

**COMISSÃO NACIONAL DE ENERGIA NUCLEAR****PORTARIA PR/CNEN Nº 35/2021**

Aprova o Programa de Governança em Privacidade da Comissão Nacional de Energia Nuclear (PGP/CNEN), em conformidade com a Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

**O PRESIDENTE DA COMISSÃO NACIONAL DE ENERGIA NUCLEAR (CNEN)**, no uso das atribuições que lhe confere o artigo 15, incisos I e V, do Anexo I, ao Decreto nº 8.886, publicado no Diário Oficial da União de 25 de outubro de 2016,

**RESOLVE:**

Art. 1º Aprovar, na forma do Anexo a esta Portaria, o Programa de Governança em Privacidade da Comissão Nacional de Energia Nuclear (PGP/CNEN), em conformidade com a Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) .

Art. 2º Estabelecer que o Comitê Gestor de Proteção de Dados Pessoais da CNEN (CPDP/CNEN), instituído pela Portaria PR/CNEN nº 10, de 11 de fevereiro de 2021, promova as ações necessárias para implementação do PGP/CNEN.

Art. 3º Esta Portaria entre em vigor na data da sua publicação.

**Paulo Roberto Pertusi**

Presidente

Comissão Nacional de Energia Nuclear



Documento assinado eletronicamente por **Paulo Roberto Pertusi, Presidente**, em 17/06/2021, às 22:25, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#) e no §1º do art. 7º da Portaria PR/CNEN nº 80, de 28 de dezembro de 2018.



A autenticidade deste documento pode ser conferida no site [http://sei.cnem.gov.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](http://sei.cnem.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **0942824** e o código CRC **BAD24163**.

**ANEXO I****PROGRAMA DE GOVERNANÇA EM PRIVACIDADE DA CNEN (PGP/CNEN)**



# **Programa de Governança em Privacidade da CNEN (PGP/CNEN)**

Edição 1  
Junho/2021

## **Apresentação**

O Programa de Governança em Privacidade da Comissão Nacional de Energia Nuclear (PGP/CNEN) é o documento de orientação para adequação de estrutura e procedimentos da CNEN às exigências da Lei Geral de Proteção de Dados Pessoais (LGPD, Lei 13.709/2018). Esta nova legislação, pela ampla abrangência do escopo regulatório, impacta de forma considerável rotinas e estruturas, tanto na esfera pública como na área privada, exigindo das instituições um elevado nível de planejamento para sua implantação e adaptação da cultura organizacional.

Para acompanhar e regular o seu cumprimento, o Governo Federal criou a Autoridade Nacional de Proteção de Dados (ANPD). Além disso, órgãos de fiscalização e controle do setor público (Tribunal de Contas da União - TCU e Controladoria-Geral da União - CGU) têm somado esforços para monitorar e cobrar a implementação da LGPD. Em outra linha de ação voltada à promoção da adequação à essa Lei, também vêm sendo publicados guias sobre o tema e seus diferentes desdobramentos. As orientações contidas neste PGP/CNEN estão embasadas justamente nestas instruções.

A Portaria PR/CNEN 10/2021 instituiu o Comitê Gestor de Dados Pessoais da CNEN, instância a qual cabe analisar a legislação, a situação da Autarquia e propor ações voltadas à sua adequação legal. Este documento é, essencialmente, parte desta tarefa.

Também foram definidos os servidores aos quais foi delegada a função da figura legal do “encarregado”, prevista no art. 5º da LGPD. A eles cabe receber e dar retorno às demandas dos cidadãos (titulares dos dados pessoais), zelar pelo cumprimento da legislação na instituição e observar orientações e quaisquer demandas da ANPD. A Portaria PR/CNEN 14/2021 designou os encarregados da sede da CNEN (incluindo escritórios, distritos e CRCN-CO), do IPEN, IEN, IRD, CRCN-NE, CDTN e Lapoc.

Já foram iniciadas ações preliminares para elaboração de um diagnóstico dos dados pessoais armazenados e operados pela CNEN. O Comitê tem buscado subsídios com vistas ao dimensionamento do volume de informações abrangidas pela Lei e identificação das contundentes intervenções que precisarão ser feitas na estrutura e nos procedimentos da instituição.

Este documento, o PGP/CNEN, apresenta o rumo a ser seguido para a proteção de dados pessoais na CNEN, viabilizando o exercício dos direitos dos cidadãos, titulares destes dados.

## Sumário

- 1 Definições
- 2 Referências
- 3 Objetivo
- 4 Escopo
- 5 Disposições Gerais
- 6 Metodologia de implementação do PGP/CNEN
- 7 Cronograma de implementação do PGP/CNEN
- 8 Atribuições e Responsabilidades
- 9 Canais de Comunicação e Publicidade
- 10 Gestão de Riscos
- 11 Aprovação e Controle

## 1. DEFINIÇÕES

- 1.1. Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública federal integrante da Presidência da República que possui autonomia técnica e decisória, responsável por zelar pela proteção dos dados pessoais, e por orientar, regulamentar e fiscalizar o cumprimento da legislação.
- 1.2. Comitê de Proteção de Dados Pessoais: grupo responsável pela avaliação dos mecanismos de tratamento e proteção de dados pessoais existentes e proposição de ações voltadas ao seu aperfeiçoamento contínuo, salvaguardas e prevenção de riscos.
- 1.3. Dado pessoal: informação relacionada à pessoa natural identificada ou identificável.
- 1.4. Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou 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.
- 1.5. Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
- 1.6. Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais;
- 1.7. Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
- 1.8. Encarregado: 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).
- 1.9. Tratamento de 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.
- 1.10. Programa de Governança em Privacidade: programa que identifica e consolida os requisitos de privacidade com o intuito de ditar e influenciar como os dados pessoais são manuseados no seu ciclo de vida como um todo.

## 2. REFERÊNCIAS

- 2.1. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados pessoais (LGPD). Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).
- 2.2. Guia de Boas Práticas LGPD – Lei Geral de Proteção de Dados, da Secretaria de Governo Digital (SGD). Versão 2, agosto de 2020.
- 2.3. Guia de Elaboração de Programa de Governança em Privacidade, da Secretaria de Governo Digital (SGD). Versão 1.0, outubro de 2020.
- 2.4. Guia de Elaboração de Inventário de Dados Pessoais, da Secretaria de Governo Digital (SGD). Versão 1.0, setembro de 2020.
- 2.5. Instrução Normativa SGD/ME nº 117, de 19 de novembro de 2020.
- 2.6. Portaria PR/CNEN nº 10/2021, de 10 de fevereiro de 2020.

## 3. OBJETIVO

O Programa de Governança em Privacidade da CNEN (PGP/CNEN) objetiva estabelecer as diretrizes para a governança de privacidade e de proteção dos dados pessoais no âmbito da Comissão Nacional de Energia Nuclear (CNEN), em conformidade com o disposto na Lei Geral de Proteção de Dados Pessoais - LGPD (Lei nº 13.709, de 14 de agosto de 2018) e em atendimento à Portaria PR/CNEN nº 10/2021, de 10 de fevereiro de 2021.

## 4. ESCOPO

O Programa de Governança em Privacidade da CNEN (PGP/CNEN) se aplica:

- I - Ao Controlador, Comissão Nacional de Energia Nuclear (CNEN), e todas suas Unidades;
- II - Aos Encarregados de Dados Pessoais (DPO);
- III - Ao Comitê de Proteção de Dados Pessoais (CPDP);
- IV - Aos Operadores que realizam o tratamento de dados pessoais em nome da CNEN; e
- V - Aos Titulares dos dados pessoais que são objeto de tratamento pela CNEN.

## 5. DISPOSIÇÕES GERAIS

5.1. A governança de privacidade e dados da CNEN deve ser pautada na relação de confiança com os titulares de dados pessoais, por meio de atuação transparente, com monitoramento contínuo e avaliações periódicas integradas à estrutura geral de governança da própria CNEN.

5.2. As adequações dos processos para o tratamento de dados pessoais na CNEN devem ter uma abordagem sistemática que se apoie em padrões e adote condutas de privacidade, de forma proativa e consistente, envolvendo aplicações de tecnologias da informação, práticas organizacionais, prestação de serviços e redes de informação e comunicação, dentre outros.

5.3. O tratamento dos dados pessoais na CNEN deve observar a boa-fé e os seguintes princípios:

- I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- III - Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
- IV - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
- V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
- VI - 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;
- VII - 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;
- VIII - Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
- X - Responsabilização e prestação de contas: demonstração, pelo agente, 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.

5.4. O tratamento dos dados pessoais deve ser realizado mediante enquadramento em uma das bases legais previstas no art. 7º da LGPD. No caso de dados pessoais sensíveis, devem ser consideradas as bases legais previstas no art. 11 da LGPD.

5.5. O tratamento de dados pessoais deve observar a boa-fé e o princípio da necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. A privacidade, por padrão, é obtida por meio da adoção das seguintes práticas:

- I - Especificação da finalidade: os objetivos para os quais os dados pessoais são coletados, usados, retidos e divulgados devem ser comunicados ao titular dos dados antes ou no momento em que as informações são coletadas. As finalidades especificadas devem ser claras, limitadas e relevantes em relação ao que se pretende ao tratar os dados pessoais.
- II - Limitação da coleta: a coleta de dados pessoais deve ser legal e limitada ao necessário para os fins especificados.
- III - Minimização dos dados: a coleta dos dados pessoais que possa identificar individualmente o titular de dados deve obter o mínimo necessário de informações pessoais. A concepção de programas, tecnologias e sistemas de informação e comunicação deve começar com interações e transações não identificáveis, como padrão. Qualquer vinculação de dados pessoais deve ser minimizada. A possibilidade de informações serem usadas para identificar o titular de dados deve ser minimizada.
- IV - Limitação de uso, retenção e divulgação: o uso, retenção e divulgação de dados pessoais devem limitar-se às finalidades relevantes identificadas para o titular de dados, para as quais ele consentiu ou é exigido ou permitido por lei. Os dados pessoais serão retidos apenas pelo tempo necessário para cumprir as finalidades declaradas e depois eliminados com segurança. Quando a necessidade ou uso de dados pessoais não forem claros, deve haver uma presunção de privacidade e o princípio da precaução deve ser aplicado. Dessa forma, as configurações padrão devem ser as de maior proteção à privacidade.

5.6. Em caso de realização de tratamento baseado no consentimento do titular, devem ser observadas as condições para obtenção, previstas no art. 8º da LGPD: deve ser expresso, claro e destacado de outras cláusulas envolvidas na atividade/serviço, livre de vícios e possuir finalidades determinadas.

5.7. Os incidentes relacionados à violação de privacidade ou que gerem danos aos titulares de dados pessoais devem ser encaminhados para os Encarregados de Dados Pessoais (DPO).

## 6. METODOLOGIA DE IMPLEMENTAÇÃO DO PGP/CNEN

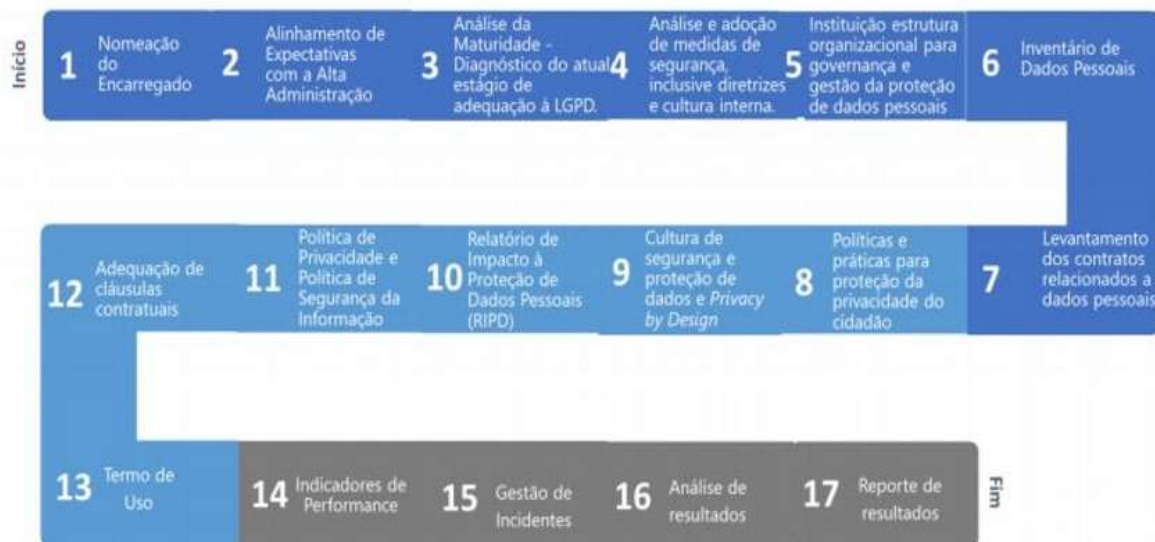
6.1. O Guia de Elaboração de Programa de Governança em Privacidade da Secretaria de Governo Digital (SGD) estabelece as características mínimas de PGP, conforme a seguir:

- I - Necessidade de comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
- II - Deve ser aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
- III - Deve ser adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
- IV - Deve estabelecer políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;



- V - Deve estabelecer relação de confiança com o titular de dados, por meio de atuação transparente e que assegure mecanismos de participação do titular;
- VI - Deve estar integrado à estrutura geral de governança da instituição, além de estabelecer e aplicar mecanismos de supervisão internos e externos;
- VII - Deve possuir planos de resposta a incidentes e remediação; e
- VIII - Deve ser constantemente atualizado com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

6.2. O PGP/CNEN seguirá as etapas previstas no Guia de Elaboração de Programa de Governança em Privacidade da Secretaria de Governo Digital (SGD), conforme a seguir:



Fonte: Guia de Elaboração de Programa de Governança em Privacidade da SGD.

### 6.3. Etapa 1- Iniciação e Planejamento:

A etapa de Iniciação e Planejamento objetiva compreender quais são as primeiras informações e os dados importantes que devem ser conhecidos pela CNEN. É composta pelas seguintes subetapas:



Fonte: Guia de Elaboração de Programa de Governança em Privacidade da SGD.

#### 6.3.1. Nomeação do Encarregado

- I - Nomeação do encarregado: os encarregados foram nomeados pela Portaria PR/CNEN nº 14/2021, de 10 de fevereiro de 2021; e
- II - Criação de uma estrutura organizacional para identificar os dados pessoais em toda a entidade ou órgão, além de supervisionar as três etapas de ação para criar e manter o PGP: o Comitê de Proteção de Dados Pessoais foi constituído pela Portaria PR/CNEN nº 10/2021, de 10 de fevereiro de 2020.

#### 6.3.2. Alinhamento de Expectativas com a Alta Administração

Devem ser implementadas ações que promovam o alinhamento das expectativas com a alta administração da CNEN, priorizando as ações mais urgentes com vistas ao estabelecimento da cultura de proteção de dados na instituição.

#### 6.3.3. Análise da Maturidade - Diagnóstico de Adequação

6.3.3.1. Deve ser realizado periodicamente o diagnóstico disponível no portal gov.br, com o propósito de auxiliar constantes medições do índice de maturidade da CNEN em relação à LGPD. Além de retratar o nível de adequação à LGPD, o índice de maturidade é também utilizado como um índice de performance, que abrange as dimensões de Governança, Conformidade Legal e respeito aos princípios, transparência e direitos do titular, rastreabilidade, adequação de contratos e de relações com parceiros, segurança da informação e violação de dados.

6.3.3.2. A periodicidade de realização do diagnóstico e índice de adequação da CNEN à LGPD é definida no item 7 - Cronograma de implementação do PGP/CNEN.

6.3.4. Análise e adoção de medidas de segurança, inclusive diretrizes e cultura interna.  
Medidas de segurança devem ser analisadas e adotadas com vistas a revisar e propor o aprimoramento das diretrizes e cultura internas da CNEN.

6.3.5. Instituição de estrutura organizacional para Governança e Gestão da Proteção de Dados Pessoais (PDP)

A Portaria PR/CNEN nº 10/2021, de 10 de fevereiro de 2021, instituiu o Comitê de Proteção de Dados Pessoais da CNEN (CPDP), cujo objetivo inicial foi a elaboração deste PGP. A fim de dar continuidade à implementação do Programa e ao seu monitoramento, as finalidades deste Comitê deverão ser ampliadas, por meio de nova portaria, a fim de torná-lo a estrutura organizacional para governança e gestão da proteção de dados pessoais na CNEN.

6.3.6. Inventário de Dados Pessoais

Deve ser elaborado o Inventário de Dados Pessoais da CNEN com vistas a documentar o tratamento de dados pessoais a ser realizado pela instituição, em alinhamento ao previsto pelo art. 37 da LGPD. O inventário consiste em uma forma de fazer um balanço do que a CNEN faz com os dados pessoais, identificando quais dados pessoais são tratados, onde estão e que operações são realizadas com eles. Referência: Guia de Elaboração de Inventário de Dados Pessoais da Secretaria de Governo Digital (SGD). Algumas perguntas que o inventário de dados deve responder são:

- I - Que categorias de dados pessoais são tratadas?
- II - Qual a finalidade do tratamento?
- III - Qual o contexto do tratamento?
- IV - Qual a origem e destino dos dados pessoais?
- V - Qual o volume de dados pessoais armazenados?
- VI - Por quanto tempo os dados pessoais são armazenados?
- VII - Qual o formato dos dados? Estão armazenados de forma estruturada ou não estruturada?
- VIII - Com quem os dados pessoais são compartilhados (interna e externamente)?

6.3.7. Levantamentos dos contratos relacionados a dados pessoais (DP)

Deve ser feito um levantamento dos serviços que tratam dados pessoais no Inventário de Dados com vistas a viabilizar a realização de uma correlação com os contratos que os suportam. Esse mapeamento dos contratos que coletam, transferem e processam dados pessoais visa contribuir para possíveis e necessárias adequações contratuais, tanto nos contratos existentes, quanto nos futuros. Permite também identificar quais lacunas existem para a correta adequação às legislações aplicáveis. Algumas perguntas que o Levantamentos dos Contratos relacionados a DP deve responder são:

- I - Qual a base legal para o tratamento dos dados pessoais (art. 7º da LGPD)?
- II - Existem dados pessoais sensíveis sendo tratados (art. 11º)? Se sim, quais as bases legais e quais as medidas de segurança para sua proteção adicional?
- III - Existem dados pessoais de crianças e adolescentes sendo tratados (art. 14º)?
- IV - Há necessidade de consentimento parental? Quais as medidas para confirmar a obtenção desse consentimento?
- V - Quais os procedimentos para eliminação de dados pessoais? Quais as exceções legais aplicáveis para armazenamento de dados além do período pré-estabelecido (art. 16)?
- VI - Quais os procedimentos que permitem aos titulares de dados serem informados e exercerem seus direitos (art. 18)?
- VII - As regras para tratamento de dados pessoais pelo poder público são cumpridas (arts. 23 a 27)?
- VIII - Há operações de transferência internacional de dados pessoais? Se sim, para onde são enviados, quais as entidades envolvidas, qual o procedimento? Qual a base legal para a transferência internacional (art. 33)?
- IX - Existe registro das operações de tratamento de dados pessoais? Como esse registro é atualizado (art. 37)?
- X - Foi realizada uma análise de riscos preliminar das operações de tratamento? Há necessidade de elaboração de um Relatório de Impacto de Proteção de Dados (art. 38)? Este relatório foi elaborado?
- XI - Existe encarregado de proteção de dados pessoais? Quais suas competências (art. 41)?
- XII - Quais medidas de segurança, técnicas e administrativas são adotadas para proteger os dados pessoais de acessos não autorizados e outras situações acidentais ou ilícitas - destruição, perda, alteração, comunicação, tratamento inadequado ou ilícito (art. 46)?
- XIII - Quais os procedimentos para responder a incidentes de segurança/vazamento de dados pessoais (art. 48)?

6.4. Etapa 2 - Construção e Execução:

A etapa de Construção e Execução objetiva desenvolver, implementar e promover procedimentos, políticas e ações com vistas a proteger os direitos do cidadão (titular) em relação à privacidade dos dados pessoais. É composta pelas seguintes subetapas:



Fonte: Guia de Elaboração de Programa de Governança em Privacidade da SGD.

#### 6.4.1. Políticas e Práticas para Proteção da Privacidade do Cidadão

Devem ser definidas políticas e práticas para proteger a privacidade do cidadão (titular), garantindo que todos os usos dos dados pessoais sejam conhecidos e adequados de acordo com as leis, bem como sua proteção contra mau uso ou revelação inadvertida ou deliberada. A CNEN deve: especificar papéis dos servidores envolvidos na coleta, retenção, processamento, compartilhamento e eliminação de dados pessoais, assim como promover a capacitação dos servidores e colaboradores em relação a políticas e práticas de proteção de privacidade e divulgar para os cidadãos os seus direitos quanto à privacidade da informação.

#### 6.4.2. Cultura de Segurança de Proteção de Dados e Privacy by Design

Devem ser implementadas ações para a promoção de uma cultura de segurança e proteção de dados pessoais com vistas a comunicar os objetivos, metas, procedimentos e indicadores utilizados, além de divulgar o papel da CNEN, enquanto controladora, como custodiante dos dados e sua responsabilidade ao tratar os dados pessoais dos cidadãos (titulares). As informações do PGP/CNEN devem ser disponibilizadas de forma clara e eficiente, além de estarem facilmente acessíveis. Capacitação e treinamento devem ser planejados e oferecidos desde a Etapa 1 - Iniciação e Planejamento, para que uma cultura de Privacidade desde a Concepção ("privacy by design") seja instituída.

#### 6.4.3. Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

Deve ser elaborado o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), instrumento importante de verificação e demonstração da conformidade do tratamento de dados pessoais realizado pela instituição que servirá tanto para a análise quanto para a documentação do tratamento dos dados pessoais. O RIPD visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

#### 6.4.4. Política de Privacidade e Segurança da Informação

Deve ser elaborada a Política de Privacidade e Segurança da Informação da CNEN, documento informativo pelo qual a CNEN, enquanto controlador e prestador de serviço informará ao usuário (titular) como os dados pessoais serão tratados, armazenados e transmitidos para atender às necessidades organizacionais e às legislações aplicáveis, definindo todos os aspectos relativos à proteção de dados. Seus principais componentes são:

- I - Objetivo: porque a política existe e metas a serem alcançadas;
- II - Escopo: que recursos (pessoas, processos e tecnologias) a política protege;
- III - Responsabilidades: quais papéis são responsáveis por quais atividades relacionadas à proteção de dados, incluindo líderes, gerentes, demais funcionários e terceiros; e
- IV - Conformidade: estrutura para garantir a adequação às normas aplicáveis, incluindo políticas e procedimentos complementares (ex. política de controle de acesso) e regime de sanções disciplinares por desrespeito à política de privacidade.

#### 6.4.5. Adequação das Cláusulas Contratuais

Deve ser feita uma revisão dos documentos vigentes e dos dados já coletados, com vistas a adequar os contratos, convênios e outros instrumentos que impliquem no tratamento de dados pessoais, mapeados pelo Inventário realizado na etapa de Iniciação e Planejamento. Como um dos princípios listados é a transparência, torna-se essencial que o contrato apresente informações claras e objetivas, abordando, se pertinente:

- I - Delimitações claras e objetivas das responsabilidades do controlador e operador;
- II - A forma que é realizada a coleta e o tratamento de dados;
- III - A existência da possibilidade de o titular acessar os seus dados coletados;
- IV - A forma que é realizada a correção, bloqueio ou eliminação de dados mediante solicitação do titular;
- V - A existência da possibilidade de revogação do consentimento dado pelo titular;
- VI - O detalhamento de quem tem acesso aos dados, o responsável por seu uso e tratamento, a forma de armazenamento e as particularidades de possíveis auditorias; e
- VII - As medidas de proteção e segurança dos dados coletados e armazenados pela contratada.

#### 6.4.6. Termo de Uso

Deve ser elaborado e implementado o Termo de Uso que, assim como a Política de Privacidade, advém da consciência do controlador e operador ser transparente com o titular de dados pessoais e comunicar como as atividades de tratamento desses dados observam os princípios dispostos no art. 6º da LGPD. Em cumprimento aos princípios da publicidade e da transparência, e a fim de assegurar aos cidadãos amplo acesso às informações, os termos devem ser regularmente atualizados a fim de refletir, de modo claro e preciso, as finalidades de coleta, uso, armazenamento, tratamento e proteção dos dados pessoais dos titulares, que comumente serão utilizados pelo órgão e entidade no exercício de suas competências legais ou execução

de políticas públicas, devidamente previstas em lei, regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres. Os tópicos que devem constar no Termo de Uso estão listados no quadro a seguir:

- I - Aceitação dos Termos e Políticas;
- II - Definições;
- III - Arcabouço Legal;
- IV - Descrição do serviço;
- V - Direitos do usuário;
- VI - Responsabilidades do usuário e da Administração Pública;
- VII - Mudanças no Termo de Uso;
- VIII - Informações para contato; e
- IX - Foro.

#### 6.5. Etapa 3 – Monitoramento:

Deve ser realizado periodicamente o monitoramento do Programa de Governança em Privacidade por meio da coleta e análise de informações, bem como da elaboração de relatórios e apresentações de resultados. A Figura a seguir apresenta os marcos da Etapa de Monitoramento:



Fonte: Guia de Elaboração de Programa de Governança em Privacidade da SGD.

##### 6.5.1. Indicadores de Performance

Devem ser estabelecidos e implementados os Indicadores de Performance ("Key Performance Indicator" - KPI), que incluem a análise regular dos principais indicadores de desempenho com vistas a identificar lacunas no Programa de Governança em Privacidade da CNEN.

##### 6.5.2. Gestão de Incidentes

6.5.2.1. Deve ser elaborado e implementado um Plano de Gestão de Incidentes que registre os incidentes de segurança da informação e de privacidade ocorridos e que armazene informações como: a descrição dos incidentes ou eventos; as informações e sistemas envolvidos; as medidas técnicas e de segurança utilizadas para a proteção das informações; os riscos relacionados ao incidente e as medidas tomadas para mitigá-los a fim de evitar reincidências.

6.5.2.2. É válido também implementar e manter controles e procedimentos específicos para detecção, tratamento, coleta/preservação de evidências e resposta a incidentes de segurança da informação e privacidade. É recomendado que a Gestão de Incidentes possua um Plano de Comunicação orientando a forma que os incidentes de segurança, que acarretem risco ou dano, sejam informados aos órgãos fiscalizatórios e à imprensa.

##### 6.5.3. Análise e Reporte de Resultados

Os resultados devem ser analisados e reportados para a alta administração da CNEN. É uma etapa de monitoramento para demonstrar o valor do PGP/CNEN, a evolução das ações e resultados obtidos, bem como o papel da privacidade para o cidadão, com vistas a reforçar e fortalecer a cultura de privacidade dos dados.

## 7. CRONOGRAMA DE IMPLEMENTAÇÃO DO PGP/CNEN

O cronograma da implementação das etapas mencionadas na metodologia de implementação (item 6) será definido pelo Comitê de Proteção de Dados Pessoais, considerando a aprovação deste Programa, bem como a definição se a execução das ações deste Programa será integralmente executada pela CNEN ou se haverá contratação de serviços externos.

## 8. ATRIBUIÇÕES E RESPONSABILIDADES

8.1. Encarregados: pessoas indicadas para atuarem como canal de comunicação entre a CNEN, seus operadores, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), designados por portaria da Presidência, tendo sido a primeira a Portaria PR/CNEN nº 14 de 11 de fevereiro de 2021, que designou um encarregado para cada uma das seguintes unidades:

- I - Sede, Escritórios, Distritos e CRCN-CO;
- II - Centro de Desenvolvimento da Tecnologia Nuclear (CDTN/CNEN);
- III - Centro Regional de Ciências Nucleares do Nordeste (CRCN-NE/CNEN);
- IV - Instituto de Engenharia Nuclear (IEN/CNEN);
- V - Instituto de Pesquisas Energéticas e Nucleares (IPEN/CNEN);
- VI - Instituto de Radioproteção e Dosimetria (IRD/CNEN)
- VII - Laboratório de Poços de Caldas (LAPOC/CNEN)

##### 8.1.1. São atribuições dos Encarregados pelo Tratamento de Dados Pessoais:

- I - Aceitar reclamações e comunicações dos titulares (pessoas naturais a quem se referem os dados pessoais que são objeto de tratamento), prestar esclarecimentos e adotar providências;
- II - Receber comunicações da autoridade nacional e adotar providências;
- III - Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- IV - Apoiar a definição das diretrizes de construção do inventário de dados pessoais relativas ao registro das operações de tratamento de dados pessoais determinado pelo art. 37 da LGPD;
- V - Conduzir ou aconselhar a elaboração do relatório de impacto à proteção de dados pessoais, de acordo com casos previstos na LGPD em que tal documento é necessário;
- VI - Conduzir ou aconselhar a implementação de regras de boas práticas e de governança especificadas pelo art. 50 da LGPD; e
- VII - Executar as demais atribuições determinadas pela CNEN ou estabelecidas em normas complementares.

8.2. Comitê Gestor de Proteção de Dados Pessoais: responsável pela elaboração do PGP/CNEN, pela avaliação dos mecanismos de tratamento e proteção de dados e pela proposição de ações voltadas ao seu aperfeiçoamento, com vistas ao cumprimento das disposições da Lei nº 13.709, de 14 de agosto de 2018 e na Instrução Normativa SGD/ME nº 117, de 19 de novembro de 2020.

8.2.1. O Comitê Gestor de Proteção de Dados Pessoais da CNEN (CPDP/CNEN) é composto por representantes de todas as unidades da CNEN, definido por portaria específica, tendo sido a primeira a Portaria PR/CNEN nº 10 de 11 de fevereiro de 2021. O Comitê tem representantes da Presidência, de todas as Diretorias e das unidades que tenham encarregados designados.

8.2.2. Atribuições do CPDP/CNEN:

- I - Submeter à Presidência da CNEN minuta de Portaria para implementação do Comitê Permanente em prosseguimento às atividades determinadas pela Portaria PR/CNEN nº 10/2021, de 10 de fevereiro de 2021, em vigor, que instituiu o CPDP.
- II - Avaliar o Programa de Governança em Privacidade da CNEN anualmente, revisando-o se necessário.
- III - Elaborar e implementar, em conjunto com os Encarregados (DPO), as diretrizes para a governança de privacidade e de proteção dos dados pessoais no âmbito da CNEN; e
- IV - Prestar suporte aos Encarregados pelo Tratamento dos Dados Pessoais (DPO).

8.2.3. O CPDP/CNEN poderá convidar representantes de outros órgãos da administração pública federal, estadual ou municipal, de entidades privadas, de organizações da sociedade civil e de organismos internacionais, para participar de reuniões, sem direito a voto, com o propósito de contribuir para a execução dos trabalhos.

8.3. Controlador: Comissão Nacional de Energia Nuclear (CNEN), a quem compete as decisões referentes ao tratamento de dados pessoais.

8.3.1. O Controlador deve assegurar ao Encarregado pelo Tratamento dos Dados Pessoais:

- I - Acesso direto à alta administração;
- II - Pronto apoio das unidades administrativas no atendimento das solicitações de informações; e
- III - Contínuo aperfeiçoamento relacionado aos temas de privacidade e proteção de dados pessoais.

8.3.2. O Controlador deve manter registro das operações de tratamento de dados pessoais que realizar, especialmente quando baseado no legítimo interesse.

8.3.3. O Controlador deve comunicar à Autoridade Nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante.

8.4. Operador: pessoa natural e jurídica que realiza o tratamento de dados pessoais em nome da CNEN, a saber:

- I - Servidores;
- II - Colaboradores;
- III - Estagiários;
- IV - Bolsistas;
- V - Empresas contratadas para prestação de serviços;
- VI - Parceiros comerciais e fornecedores, sempre que ocorrer compartilhamento de dados pessoais; e
- VII - Organismos internacionais, sempre que ocorrer compartilhamento de dados pessoais.

8.4.1. O Operador deve:

- I - Manter registro das operações de tratamento de dados pessoais que realizarem;
- II - Realizar o tratamento dos dados pessoais segundo as instruções fornecidas pela CNEN, enquanto controlador; e
- III - Cumprir o disposto no PGP/CNEN utilizando de forma responsável, profissional, ética e legal as informações corporativas que contenham dados pessoais, respeitando os direitos e a privacidade dos titulares dos dados.

8.5. As áreas de Tecnologia da Informação e Comunicações são responsáveis pela gestão dos Recursos de Tecnologia da Informação da CNEN, e:

- I - Cabe à Coordenação Geral de Tecnologia da Informação e Comunicações (CGTI) adequar políticas e diretrizes de Tecnologia da Informação;
- II - Cabe às áreas de Tecnologia da Informação da sede e das unidades adaptarem os sistemas, serviços e a infraestrutura de Tecnologia da Informação; e
- III - Cabe às áreas de Tecnologia da Informação da sede e das unidades prestarem informações e suporte técnico aos Encarregados pelo Tratamento dos Dados Pessoais.

8.6. As Unidades Administrativas e Áreas Interlocutoras, responsáveis pelos processos/atividades que levam ao tratamento dos dados na CNEN, devem prestar informações e suporte ao CPDP/CNEN e aos Encarregados pelo Tratamento dos Dados Pessoais, sempre que solicitado.

8.7. A Coordenação de Comunicação Social (COCOM), responsável pelas ações de comunicação da CNEN, apoiada pelas áreas de Comunicação das unidades, deve:

- I - Prestar suporte e assessoramento às ações de comunicação a serem efetivadas pelos Encarregados pelo Tratamento dos Dados Pessoais; e
- II - Participar da elaboração e gestão do Plano de Comunicação integrante do Plano Gestão de Incidentes, com vistas a orientar a forma que os incidentes de segurança, que acarretem risco ou danos aos titulares, sejam informados aos órgãos fiscalizatórios, às autoridades, à imprensa e ao público em geral.

8.8.

8.9. O Gabinete da Presidência deve prestar apoio administrativo ao CPDP/CNEN.

## 9. CANAIS DE COMUNICAÇÃO E PUBLICIDADE

9.1. A CNEN, atendendo ao disposto no inciso I do art. 23 da LGPD, que impõe às pessoas jurídicas de direito público obrigações de transparência ativa, deve:

- I - Publicar em seus sítios eletrônicos informações sobre os tratamentos de dados de forma clara e atualizada, detalhando a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução desses tratamentos;
- II - Dar publicidade aos tratamentos de dados pessoais sensíveis em que seja dispensado o consentimento do titular, seja para cumprimento de obrigação legal ou regulatória, seja para tratamento compartilhado de dados necessários para a execução de políticas públicas previstas em leis ou regulamentos, conforme prevê o §2º do art. 11 da LGPD; e
- III - publicar a identidade e informações de contato do encarregado, por força do art. 41, §1º da LGPD.

9.2. Devem ser publicadas as seguintes informações sobre os encarregados:

- I - Nome e cargo do encarregado indicado pelo controlador;
- II - Localização;
- III - Horário de atendimento; e
- IV - Telefone e e-mail específico para orientação e esclarecimento de dúvidas.

9.3. A fim de atender à legislação e à Portaria PR/CNEN nº de 10 de fevereiro de 2021, já foram publicados no sítio da CNEN os dados referentes ao item 9.2.

9.4. A plataforma Fala.BR será o canal utilizado pela CNEN para endereçamento de petições e reclamações dos titulares de dados pessoais, previstas nos arts. 18 e 20 da LGPD.

## 10. GESTÃO DE RISCOS

Para que um Programa de Governança em Privacidade seja bem implementado, é essencial mitigar os riscos associados. De acordo com o Plano de implementação a ser definido (item cronograma) e com a Política de Riscos da CNEN, a avaliação e o gerenciamento dos riscos deverão ser feitos, considerando o seu grau de ameaça à implementação do PGP/CNEN.

## 11. APROVAÇÃO E CONTROLE

11.1. O PGP/CNEN é aprovado pelo Presidente da CNEN, ficando o CPDP/CNEN responsável para efetuar o seu controle.

11.2. Quadro de Edição

REVISÃO	PAGINA	DATA	ELABORAÇÃO	OBSERVAÇÃO
00	TODAS	JUNHO/2021	CPDP/CNEN	Primeira versão do documento

11.3. Quadro de Elaboração/Participação:

ELABORAÇÃO / PARTICIPAÇÃO	
PARTICIPANTES	LOTAÇÃO
Luís Antônio Alves Machado	PR/COCOM
Tindyua de Moraes Nogueira	PR/GAB
Cássia Helena Pereira Lima	PR/GAB
Helenice Feijó de Carvalho	PR/GAB
Alberto Barbosa de Almeida Neto	PR/CGPA
Viviane da Silva Simões	PR/CGAI

Leonardo Ferreira Bezerra	DGI/CGRH
José Augusto Rocha	DGI/CGTI
Deborah Aires Nepomuceno de Andrade	DGI/CGAL
Bruno Flávio Machado de Araújo	DPD/CDTN/CNEN
Gilvânia de Brito Ferreira	DPD/CRCN-NE
Marcus Vinicius Alves da Silva	DPD/IEN
Ítalo Henrique Alves	DPD/IPEN
Eduardo Ferraz Martins	DPD/IRD
Ricardo Augusto da Silva Alfenas	DRS/LAPOC

Assinaturas dos servidores que elaboraram e participaram encontram-se na minuta deste Plano, documento Programa de Governança em Privacidade CPDP (0942038)