Política Global de Conformidade à LGPD da ETIPI - Empresa de Tecnologia da Informação do Piauí

LGPDNOW

Junho/2025

POLÍTICA GLOBAL DE CONFORMIDADE À LGPD DA EMPRESA DE TECNOLOGIA DA INFORMAÇÃO DO PIAUÍ - ETIPI

1. CONSIDERAÇÕES INICIAIS

A presente Política tem como objetivo estabelecer diretrizes que permitam que a governança em privacidade e a proteção dos dados pessoais da Empresa de Tecnologia da Informação do Piauí - ETIPI seja desenvolvida com parâmetros de eficiência e eficácia, de modo seguro e transparente, garantindo a disponibilidade, integridade, autenticidade, legalidade e sigilo das informações pessoais as quais a organização tem acesso, de forma alinhada aos requisitos legais da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais - LGPD, as demais normas e resoluções, nacionais, estaduais e internas sobre o tema, aplicando-se a todos os órgãos e setores da organização.

2. OBJETIVOS

A presente Política tem os seguintes objetivos:

- **Conformidade com a LGPD:** Assegurar que todas as atividades envolvendo o tratamento de dados pessoais estejam de acordo com a legislação vigente;
- **Proteção de Dados:** Garantir a segurança dos dados pessoais por meio de medidas técnicas e administrativas adequadas;
- **Responsabilidade Organizacional:** Promover uma cultura de responsabilidade no tratamento de dados pessoais entre toda a equipe ETIPI;
- **Gerenciamento de Riscos:** Identificar, avaliar e mitigar riscos relacionados à privacidade e à proteção de dados; e
- **Transparência e Confiança:** Manter um relacionamento transparente com os titulares de dados, comunicando como seus dados são tratados.

3. LEGISLAÇÕES APLICÁVEIS

- Constituição Federal;
- Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais, ou LGPD;
- Decreto Estadual nº 21.979/2023, que institui a Política de Transformação Digital do âmbito do Poder Executivo do Estado, o portal único de serviços, regulamenta as Leis Federais nº 14.129/2021 e 13.460/2017 e dá outras providências;
- Decreto Estadual nº 23.003/2024, que institui a Política Estadual de Proteção de Dados Pessoais e Privacidade;
- Resolução CD/ANPD nº 1/2021, Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados;
- Resolução CD/ANPD nº 15/2024, Regulamento de Comunicação de Incidente de Segurança;
- Resolução CD/ANPD nº 18/2024, Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais;

- Resolução CD/ANPD nº 19/2024, que dispõe sobre a Transferência Internacional de Dados;
- Guia orientativo - atuação do Encarregado pelo tratamento dos dados pessoais;
- Lei nº 12.527/2011, Lei de Acesso à Informação - LAI;
- Lei nº 12.965/2014, Marco Civil da Internet - MCI;
- 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;
- Demais normas relativas ao tema.

4. DEFINIÇÕES IMPORTANTES

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

- **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;
- **Dado anonimizado:** dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
- **Banco de dados:** conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
- **Titular dos dados:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. **Somos nós**;
- **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
- **Encarregado de dados:** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)
- **Autoridade Nacional de Proteção de Dados (ANPD):** órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional;
- **Tratamento dos dados pessoais:** 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;

- **Anonimização:** utilização de 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;
- **Consentimento:** manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
- **Bloqueio:** suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
- **Eliminação:** exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
- **Transferência internacional de dados:** transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
- **Uso compartilhado de dados:** comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;
- **Incidente de segurança:** qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais; e
- **Medidas de segurança:** medidas técnicas e/ou administrativas adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

4. DIRETRIZES GERAIS

Toda informação pessoal tratada pela **ETIPI** deve ser preservada, de acordo com a necessidade de serviço ou determinação legal. Assim sendo, os quem trata dados pessoais em nome da organização, sendo este um funcionário, prestador de serviço, contratado ou terceiro com quem se compartilha dados pessoais para exercício de uma função ou prestação de um serviço, deve adotar um comportamento seguro e consciente, nos termos das normas internas, com o objetivo de preservar e proteger as informações de propriedade e/ou responsabilidade da mesma.

Nesse sentido, além das normativas internas, reitera-se que seja observadas as seguintes orientações/boas práticas:

- Não divulgar informações privilegiadas e/ou sigilosas sem autorização prévia;
- Evitar modificação, despersonalização ou perda da informação;
- Evitar o descarte inseguro das informações;
- Não armazenar, transmitir ou compartilhar conteúdo indevido ou ilegal nos ativos de
- propriedade e/ou responsabilidade da ETIPI;
- 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 pela ETIPI; e

- Comunicar ao encarregado do tratamento de dados pessoais qualquer evento que possa colocar em risco os dados pessoais tratados pela ETIPI.

As informações geradas, acessadas, manuseadas, armazenadas ou descartadas pelos dirigentes, servidores, colaboradores e terceiros, no exercício de suas atividades profissionais com a **ETIPI**, bem como os demais recursos tangíveis e intangíveis disponibilizados pela instituição a esses atores, são de propriedade exclusiva da organização em questão, e devem ser empregadas exclusivamente em atividades de interesse institucional.

5. ESTRUTURA DA GOVERNANÇA EM PRIVACIDADE

A estrutura da Governança em Privacidade está dividida conforme disposto a seguir:

- **Alta Gestão:** É responsável por fornecer suporte institucional e financeiro para a implementação das políticas de privacidade e segurança da informação;

- **Líderes dos setores:** São responsáveis por assegurar que suas equipes cumpram as políticas e procedimentos estabelecidos no Programa de Privacidade;

- **Comitê de Privacidade de Dados:** O Comitê de Privacidade de Dados é o órgão responsável pela definição, implementação e supervisão das políticas de proteção de dados. Suas principais funções incluem: **(i)** Ofertar parecer sobre privacidade e proteção de dados pessoais nos casos em que for consultado pelo Encarregado; **(ii)** Propor, revisar e supervisionar as políticas e normas corporativas, referente a Segurança e Privacidade de Dados; **(iii)** Propor ações de capacitação e conscientização em segurança da informação, definindo o conteúdo, periodicidade e público-alvo; e **(iv)** Encaminhar ao comitê de ética os incidentes ocorridos a fim de avaliar violações e resultados de auditorias do sistema de Segurança da Informação e propor ações para tratá-las;

- **Encarregado pelo tratamento dos dados pessoais (Encarregado de dados ou DPO):** O Encarregado de dados será nomeado através de Portaria devidamente publicada e terá suas funções estabelecidas conforme disposto na Lei nº 13.709/2018, Resolução CD/ANPD nº 18/2024 e outras regulamentações a serem estabelecidas. Para mais informações, foi desenvolvida uma cartilha específica sobre os requisitos, atribuições e demais diretrizes para o exercício da função;

- **Demais pessoas vinculadas à organização:** Todos devem estar cientes e seguir as políticas e orientações da ETIPI, relativas ao tratamento de dados pessoais e participar dos treinamentos sobre privacidade e segurança.

6. DA PROTEÇÃO DE DADOS PESSOAIS

Para fins desta Política, considera-se a proteção de dados pessoais como uma combinação de dois pilares: Privacidade de Dados Pessoais e Segurança da Informação. Tais pilares são abordados

em normativas internas específicas, tais como a Política de Privacidade e a Política de Segurança da Informação da **ETIPI.**

Adicionalmente, a proteção de dados pessoais, segundo a LGPD, tem como fundamentos:

- respeito à privacidade;
- autodeterminação informativa;
- liberdade de expressão, de informação, de comunicação e de opinião;
- inviolabilidade da intimidade, da honra e da imagem;
- desenvolvimento econômico e tecnológico e a inovação;
- livre iniciativa, a livre concorrência e a defesa do consumidor; e
- os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Entende-se por autodeterminação informativa o poder conferido ao titular de dados (ou seja, a quem pertence uma informação) o direito de controlar seus próprios dados pessoais, com base nos princípios listados na LGPD, sendo estes:

- **Boa-fé:** é um princípio jurídico que visa garantir a justiça, a confiança e a segurança nas relações jurídicas. É um acordo implícito que estabelece a expectativa de que as partes envolvidas em uma transação ou acordo ajam com honestidade, integridade e lealdade;
- **Finalidade**: o tratamento de dados pessoais deve ser realizado apenas para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. É vedado o tratamento para outras finalidades e fins discriminatórios ilícitos ou abusivos;
- **Adequação:** o tratamento dos dados deve ser compatível com as finalidades informadas ao titular (Cliente, fornecedor, parceiro, colaborador, entre outros);
- **Necessidade**: o tratamento dos dados deve ser aplicado ao mínimo necessário para a realização das finalidades do tratamento de dados, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação a essas;
- **Livre Acesso:** garante aos titulares de dados pessoais a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
- **Qualidade dos dados**: garante aos titulares de dados pessoais a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
- **Transparência**: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
- **Segurança:** utilização de medidas 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 difusão;

- **Prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

- **Não Discriminação**: não realizar tratamento de dados pessoais para fins discriminatórios ilícitos ou abusivos; e

- **Responsabilização e Prestação de Contas:** demonstração da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Aliado aos princípios, a LGPD dispõe que o tratamento dos dados pessoais e dos dados pessoais sensíveis deve ser realizado de acordo com as bases legais, ou seja, com as hipóteses que autorizam o uso deles.

No caso dos dados pessoais, as hipóteses que autorizam seu tratamento são:

- mediante o fornecimento de consentimento pelo titular;

- para o cumprimento de obrigação legal ou regulatória pelo controlador;

- pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV da LGPD;

- para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

- quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

- para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

- para a proteção da vida ou da incolumidade física do titular ou de terceiros;

- para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

- quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

- para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Já no caso dos dados pessoais sensíveis ou qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica, as bases legais que autorizam o seu uso são estas:

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

- 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, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

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;

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 da LGPD e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Vale mencionar que os princípios e as bases legais devem ser observados em todas as fases do tratamento dos dados pessoais, ou seja, em toda operação realizada com os dados, em todo o ciclo de vida dos dados pessoais.

E o que seria ciclo de vida dos dados pessoais? É, por assim dizer, as 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:** é a etapa onde a informação é criada e manipulada.
- **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 **ETIPI** ou com terceiros (fornecedor, parceiro, clientes, etc). Pode ser entendido como qualquer comunicação, difusão, transferência internacional, interconexão de dados pessoais.

- **Eliminação:** essa fase refere-se à eliminação/descarte 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). Para mais informações sobre as diretrizes e procedimentos de eliminação dos dados pessoais da **ETIPI**, orienta-se a leitura Política de Retenção e Descarte da organização.

Para todas as fases do ciclo de vida dos dados pessoais dentro da organização, as informações tratadas devem ter um setor específico e/ou responsável(eis) definido(s). É o controle de acesso às informações, uma medida técnica administrativa que evita que pessoas diversas tenham acesso às informações que não lhe são úteis ou necessárias. Além disso, em caso de incidentes de segurança com algum dado pessoal, é possível verificar qual o setor e pessoal responsável pelo tratamento dele, auxiliando nas medidas mais efetivas para solucionar o fato.

Nesse sentido, recomenda-se que as informações sejam classificadas de acordo com seu grau de sensibilidade e confidencialidade, assegurando o acesso pelos profissionais devidamente autorizados, de acordo com os critérios dispostos pelos órgãos de controle da transparência e classificação das informações de órgãos públicos estaduais.

Adicionalmente, como boa prática, deve ser observado, ainda, que:

- o conhecimento da informação deve ser usado apenas para os propósitos de interesse da ETIPI;

- toda informação deve possuir um proprietário, responsável por sua classificação que deverá ser determinada no momento de criação;

- as alterações de classificação devem ser providas preferencialmente por quem a classificou originalmente e na sua ausência, por colaboradores que assumiram a sua função ou possuem nível hierárquico superior ao exigido para a sua classificação;

- o descarte de informações classificadas como confidenciais deve ser feito de forma que impossibilite a recuperação; e

- toda informação não classificada será considerada por padrão como interna.

7. TRATAMENTO DE DADOS PESSOAIS DE VULNERÁVEIS

7.1. Crianças e adolescentes

O artigo 227 da Constituição da República Federativa do Brasil, ao reconhecer que crianças e adolescentes estão em uma fase peculiar de desenvolvimento, preceitua que é dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.

Por consequência, a base filosófica da Lei nº 8.069, de 13 de julho de 1990, – Estatuto da Criança e do Adolescente (ECA) – fundado no dever constitucional, é o comprometimento integral com todas as crianças e adolescentes, que, segunto o referido estatuto, define:

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

Alinhada a esses propósitos, a Lei nº 13.709/2028 - Lei Geral de Proteção de Dados Pessoais (LGPD), em seu Capítulo II, reservou uma seção específica para o tema, na qual foi estabelecido um regramento próprio para a proteção de dados pessoais de crianças e adolescentes, baseado, em especial, nos seguintes princípios e regras:

- observar o Enunciado CD/ANPD nº 1/2023, que dispõe que “O tratamento de dados pessoais de crianças e adolescentes poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da Lei Geral de Proteção de Dados Pessoais (LGPD), desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei".
- o princípio do “melhor interesse”, que deve sempre ser observado no tratamento de dados pessoais de crianças e adolescentes;
- o consentimento específico e em destaque, a ser obtido dos pais ou do responsável legal pela criança, quando necessário ao tratamento de seus dados pessoais, cabendo ao controlador realizar todos os esforços razoáveis para verificar a adequação do consentimento fornecido, consideradas as tecnologias disponíveis;
- a impossibilidade de o Controlador exigir o fornecimento de informações pessoais como condição à participação de crianças em jogos, aplicações de internet e outras atividades, ressalvadas as informações estritamente necessárias à atividade em questão; e
- o fornecimento pelos controladores de informações de maneira simples, clara e acessível sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos dos titulares, considerando as suas características físico-motoras, perceptivas, sensoriais, intelectuais e mentais, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

Em conformidade com a Constituição Federal e o Estatuto da Criança e do Adolescente, e considerando especialmente o previsto na LGPD, a Autoridade Nacional de Proteção de Dados – ANPD, autarquia federal de natureza especial, criada com a responsabilidade e competência para zelar pela proteção de dados pessoais no país, estabeleceu a garantia de direitos dos titulares crianças e adolescentes, em particular no ambiente digital, como um dos temas prioritários de sua atuação.

7.2. Demais vulneráveis

Aqui se incluem, mas não se limitam a: idosos, pessoas com deficiência, integrantes de minorias, pessoas com doenças graves e aqueles que:

- As circunstâncias limitam a sua habilidade de fornecer consentimento livre ou de se opor ao tratamento;
- Sua capacidade de compreensão de como os dados são usados, os impactos do tratamento e como se proteger for restrita;
- Há desequilíbrio de poder na relação com o Controlador; e
- Existir situação social, financeira ou de saúde desfavorável do titular.

Nesses casos, para evitar discriminações e a não observância aos direitos daqueles que se enquadrarem nesta categoria é importante que sejam adotadas medidas mais rígidas para garantir a segurança e a confidencialidade dos dados, adaptando os avisos de privacidade e política de atendimento a requisições de titulares em atenção à vulnerabilidade identificada e revisando os processos automatizados, sobretudo para não ampliar vulnerabilidades.

A vulnerabilidade do titular e a restrição de sua capacidade de autodeterminação afeta a forma de informar titulares acerca do tratamento e de solicitar o consentimento, quando necessário.

8. DO 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, resguardado o interesse público; ou
- determinação pela autoridade nacional, quando houver violação à proteção de dados pessoais.

A **ETIPI** realiza o tratamento de dados pessoais pelo tempo necessário para cumprir a finalidade para os quais foram coletados, de acordo com sua base legal. Quando no término do tratamento, os dados pessoais serão eliminados, cumprindo a fase final do ciclo da vida da referida informação junto à organização, sendo autorizada a conservação nas situações previstas na legislação vigente.

Para mais informações sobre as diretrizes e procedimentos de eliminação dos dados pessoais da **ETIPI**, orienta-se a leitura Política de Retenção e Descarte da organização.

9. DOS INCIDENTES DE SEGURANÇA DA INFORMAÇÃO COM DADOS PESSOAIS

Segundo a Resolução CD/ANPD nº 15/2024, que regulamenta a comunicação de incidentes de segurança envolvendo dados pessoais, incidente de segurança pode ser definido como qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais, podendo acarretar risco ou dano relevante aos titulares quando puder afetar significativamente interesses e direitos fundamentais dos titulares e, cumulativamente, envolver, pelo menos, um dos seguintes critérios:

- dados pessoais sensíveis;
- dados de crianças, de adolescentes ou de idosos;
- dados financeiros;
- dados de autenticação em sistemas;
- dados protegidos por sigilo legal, judicial ou profissional; ou
- dados em larga escala.

Para mais informações sobre as diretrizes e procedimentos de eliminação dos dados pessoais da **ETIPI**, orienta-se a leitura do **Manual de Gestão de Incidentes de Segurança com Dados Pessoais da ETIPI e Norma de Gestão de Incidentes**, lembrando que quaisquer dúvidas e que todos os incidentes com dados pessoais devem ser comunicados ao Encarregado de dados (DPO).

10. DOS DIREITOS DOS TITULARES DE DADOS

São direitos dos titulares dos dados, ou seja, seus direitos, previstos no artigo 18 da LGPD, podendo ser obtidos, a qualquer momento e mediante requisição:

- a confirmação da existência de tratamento;
- o acesso aos dados;
- a correção de dados incompletos, inexatos ou desatualizados;
- a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
- a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
- a eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD;
- a informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e
- a revogação do consentimento, mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação.

Para exercer qualquer um desses direitos, o titular deverá entrar em contato, gratuitamente, seja pelo Fala.BR, seja pelo Portal do Titular, ou, ainda, via e-mail do Encarregado de dados (lgpd@saude.pi.gov.br).

Lembrando que há prazos para o atendimento aos direitos dos titulares, podendo ser de até 15 dias corridos a contar da data do protocolo da solicitação ou o prazo da LAI, se a organização for pessoa jurídica de direito público referida no parágrafo único do art. 1º da Lei nº 12.527, de 18 de

novembro de 2011 (Lei de Acesso à Informação), órgãos notariais e de registro, ou empresas públicas e sociedades de economia mista quando do tratamento de dados pessoais para a prestação de um serviço de interesse público.

As tratativas sobre a resposta aos titulares de dados pessoais estão em uma norma interna específica, sendo essa o **Manual para atendimento aos direitos dos titulares de dados da ETIPI.**

11. DA TRANSFERÊNCIA INTERNACIONAL DOS DADOS PESSOAIS

A transferência internacional de dados pessoais foi regulada pela Resolução CD/ANPD nº 19/2024, que dispõe sobre as cláusulas-padrão contratuais, as cláusulas-padrão contratuais equivalentes, às cláusulas contratuais específicas, as normas corporativas globais e as decisões de adequação.

Em cumprimento à LGPD e à resolução acima, a **ETIPI** elaborou a **Norma sobre a transferência internacional de dados pessoais.**

12. DAS RESPONSABILIDADES

O descumprimento desta poderá implicar em penalidades. Por isso, caberá a cada elo envolvido na governança em privacidade executar as ações abaixo registradas:

- **Alta Administração**: estabelecer as diretrizes constantes nesta política, alocar os recursos necessários à sua execução e zelar pelo seu cumprimento.

- **Todos os internos**: **(i)** zelar pelo cumprimento das políticas, normas e procedimentos do sistema de segurança da informação; (**ii)** garantir a proteção das informações físicas e eletrônicas, evitando a exposição de dispositivos de armazenamento removíveis, documentos impressos sobre mesas e impressoras, etc; **(iii)** efetuar o descarte adequado de documentos de acordo com seu grau de classificação; **(iv)** relatar todo e qualquer incidente percebido; e **(v)** participar dos treinamentos desenvolvidos pela organização.

- **Comitê de Proteção de Dados Pessoais: (i)** ofertar parecer sobre privacidade e proteção de dados pessoais nos casos em que for consultado pelo(a) Encarregado(a); **(ii)** propor, revisar e supervisionar as políticas e normas corporativas, referente a Segurança e Privacidade de Dados; **(iii)** propor ações de capacitação e conscientização em segurança da informação, definindo o conteúdo, periodicidade e público-alvo; **(iv)** relatar os incidentes ocorridos, a fim de avaliar violações e resultados de auditorias do sistema de segurança da informação e propor ações para tratá-las; **(v)** realizar o monitoramento das ações dos incidentes de segurança da informação.

- **Encarregado de Dados: (i)** manter o registro de incidentes e fragilidades de segurança da informação para apresentação periódica ao Comitê Interno de Privacidade de Dados; **(ii)** reportar quando necessário ao Comitê Interno de Privacidade de Dados incidente de segurança da informação, para análise e tomada de decisão.

- **Gestores das áreas/unidades**: **(i)** classificar todas as informações pertinentes à sua área/unidades; **(ii)** 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.

13. DO PROCESSOS DE GOVERNANÇA EM PRIVACIDADE IMPLEMENTADOS

Considerando os pontos trazidos nos itens acima, foram implementados os seguintes processos de governança em privacidade da ETIPI:

- **Minutas** de nomeação do Encarregado de Dados (DPO) e Comitê de Proteção de Dados Pessoais.

- **Política de Privacidade:** documento que determina os critérios e procedimentos para o tratamento de dados pessoais, detalhando: as finalidades para as quais os dados são coletados e tratados; os direitos dos titulares; as medidas de segurança aplicáveis; os procedimentos para a exclusão e anonimização de dados.

- **Política de Segurança da Informação:** define medidas técnicas e organizacionais para proteger as informações, incluindo: **controle de acesso:** Somente pessoas autorizadas podem acessar os dados; **criptografia:** Utilização de criptografia para proteger dados sensíveis; **monitoramento contínuo:** Ferramentas para identificar e mitigar ameaças em tempo real; **gerenciamento de incidentes:** Procedimentos claros para lidar com violações de segurança, desde a detecção até a notificação à ANPD e aos titulares de dados.

- **Política de Retenção de Dados:** estabelece prazos claros para a retenção de dados, garantindo que os dados pessoais sejam armazenados apenas pelo tempo necessário para o cumprimento de suas finalidades e que sejam descartados de forma segura após esse período.

- **Elaboração do Inventário dos dados pessoais**, com os riscos e plano de ação para mitigá-los.

- **Elaboração do Relatório de Impacto à Proteção dos Dados Pessoais**.

- **Portal do Titular,** para que o titular dos dados pessoais possa exercer, de forma gratuita e facilitada, os seus direitos.

- **Manual para atendimento dos direitos dos titulares de dados**, com o fluxo da gestão das solicitações dos titulares, com modelos de respostas, considerando todos os direitos dos titulares de dados, elencados no artigo 18 da LGPD.

- **Minutas de cláusulas-padrão para contratos** (seja com prestadores de serviços, fornecedores ou terceiros).

- **Manual sobre o uso do consentimento e Termo de Consentimento**: para ser usado nos casos que necessitem o consentimento, garantindo que os consentimentos para o tratamento de dados que exigem esta base legal sejam obtidos de maneira clara e informada, conforme exigido pela LGPD, bem como seja assegurada a gestão adequada desses consentimentos.

- **Gestão de Terceiros:** processo de avaliação de fornecedores e terceiros que tratem dados pessoais em seu nome, garantindo que todos estejam em conformidade com a legislação

de proteção de dados. As etapas incluem: **(i) verificação prévia:** antes da contratação, será feita uma avaliação de conformidade dos fornecedores, verificando suas práticas de privacidade e segurança da informação; **(ii) controles rigorosos:** Durante a relação contratual, serão implementados controles periódicos para monitorar e garantir que os fornecedores continuem em conformidade; **(iii) responsabilidade contratual:** Todos os contratos com terceiros devem incluir cláusulas de responsabilidade sobre a proteção de dados, garantindo que os fornecedores adotem as mesmas normas e boas práticas da organização; **(iv) monitoramento contínuo:** auditorias periódicas dos processos e sistemas dos fornecedores para assegurar a conformidade contínua.

- **Gestão de Riscos e Incidentes:** O gerenciamento de riscos envolve a identificação, análise e avaliação contínua de riscos associados ao tratamento de dados pessoais. As avaliações devem ser conduzidas periodicamente para garantir que medidas preventivas e corretivas sejam implementadas. Para melhor direcionamento, vide manual **sobre a comunicação dos incidentes de segurança com dados pessoais**, nos termos da LGPD e da Resolução CD/ANPD nº 15/2024.

- **Treinamento e Conscientização:** Conforme o **Plano Anual de Treinamento**, como garantia à cultura de proteção de dados pessoais e compliance da organização.

- **Campanhas de Conscientização:** visa a realização de campanhas internas de conscientização para reforçar os conceitos de segurança da informação e proteção de dados, com materiais educativos e workshops regulares.

- **Monitoramento e Atualização das Políticas e normativas:** as normativas e demais processos que envolvem o programa global de conformidade, inclusive o presente documento, deverão ser revisados periodicamente, para garantir a conformidade contínua com a LGPD e outros regulamentos aplicáveis.

Aqui deverá ser observado: a revisão de políticas e procedimentos, a revisão dos controles técnicos e organizacionais implementados para garantir a segurança dos dados pessoais; e os relatórios de conformidade, com recomendações de melhoria, quando aplicável, a serem apresentados à alta gestão; e revisão periódica e atualização de políticas e normas, com o objetivo de mantê-las atualizadas em conformidade com as melhores práticas de mercado e mudanças na legislação.

Ademais, as revisões devem ocorrer a cada dois anos ou sempre que houver uma alteração regulatória significativa e observar os seguintes critérios:

- **Processo de revisão:** As políticas e normas serão submetidas a uma análise criteriosa por parte do Comitê de Privacidade de Dados, com participação do Encarregado de dados (DPO) e das áreas envolvidas no tratamento de dados pessoais; e
- **Atualizações e publicização:** As atualizações serão comunicadas de forma transparente ao público interno e externo, garantindo que todos os envolvidos estejam cientes das novas diretrizes. Internamente, serão realizadas campanhas de divulgação para reforçar a adoção das novas práticas, enquanto externamente, as políticas poderão ser disponibilizadas em canais oficiais da organização, como o site institucional.

14. DAS VERSÕES E ATUALIZAÇÕES

Esta Política deverá ser revisada a cada dois anos ou sempre que houver alterações significativas na legislação aplicável, em normativos da ANPD, mudanças estruturais na organização ou identificação de riscos relevantes no tratamento de dados pessoais.