar medidas de proteção e salvaguardas adequadas para assegurar a conformidade com a LGPD.
- **Privacy by Design (Privacidade desde a Concepção):** Princípio que estabelece a incorporação de medidas de privacidade e proteção de dados pessoais desde as etapas iniciais de concepção, planejamento e desenvolvimento de processos, projetos, produtos, serviços e sistemas, mantendo-as durante todo o seu ciclo de vida. Tem como objetivo prevenir riscos à privacidade, minimizar a coleta e o tratamento desnecessário de dados pessoais e assegurar a adoção de medidas técnicas e administrativas de segurança, em conformidade com os princípios e requisitos da Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente o disposto no art. 46, § 2º.

5. DIRETRIZES GERAIS

Toda informação gerada ou de responsabilidade da FINDES e suas entidades deve ser preservada de acordo com a necessidade de serviço ou determinação legal. Assim sendo, os usuários devem adotar comportamento seguro e consciente, com o objetivo de preservar e proteger as informações de propriedade e/ou responsabilidade das entidades, com destaque para as diretrizes abaixo:

- Não divulgar informações privilegiadas e/ou sigilosas sem autorização prévia;
- Evitar modificação, despersonalização ou perda da informação;
- Evitar o descarte inseguro das informações;
- Obter o consentimento, quando necessário, para o tratamento de dados pessoais;
- Cumprir as normas, recomendações, orientações de segurança da informação e prevenção de incidentes de segurança da informação publicadas pelas entidades;
- Comunicar ao encarregado do tratamento de dados pessoais qualquer evento que possa colocar em risco os dados pessoais tratados pela FINDES e suas entidades;
- As informações geradas, acessadas, manuseadas, armazenadas ou descartadas pelos dirigentes, colaboradores e terceiros no exercício de suas atividades profissionais com as entidades da FINDES, bem como os demais recursos tangíveis e intangíveis disponibilizados pela instituição a esses atores, são de responsabilidade/controle exclusiva das entidades e devem ser empregadas exclusivamente em atividades de interesse institucional.

6. RESPONSABILIDADES

6.1. ALTA ADMINISTRAÇÃO

- Cabe aos executivos das entidades estabelecer as diretrizes constantes nesta política, alocar os recursos necessários à sua execução e zelar pelo seu cumprimento.

6.2. TODOS OS USUÁRIOS

- Zelar pelo cumprimento das políticas, normas e procedimentos do sistema de segurança da informação;
- Garantir a proteção das informações físicas e eletrônicas, evitando a exposição de dispositivos de armazenamento removíveis, documentos impressos sobre mesas e impressoras, etc;
- Descarte adequado de documentos de acordo com seu grau de classificação;
- Relatar todo e qualquer incidente percebido;
- Participar dos treinamentos desenvolvidos pela organização.

6.3. COMITÊ DE DADOS, SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

- Ofertar parecer sobre privacidade e proteção de dados pessoais nos casos em que for consultado pelo (a) encarregado (a);
- Propor, revisar e supervisionar as políticas e normas corporativas, referente a Segurança e Privacidade de Dados;

- Propor ações de capacitação e conscientização em segurança da informação, definindo o conteúdo, periodicidade e público-alvo;
- Encaminhar ao Comitê de Ética os incidentes em que a apuração indicar possível violação de norma, conduta dolosa ou culposa relevante ou hipótese sujeita à Política de Gestão de Consequências e Medidas Disciplinares, para avaliação e adoção das medidas cabíveis;
- Monitorar as ações decorrentes de incidentes de segurança da informação, solicitações de titulares e Relatórios de Impacto à Proteção de Dados Pessoais que apresentem riscos altos ou muito altos;
- Apoiar a governança de dados, privacidade e segurança da informação, deliberando sobre riscos, RIPDs, indicadores do programa de privacidade, diretrizes de Privacy by Design e aspectos relacionados à adoção e governança de novas tecnologias.

6.4. ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS

- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- Receber comunicações da autoridade nacional e adotar providências;
- Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- Manter registro de incidentes e fragilidades de segurança da informação para apresentação periódica ao Comitê de Dados, Segurança da Informação e Privacidade;
- Reportar quando necessário ao Comitê de Dados, Segurança da Informação e Privacidade, para análise e tomada de decisão;
- Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

6.5. GESTORES DAS ÁREAS/UNIDADES

- Classificar todas as informações pertinentes à sua área/unidades;
- Difundir a Política de Segurança da Informação e viabilizar, no âmbito de sua área de atuação, o treinamento e a conscientização de sua equipe, garantindo o cumprimento de todas as diretrizes e controles definidos.

6.6. GERÊNCIA DE TECNOLOGIA E TRANSFORMAÇÃO DIGITAL

- Administrar e garantir a segurança dos bancos de dados, sistemas e infraestrutura de TI, incluindo ambientes em nuvem;
- Implementar controles técnicos de segurança, disponibilidade, integridade e recuperação dos ativos de informação;
- Apoiar as áreas responsáveis por Privacidade e Segurança da Informação na implementação de controles, avaliações de risco, incidentes e atendimento às demandas relacionadas a dados pessoais.

6.7. GERÊNCIA DE COMPLIANCE E INTEGRIDADE

- **Guardar** os originais desta Política e suas revisões;
- **Divulgar** em canal corporativo a versão atual desta Política.

7. PROTEÇÃO DE DADOS PESSOAIS

Para fins desta Política, a proteção de dados pessoais está estruturada em dois pilares complementares: Segurança da Informação e Privacidade de Dados.

A Privacidade de Dados compreende as diretrizes e os procedimentos aplicáveis ao tratamento de dados pessoais ao longo de seu ciclo de vida, incluindo coleta, retenção, processamento, compartilhamento e eliminação.

A Segurança da Informação é disciplinada pela Política de Segurança da Informação e pelos demais normativos internos aplicáveis, que estabelecem medidas técnicas e administrativas destinadas à preservação da confidencialidade, integridade e disponibilidade das informações.

A proteção de dados pessoais observará os fundamentos previstos no art. 2º da LGPD.

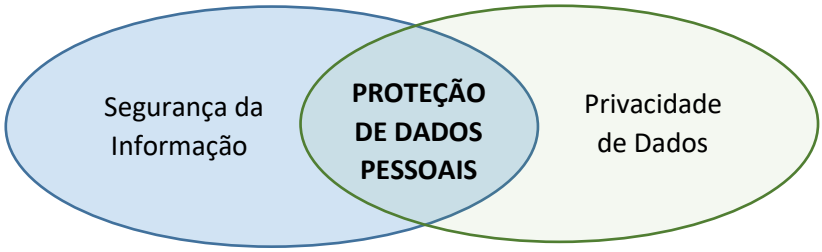


Figura 1: Convergência entre Segurança da Informação e Privacidade de Dados

7.1 Princípios da Proteção de Dados Pessoais

Para o uso adequado dos dados pessoais é necessário que o seu tratamento observe os seus princípios, em especial na coleta, armazenamento, compartilhamento interno e compartilhamento externo, para estar em conformidade com a legislação vigente sobre proteção de dados pessoais.

As atividades de tratamento de dados pessoais deverão observar a boa-fé e os princípios trazidos no artigo 6º da LGPD.

7.2 Ciclo de vida da informação

O ciclo de vida da informação contém etapas e eventos como produção, recebimento, armazenamento, acesso, uso, alteração, cópia, transporte e descarte da informação. Para efeito desta política, será considerado o seguinte ciclo de vida da informação:



- **Coleta:** etapa em que a informação é obtida, recebida ou registrada.
- **Retenção:** consiste no armazenamento da informação, seja em um banco de dados, em um papel, em mídia eletrônica externa, entre outros.
- **Processamento:** essa fase é quando o documento é alterado, consultado, classificado, utilizado, entre outros.
- **Compartilhamento:** ocorre quando a informação é compartilhada com outras unidades de dentro da FINDES ou com terceiros (fornecedor, parceiro, clientes, etc).
- **Eliminação:** essa fase refere-se à eliminação de documento impresso (depositado fragmentado na lixeira e/ou mantido em empresa de armazenagem), eliminação de arquivo eletrônico ou destruição de mídias de armazenamento (por exemplo, CDs, DVDs, disquetes, pen-drives).

7.3 Tratamento de Dados Pessoais

O tratamento de dados pessoais é qualquer ação que se faça com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, compartilhamento, armazenamento, eliminação, modificação ou comunicação.

7.4 Dados coletados e Finalidade

A quantidade e o tipo de Dados Pessoais coletados podem variar de acordo com o contexto da relação firmada com a pessoa relacionada a determinado Dado Pessoal. Assim, prezando pela transparência, listamos abaixo, os Dados Pessoais que poderão ser tratados, de acordo com os diferentes contextos de tratamento, e as finalidades para as quais estes poderão ser utilizados, incluindo, mas não se limitando a:

Dados Pessoais	Tipo de Dado	Finalidade do Tratamento
Nome e e-mail fornecidos por meio do "Fale Conosco"	Dados cadastrais e de contato	Atender solicitações, prestar suporte, responder dúvidas e manter comunicação com o titular.
Dados constantes em currículos e processos seletivos (escolaridade, experiência profissional, competências, qualificações, remuneração, referências, entre outros)	Dados cadastrais, profissionais e educacionais	Conduzir processos de recrutamento e seleção, avaliar candidatos e administrar a relação pré-contratual e contratual.
Informações de saúde (atestados, relatórios médicos, receitas e resultados de exames)	Dados pessoais sensíveis (saúde)	Cumprir obrigações legais e regulatórias, executar contratos, garantir a saúde e segurança ocupacional e prestar os serviços contratados, quando aplicável.
Informações constantes em certidões judiciais e extrajudiciais	Dados cadastrais e informações de natureza judicial	Verificar requisitos legais, regulatórios e contratuais, quando necessário para a prestação dos serviços ou cumprimento de obrigações legais.
Dados para participação em concursos, eventos, treinamentos, capacitações, questionários e pesquisas	Dados cadastrais, profissionais e, quando necessário, dados de participação	Viabilizar a inscrição, organização, execução e gestão de eventos, treinamentos, pesquisas e demais iniciativas promovidas pela instituição.
Dados pessoais e de responsáveis legais para matrícula em cursos	Dados cadastrais, acadêmicos e de identificação	Realizar matrículas, administrar a relação educacional e cumprir obrigações legais e regulatórias aplicáveis.
Dados de prestadores de serviços e representantes de empresas contratadas	Dados cadastrais, profissionais e de contato	Cadastrar fornecedores, formalizar contratos, gerenciar a prestação dos serviços e manter o relacionamento comercial.
Dados de saúde, ocupacionais e profissionais relacionados aos serviços prestados	Dados pessoais sensíveis (saúde) e dados profissionais	Executar os serviços contratados, prestar assistência, cumprir obrigações legais e garantir a adequada execução das soluções ofertadas.
Dados necessários para execução de contratos (associativos, educacionais e outros)	Dados cadastrais, financeiros, profissionais e de identificação	Executar contratos, cumprir obrigações legais e contratuais e administrar a relação com o titular.
Dados fornecidos por meio de formulários, telefone, e-mail, pré-cadastros ou plataformas de comunicação	Dados cadastrais e de contato	Viabilizar o atendimento, responder solicitações, prestar suporte e manter a comunicação com o titular.
Dados coletados por cookies e tecnologias semelhantes	Dados de navegação, identificadores eletrônicos e informações sobre dispositivos	Garantir o funcionamento do site, melhorar a experiência do usuário, realizar análises de uso, reforçar a segurança e, quando aplicável, personalizar conteúdos e serviços.

7.5 Cookies e Links para outros sites



Utilizamos cookies e tecnologias semelhantes para garantir o funcionamento adequado do nosso site, melhorar a experiência de navegação e, quando autorizado pelo titular, coletar informações para fins estatísticos e de marketing.

Os cookies utilizados podem ser classificados da seguinte forma:

- **Cookies necessários (obrigatórios):** são essenciais para o funcionamento do site e para a disponibilização de suas funcionalidades. Esses cookies permitem, por exemplo, o acesso a áreas restritas, garantem a segurança da navegação e possibilitam a correta operação do ambiente. Por serem indispensáveis, não podem ser desativados pelo usuário por meio da ferramenta de gerenciamento de cookies.
- **Cookies estatísticos (opcionais):** coletam informações sobre a forma como os usuários utilizam o site, permitindo a geração de estatísticas e relatórios que auxiliam na melhoria contínua dos nossos serviços. Esses cookies somente serão utilizados mediante o consentimento do titular.
- **Cookies de marketing (opcionais):** são utilizados para compreender os interesses e preferências de navegação do usuário, possibilitando a apresentação de conteúdos e campanhas mais relevantes. Esses cookies também dependem do consentimento do titular para sua utilização.

O titular poderá, a qualquer momento, **aceitar, recusar ou alterar suas preferências em relação aos cookies opcionais**, por meio da Central de Preferências de Cookies disponibilizada em nosso site. A alteração das preferências não afeta a licitude do tratamento realizado antes da revogação do consentimento.

A utilização de cookies necessários independe de consentimento, por serem indispensáveis ao funcionamento do site e fundamentarem-se nas hipóteses legais aplicáveis previstas na Lei Geral de Proteção de Dados (LGPD). Já os cookies estatísticos e de marketing somente serão ativados mediante manifestação de vontade do titular.

Ao acessar links para sites ou aplicativos de terceiros, o usuário estará sujeito às respectivas políticas de privacidade e termos de uso, não cabendo à FINDES o controle sobre o tratamento de dados realizado por essas plataformas.

7.6 Descarte de informações físicas e digitais

Todas as informações em papel ou em qualquer outra mídia que não serão mais utilizadas, devem ser destruídas

antes de serem colocadas no lixo. Além disso, é preciso tomar alguns cuidados ao apagar arquivos no computador porque existem técnicas de recuperação de dados previamente apagados. O descarte de informações deve seguir as seguintes regras:

- Documentos impressos que contenham informações pessoais, financeiras ou outros dados importantes para a FINDES e suas entidades devem ser destruídos e não podem ser reutilizados.
- Periodicamente os usuários devem realizar uma avaliação no conteúdo dos diretórios de rede sob sua responsabilidade com o objetivo de manter no ambiente corporativo apenas informações relevantes.
- Dispositivos de armazenamento (CDs, DVDs, discos rígidos, memórias "flash" e outros meios de armazenamento) devem seguir o procedimento de Descarte de Mídia PRO-GETI-001. Em caso de dúvidas ou necessidade de suporte, a TI está à disposição através de abertura de chamado via Service Desk.

7.7 Tratamento de Dados Sensíveis

Nos termos do art. 5º, II, da LGPD, são considerados dados pessoais sensíveis os dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, dados genéticos e dados biométricos quando vinculados a uma pessoa natural. O tratamento desses dados só poderá ocorrer nas seguintes hipóteses:

I - Quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - Sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) Cumprimento de obrigação legal ou regulatória pelo controlador;

b) Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;

e) Proteção da vida ou da incolumidade física do titular ou de terceiros;

f) Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

g) Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

7.8 Tratamento de Dados Pessoais de Crianças e Adolescentes

Inicialmente para este item trazemos a diferença entre as definições de criança e de adolescente, estabelecidas pelo ECA - Estatuto da Criança e do Adolescente:

- **Adolescente**: Pessoa entre doze e dezoito anos de idade (Art. 2º do ECA).

- **Criança**: Pessoa até doze anos de idade incompletos (Art. 2º do ECA).

O tratamento de dados pessoais de crianças e adolescentes deverá observar o seu melhor interesse e as disposições dos arts. 7º, 11 e 14 da LGPD. Quando o tratamento de dados pessoais de crianças estiver fundamentado no consentimento, este deverá ser específico e em destaque e fornecido por pelo menos um dos pais ou pelo responsável legal, nos termos do art. 14, §1º, da LGPD.

7.9 Compartilhamento de Dados

A FINDES poderá realizar o compartilhamento de dados pessoais com suas entidades, órgãos e entidades públicas, fornecedores, prestadores de serviços, parceiros e demais terceiros, quando necessário ao desenvolvimento de suas atividades e ao cumprimento das finalidades legítimas e previamente estabelecidas para o tratamento.

O compartilhamento de dados pessoais deverá estar amparado em hipótese legal prevista na Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), conforme a natureza dos dados e a finalidade do tratamento, não se limitando ao consentimento do titular.

O compartilhamento deverá observar os princípios e direitos previstos na LGPD, especialmente os princípios da finalidade, adequação, necessidade, livre acesso, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas, devendo ser limitado aos dados pessoais estritamente necessários ao atendimento da finalidade que o justifica.

Sempre que aplicável, a FINDES adotará medidas técnicas, administrativas e contratuais adequadas para assegurar a proteção dos dados pessoais compartilhados, incluindo a definição das responsabilidades dos agentes envolvidos no tratamento, das finalidades autorizadas e das medidas de segurança aplicáveis.

O titular poderá obter informações sobre as entidades públicas e privadas com as quais a FINDES realizou uso compartilhado de seus dados pessoais, nos termos da legislação aplicável e por meio dos canais indicados nesta Política.

7.9.1 Transferência Internacional de Dados

Quando o compartilhamento envolver transferência internacional de dados pessoais, a FINDES observará as disposições da LGPD, especialmente o art. 33, e da regulamentação expedida pela Autoridade Nacional de Proteção de Dados – ANPD, em especial a Resolução CD/ANPD nº 19/2024.

A transferência internacional de dados pessoais somente será realizada quando estiver amparada, simultaneamente, em hipótese legal válida para o tratamento dos dados pessoais, nos termos dos arts. 7º ou 11 da LGPD, conforme aplicável, e em mecanismo válido de transferência internacional, dentre aqueles previstos no art. 33 da LGPD e na regulamentação da ANPD.

A FINDES adotará medidas técnicas, administrativas e contratuais adequadas para assegurar a proteção dos dados pessoais objeto da transferência internacional, considerando a natureza dos dados, a finalidade e o contexto do tratamento e os riscos aos direitos e às liberdades dos titulares.

Quando a transferência internacional estiver fundamentada em cláusulas-padrão contratuais aprovadas pela ANPD, estas deverão ser incorporadas ao respectivo instrumento contratual de forma integral e sem alteração de seu texto obrigatório, observados os requisitos estabelecidos pela regulamentação aplicável.

A FINDES assegurará, ainda, a transparência aos titulares acerca das transferências internacionais realizadas, disponibilizando, nos termos da legislação e da regulamentação aplicáveis, informações claras e acessíveis sobre a realização dessas operações e os meios disponíveis para o exercício dos direitos dos titulares.

7.10 Término do Tratamento de Dados Pessoais

De acordo com a LGPD, o término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

- Verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
- Fim do período de tratamento;
- Comunicação do titular quanto à revogação do consentimento ou solicitação de eliminação dos dados, resguardadas as hipóteses legais de conservação; ou
- Determinação pela autoridade nacional, quando houver violação à proteção de dados pessoais.

Os dados pessoais serão eliminados após o término do tratamento, observados os limites técnicos e as hipóteses de conservação previstas no art. 16 da LGPD e nos normativos internos aplicáveis.

A FINDES segue as diretrizes de retenção e descarte dos dados pessoais nos termos da sua normativa NOR-FINDES-037 – Gestão de documentos.

7.11 Medidas Técnicas e Administrativas para Proteção dos Dados Pessoais

Para manter os dados pessoais protegidos, são usadas ferramentas físicas, eletrônicas e gerenciais direcionadas para a proteção e privacidade, cujo uso leva em consideração a natureza dos dados pessoais coletados, o contexto e a finalidade do tratamento e os riscos que eventuais violações gerariam para os direitos e liberdades do titular dos dados coletados e tratados. Dentre as medidas aplicadas, estão as normativas FINDES listadas no item 3 desta Política.

Devem ser adotadas um conjunto integrado de medidas técnicas, organizacionais e administrativas de segurança para proteger os dados pessoais contra acessos não autorizados, em conformidade com o art. 46 da LGPD. As medidas de proteção são gerenciadas pela POL-FINDES-005 (Política de Segurança da Informação) e compreendem controle de acesso/MFA, criptografia, segurança de rede/EDR, gestão de vulnerabilidades, backups e conscientização, entre outros.

8. INCIDENTE DE SEGURANÇA DA INFORMAÇÃO COM DADOS PESSOAIS

Os incidentes de segurança envolvendo dados pessoais deverão, se aplicável, ser comunicados pelos colaboradores e terceiros à FINDES, por intermédio do DPO, pelos canais internos estabelecidos, para avaliação e adoção das medidas de contenção, investigação, mitigação e resposta cabíveis.

O tratamento dos incidentes deverá observar a LGPD, a Resolução CD/ANPD nº 15/2024 e o procedimento interno aplicável de resposta a incidentes com dados pessoais.

Quando o incidente puder acarretar risco ou dano relevante aos titulares, serão observadas as obrigações de

comunicação à ANPD e aos titulares afetados, nos termos e prazos estabelecidos na legislação e na regulamentação aplicáveis.

9. DIREITO DOS TITULARES

A LGPD assegura aos titulares de dados pessoais, a qualquer momento e mediante requisição, com base no art. 18, os seguintes direitos:

(i) Confirmação da existência de tratamento;

(ii) Acesso aos dados;

(iii) Correção de dados incompletos, inexatos ou desatualizados;

(iv) Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD;

(v) Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial;

(vi) Eliminação dos dados tratados com base no consentimento, ressalvadas as hipóteses de conservação previstas em lei;

(vii) Informação sobre entidades públicas e privadas com as quais a FINDES realizou uso compartilhado de dados;

(viii) Informação sobre a possibilidade de não fornecer consentimento e as consequências da negativa;

(ix) Revogação do consentimento;

(x) Revisão de decisões tomadas unicamente com base em tratamento automatizado que afetem os interesses do titular;

(xi) Direito de peticionar em relação aos seus dados perante a Autoridade Nacional de Proteção de Dados – ANPD; e

(xii) Direito de oposição ao tratamento realizado com fundamento em hipótese de dispensa de consentimento, em caso de descumprimento da LGPD, quando aplicável.

Para exercer os direitos como usuário (titular dos dados), acesse https://findes.com.br/lgpd/direitos-do-titular/.

10. AVALIAÇÃO DE RISCOS À PROTEÇÃO DE DADOS PESSOAIS

A FINDES adota, como parte de seu programa de governança em privacidade e proteção de dados pessoais, procedimentos destinados à identificação, avaliação e mitigação dos riscos decorrentes das atividades de tratamento de dados pessoais.

O Relatório de Impacto à Proteção de Dados Pessoais – RIPD será elaborado quando o tratamento puder gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais e às liberdades civis e aos direitos fundamentais dos titulares, quando solicitado pela Autoridade Nacional de Proteção de Dados – ANPD ou nas demais situações previstas na legislação, na regulamentação aplicável ou em normativos internos da FINDES.

Como regra interna de governança, a FINDES poderá determinar a elaboração de RIPD para processos ou operações

consideradas críticas, considerando, entre outros fatores, a natureza e o volume dos dados pessoais tratados, as categorias de titulares envolvidos, a utilização de dados pessoais sensíveis, o emprego de novas tecnologias e a natureza, gravidade e probabilidade dos riscos identificados.

O Teste de Legítimo Interesse – LIA será realizado quando o tratamento de dados pessoais estiver fundamentado no legítimo interesse do controlador ou de terceiros, nos termos do art. 10 da LGPD, com o objetivo de avaliar a finalidade e a legitimidade do interesse perseguido, a necessidade do tratamento, os impactos sobre os direitos e as legítimas expectativas dos titulares e as medidas de salvaguarda aplicáveis.

Os RIPDs e LIAs deverão ser documentados e revisados sempre que houver alteração relevante nas condições que fundamentaram a avaliação, especialmente quanto à finalidade, à natureza ou ao contexto do tratamento, aos dados pessoais envolvidos, às tecnologias utilizadas ou aos riscos aos direitos dos titulares.

11. RETENÇÃO E TEMPORALIDADE DOS DADOS PESSOAIS

Os dados pessoais tratados pela FINDES serão mantidos pelo período necessário ao cumprimento das finalidades que justificaram o seu tratamento, observadas as disposições da legislação aplicável e dos normativos internos de gestão documental.

A definição dos prazos de retenção deverá considerar, conforme aplicável, a finalidade do tratamento, o cumprimento de obrigações legais ou regulatórias, a execução de contratos, o exercício regular de direitos em processos judiciais, administrativos ou arbitrais, os prazos prescricionais aplicáveis e as demais hipóteses que autorizem a conservação dos dados pessoais nos termos da LGPD.

Encerrado o período de retenção e não havendo fundamento legal ou regulatório que justifique a sua conservação, os dados pessoais deverão ser eliminados ou anonimizados, observados os limites técnicos e as hipóteses previstas no art. 16 da LGPD.

Os prazos e critérios de retenção, descarte e destinação dos dados pessoais deverão observar a NOR-FINDES-037 – Gestão de Documentos, bem como os demais instrumentos e normativos internos aplicáveis.

12. USO DE DADOS PESSOAIS EM INTELIGÊNCIA ARTIFICIAL

A utilização de sistemas ou ferramentas de Inteligência Artificial que envolvam o tratamento de dados pessoais deverá estar vinculada a finalidades legítimas, específicas e compatíveis com as atividades institucionais da FINDES, observando as bases legais aplicáveis, os princípios da finalidade, adequação, necessidade, transparência, segurança, prevenção e não discriminação, bem como os demais requisitos previstos na LGPD e nas normas internas aplicáveis.

Sempre que a utilização de Inteligência Artificial envolver decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem os interesses dos titulares, a FINDES assegurará o direito de solicitar a revisão da decisão, nos termos do art. 20 da LGPD, bem como fornecerá, quando solicitado, informações claras e adequadas sobre os critérios e procedimentos utilizados, observados os segredos comercial e industrial.

O tratamento de dados pessoais realizado por meio de soluções de Inteligência Artificial deverá observar, além das disposições desta Política, as diretrizes estabelecidas na POL-FINDES-017 – Política de Inteligência Artificial e os princípios e controles aplicáveis da ISO/IEC 42001.

Deverão ser observados os requisitos relacionados à retenção e ao descarte de logs de auditoria de IA, ao expurgo seguro de dados utilizados em ambientes de teste ou Sandbox ao término dos experimentos, bem como ao descarte seguro de modelos, datasets e demais ativos relacionados à Inteligência Artificial, assegurando a adequada gestão do ciclo de vida dos dados.

13. COMPETÊNCIA

Compete ao Conselho de Administração da FINDES aprovar esta Política Corporativa.

14. DISPOSIÇÕES FINAIS

Os casos omissos, as dúvidas de interpretação e as situações não previstas nesta Política serão avaliados pelo Encarregado pelo Tratamento de Dados Pessoais – DPO e, quando necessário, submetidos ao Comitê de Dados, Segurança da Informação e Privacidade, observadas as competências estabelecidas nos normativos internos da FINDES.

O descumprimento desta Política poderá implicar a aplicação das medidas cabíveis, conforme a natureza e a gravidade da conduta, observados os normativos internos aplicáveis, sem prejuízo das demais responsabilidades previstas na legislação vigente.

Esta Política deverá ser revisada periodicamente ou sempre que houver alterações relevantes na legislação, na regulamentação aplicável, nos processos de tratamento de dados pessoais ou na estrutura de governança de privacidade e proteção de dados da FINDES.

Esta versão substitui e revoga as versões anteriores desta Política.

15. ELABORADORES / REVISORES

Área	Responsável	Cargo
Gerência de Compliance e Integridade	Viviane Dias de Lima	Gerente de Compliance e Integridade
Gerência Executiva de Infraestrutura	Reginaldo Alberto Scheffer	Analista de Infraestrutura SR
Gerência Executiva Jurídica	Daniel Marques Garcia	Gerente Executivo Jurídico

16. CONTROLE DE REVISÕES

Revisão	Data	Descrição
00	22/01/2021	Emissão da Política
01	07/04/2021	Revisão do Formulário fale conosco
02	02/09/2024	Revisão geral do texto
03	22/01/2025	Revisão geral do texto e formalização
04	15/10/2026	Revisão geral do texto