

LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA
Av. Getúlio Vargas, nº 333, - Bairro Quitandinha,
CEP 25651-075, Petrópolis - RJ - <http://www.lncc.br>

Programa de Governança em Privacidade			
CÓDIGO	VERSÃO	TIPO DE ACESSO	NÍVEL DE ACESSO
80-PGP	1.0	Externo	Público
CONTROLES DA ABNT NBR ISO/IEC 27001:2022		PUBLICADO EM	
A.5.34 – Privacidade e Proteção de Dados Pessoais		23/10/2025	

1. OBJETIVO

Estabelecer o Programa de Governança em Privacidade (PGP) do LNCC, bem como as diretrizes, princípios e responsabilidades necessárias para a sua implementação, manutenção e melhoria contínua, de modo a assegurar o cumprimento da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD), promover a cultura de privacidade e garantir a proteção dos dados pessoais tratados pela Instituição.

2. CAMPO DE APLICAÇÃO

Este Programa aplica-se a todos os processos, áreas, colaboradores, prestadores de serviço, parceiros institucionais, contratos e sistemas de informação que envolvam o tratamento de dados pessoais no âmbito do LNCC, abrangendo tanto os meios físicos quanto digitais.

3. RESPONSABILIDADE

A responsabilidade pela elaboração e revisão deste documento é da coordenação da Comissão de Privacidade e Proteção de Dados Pessoais, sendo verificada pela presidência do Comitê de Privacidade e Segurança, Comunicações e Segurança Física e pelo Coordenador da COTIC. A aprovação, por sua vez, cabe à Diretoria do LNCC.

4. DOCUMENTOS DE REFERÊNCIA

Lei nº 13.709/2018	Lei Geral de Proteção de Dados Pessoais (LGPD)
ABNT NBR ISO/IEC 27001:2022	Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos
ABNT NBR ISO/IEC 27701:2019	Extensão da ISO/IEC 27001 e ISO/IEC 27002 para Gestão da Privacidade da Informação.
Política de Proteção de Dados Pessoais	https://www.gov.br/lncc/pt-br/acesso-a-informacao/atos-normativos/portarias-1/po-534-instui-a-polica-de-protacao-de-dados-pessoais-do-laboratorio-nacional-de-computacao-ciencia-lncc.pdf

5. DOCUMENTOS COMPLEMENTARES

Os documentos a seguir poderão ser utilizados, no todo ou em parte, para viabilizar a aplicação deste procedimento.

02-PSI	Política de Segurança da Informação do LNCC
--------	---

6. SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
DPO	Data Protection Officer (Encarregado pela Proteção de Dados)

LGPD	Lei Geral de Proteção de Dados Pessoais
LNCC	Laboratório Nacional de Computação Científica
PGP	Programa de Governança em Privacidade
PSI	Política de Segurança da Informação

Nota: As siglas das UO do LNCC podem ser acessadas no Regimento Interno do Laboratório Nacional de Computação Científica (<https://www.in.gov.br/en/web/dou/-/portaria-mcti-n-7.061-de-24-de-maio-de-2023-485541159>).

7. TERMOS E DEFINIÇÕES

Para os efeitos deste documento, aplicam-se os seguintes termos e definições, baseados na Lei Geral de Proteção de Dados Pessoais, no [Glossário ANPD](#), e em conceitos de segurança da informação, adaptados para facilitar a compreensão do público externo:

Dado Pessoal	Qualquer informação que identifique ou possa identificar uma pessoa natural. Por exemplo, nome, CPF, endereço, e-mail, telefone.
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, à vida sexual, dado genético ou biométrico.
Titular de dados	Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. No contexto do LNCC, isso pode incluir servidores, pesquisadores, colaboradores, alunos e qualquer indivíduo cujos dados sejam tratados pela Instituição.
Controlador	Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Nas situações em que o LNCC decide sobre o tratamento de dados pessoais, definindo as finalidades e os meios de tratamento, ele atua como Controlador.
Operador	Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador. No contexto do LNCC, os Operadores podem ser instituições, órgãos e empresas parceiras, fornecedores de sistemas ou serviços que tratam dados pessoais em nome da Instituição.
Encarregado (DPO)	Pessoa indicada pelo Controlador para atuar como canal de comunicação entre este, os titulares dos dados e a ANPD. No LNCC, o Encarregado é indicado pela Diretoria através de portaria publicada no Diário Oficial de União e sua identificação e contato são disponibilizados no sítio eletrônico do LNCC (https://www.gov.br/lbcc/pt-br/aceso-a-informacao/privacidade/encarregado).
Tratamento de dados pessoais	Toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, modificação, comunicação, transferência, difusão ou extração.

8. CONTEXTUALIZAÇÃO

A Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), tem o objetivo de regular as atividades de “tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de

liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural” (art. 1º).

A LGPD estabelece, em seu art. 23, que o tratamento de dados no poder público “deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público”, “com informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para execução dessas atividades, em veículos de fácil acesso”.

A governança em privacidade deve incluir as estratégias, habilidades, pessoas, processos e ferramentas que os órgãos e entidades precisam prover para conquistar a confiança dos servidores e dos cidadãos e, ao mesmo tempo, cumprir com exigências apresentadas nos normativos de privacidade. Um Programa de Governança em Privacidade (PGP) captura e consolida os requisitos de privacidade com o intuito de estabelecer e influenciar como os dados pessoais são manuseados no seu ciclo de vida como um todo.

9. ESTRUTURA DO PROGRAMA DE GOVERNANÇA EM PRIVACIDADE PARA O LNCC

A estrutura do Programa de Governança em Privacidade do LNCC será inspirada no ciclo PDCA (*Plan, Do, Check e Act*), desdobrando-se em três fases principais:

- **Fase 1:** Iniciação e Planejamento
- **Fase 2:** Construção e Execução
- **Fase 3:** Monitoramento e Melhoria Contínua



Figura 1 - Fases do Programa de Governança em Privacidade.

Fonte: adaptado de Guia de Elaboração do Programa de Governança em Privacidade (BRASIL, 2024)

A seguir, apresenta-se um diagrama que detalha os passos para execução do PGP, compreendendo as três fases do Programa:



Figura 2- Detalhamento das Fases do PGP.

Fonte: adaptado de Guia de Elaboração do Programa de Governança em Privacidade (BRASIL, 2024)

9.1 Fase 1: Iniciação e Planejamento

Esta fase inicial é crucial para estabelecer as bases do PGP no LNCC, definindo o escopo, os responsáveis e os recursos necessários.

9.1.1 Nomeação do Encarregado pela Proteção de Dados (DPO)

A designação de um Encarregado pela Proteção de Dados é o ponto de partida deste PGP. Conforme o Art. 5º, inciso VIII da LGPD e a Resolução CD/ANPD Nº 18, de 16 de julho de 2024. É preferível que a escolha recaia sobre um servidor ou empregado público com reputação ilibada, e sua nomeação deve ser publicada no Diário Oficial da União, explicitando suas atribuições.

O Encarregado deverá atuar com ética, integridade e autonomia técnica, evitando situações que possam configurar conflito de interesse. Tal conflito pode surgir quando existir o acúmulo de atividades de encarregado com outras que envolvam a tomada de decisões estratégicas sobre o tratamento de dados pessoais pelo LNCC, ressalvadas as operações com dados pessoais inerentes às atribuições do encarregado. A escolha do encarregado deve ser acompanhada da realização da análise de conflito de interesses.

O Encarregado atuará como a ponte entre o LNCC, os titulares de dados e a ANPD, prestando assistência e orientação na elaboração e implementação de políticas e processos internos, no registro de incidentes e operações de tratamento, e na análise de riscos. Para isso, o LNCC deve garantir que o Encarregado possua recursos adequados, autonomia técnica e acesso direto à alta administração e às diversas áreas da instituição. As qualificações profissionais devem abranger conhecimentos da LGPD e do contexto de tratamento de dados no LNCC.

O acesso e gerenciamento do endereço de e-mail lgpd@lncc.br devem ser concedidos ao Encarregado e seu substituto e alterado, sempre que houver mudança de servidores exercendo esse papel.

Situação	Concluído
Observações	PORTARIA LNCC Nº 610, DE 9 DE OUTUBRO DE 2025

9.1.2 Alinhamento de expectativas com a Alta Administração

O sucesso do PGP depende intrinsecamente do comprometimento da alta administração do LNCC. Isso envolve não apenas o apoio formal, mas a incorporação da proteção de dados como um valor institucional. Portanto, é fundamental:

- Elaborar e aprovar políticas institucionais claras de privacidade e proteção de dados que reflitam o compromisso do LNCC com a conformidade à LGPD.
- Assegurar a disponibilidade de recursos humanos (equipe de privacidade), financeiros e tecnológicos (ferramentas de segurança e gestão) para a implementação e manutenção contínua do PGP.
- Instituir Comissão de Privacidade e Proteção de Dados, com representantes de diferentes áreas do LNCC para supervisionar e deliberar sobre as questões do PGP.

Situação	Ação contínua, já iniciada.
Observações	O compromisso da Alta Administração com o PGP pode ser acompanhado através da página de Governança no sítio eletrônico do LNCC.

9.1.3 Avaliação da Maturidade da Adequação

É imperativo que o LNCC realize uma avaliação do seu nível atual de maturidade em relação à proteção de dados pessoais. Isso permite identificar pontos fortes e fracos, direcionando o plano de ação de forma eficaz. Esse diagnóstico será realizado por meio do indicador de privacidade (iPriv), cuja metodologia está descrita no Guia do Framework de Privacidade e Segurança da Informação (PPSI). Esta avaliação inicial servirá como um mapa para as futuras ações de adequação e aprimoramento.

Situação	Realizada e atualizada
Periodicidade	Semestral
Observações	Indicador iPriv do LNCC no último ciclo de avaliação (ciclo 5 do PPSI) = 0,57

9.1.4 Revisão das Medidas de Segurança Existentes

É fundamental que seja realizada uma análise crítica das medidas de segurança da informação já em vigor no LNCC. Isso inclui a revisão e atualização de políticas internas para garantir que estejam alinhadas com os requisitos da LGPD e as melhores práticas. O objetivo dessa revisão é identificar lacunas e implementar controles técnicos e administrativos que garantam a confidencialidade, integridade, disponibilidade e autenticidade dos dados pessoais tratados, protegendo-os contra acessos não autorizados, perdas, alterações ou divulgações indevidas.

Situação	Programada - conclusão até março de 2026
Periodicidade	Anual - realizada no mês de março

9.1.5 Estrutura Organizacional para Governança de Dados

Para sustentar o PGP, o LNCC deve estabelecer uma estrutura organizacional clara. Isso pode envolver a criação de uma Comissão de Privacidade e Proteção de Dados, responsável por supervisionar a implementação do PGP e resolver questões relacionadas à proteção de dados. Além disso, é crucial definir e comunicar os papéis e responsabilidades de cada membro da equipe em relação ao tratamento de dados pessoais.

Situação	Realizada.
Observações	O Presidente do Comitê de Privacidade e Segurança da Informação instituiu a Comissão Permanente de Privacidade e Proteção de Dados Pessoais.

9.1.6 Registro das Operações de Tratamento de Dados Pessoais

O coração da fase de planejamento é o mapeamento detalhado de todos os dados pessoais tratados pelo LNCC e a quais processos estão vinculados. Essa ação é fundamental para o alinhamento com o Art. 37 da LGPD. Para cada processo/operação que trata dados pessoais, deve-se registrar:

- Nome do processo/operação
- Identificação do Controlador
- Identificação do Operador (se aplicável)
- Categoria dos titulares
- Fluxo do tratamento de dados pessoais, informando:
 - a fonte/origem de obtenção dos dados;
 - o local e suporte de armazenamento;
 - compartilhamentos realizados;
 - tempo de retenção;
 - método de eliminação e anonimização;
 - hipótese/base legal para o tratamento;
 - finalidade do tratamento;
 - natureza dos dados;
 - categorias dos dados;
 - informação sobre tratamento de dados de crianças, adolescentes e pessoas em situação de vulnerabilidade;
 - medidas de controle de privacidade/segurança da informação adotadas.

Essas informações deverão ser inseridas em formulário padronizado de inventário de dados estabelecido pelo LNCC.

Esse registro deverá ser atualizado regularmente, com o objetivo de auxiliar no controle e na demonstração da conformidade com os princípios da LGPD.

Situação	Iniciado em agosto/2025 com previsão de conclusão em dezembro/2025
Periodicidade	Anualmente, no mês de novembro, ou sempre que se identificarem novas operações

9.1.7 Levantamento dos Contratos Relacionados a Dados Pessoais

É fundamental que o LNCC identifique todos os contratos, convênios e instrumentos congêneres que envolvam o tratamento de dados pessoais por terceiros. Esse levantamento será importante para a adequação dos instrumentos vigentes e para a elaboração dos futuros.

Situação	Programado - com conclusão prevista para dezembro de 2025
-----------------	---

9.2 Fase 2: Construção e Execução

Nesta fase, as diretrizes e planos estabelecidos na etapa anterior são transformados em ações concretas e políticas operacionais.

9.2.1 Elaboração de Políticas e Procedimentos

O LNCC deve elaborar e implementar políticas claras que orientem todas as operações de tratamento de dados pessoais, estabelecendo:

- **Política de Privacidade/Proteção de Dados Pessoais:** documento acessível e compreensível para os titulares, informando como seus dados são coletados, utilizados, armazenados, protegidos e quais são seus direitos. Esta política deve refletir os princípios do Art. 6º da LGPD, como finalidade, necessidade, transparência, segurança, não discriminação e responsabilização.
- **Procedimentos padronizados:** instruções detalhadas para o ciclo de vida dos dados (coleta, processamento, armazenamento, compartilhamento, eliminação), garantindo que as operações ocorram de forma uniformizada e segura.
- **Canais de Comunicação:** definir como as políticas e procedimentos serão comunicados a todas as partes interessadas internas (servidores, colaboradores) e externas (titulares, parceiros), utilizando os canais apropriados (e-mail, intranet, site, etc.).

Situação	Realizada e atualizada
Observações	As políticas e procedimentos devem ser revisados anualmente

9.2.2 Promoção da Cultura de Privacidade

A proteção de dados não é apenas um conjunto de regras, mas uma cultura organizacional que deve valorizar a privacidade e a proteção de dados. Isso se concretiza através de:

- **Treinamentos e Capacitações:** programa permanente de conscientização para todos os colaboradores, desde a alta gestão até a equipe operacional, abordando a importância da LGPD, os riscos associados ao tratamento de dados e as práticas adequadas.
- **"Privacy by Design" e "Privacy by Default":** princípios fundamentais, que significam a incorporação da privacidade desde a concepção de novos projetos, sistemas e processos, adotando comportamento proativo, não reativo; e ter a privacidade como padrão, garantindo que apenas os dados estritamente necessários sejam processados, limitando a coleta, a extensão do tratamento e o período de armazenamento ao mínimo.

Situação	Programado para o início até dezembro de 2025
Observações	Realizado conforme o Programa Permanente de Treinamento e Comunicação em Privacidade

9.2.3 Elaboração do Relatório de Impacto à Proteção de Dados (RIPD)

No LNCC, este relatório deverá ser elaborado sempre que o tratamento de dados não seja baseado no cumprimento de obrigação legal ou regulatória ou que o tratamento não seja necessário à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, e, adicionalmente, possa:

- Gerar riscos às liberdades civis e aos direitos fundamentais;
- Envolver dados pessoais sensíveis; ou
- Envolver dados pessoais de crianças, adolescentes ou pessoas em situação de vulnerabilidade.

Nos casos em que se exija a elaboração, o RIPD deverá conter, no mínimo:

- A descrição dos tipos de dados coletados;
- A metodologia utilizada para a coleta e garantia de segurança;
- A análise do LNCC em relação às medidas, salvaguardas e mecanismos de mitigação de risco adotados;
- A identificação dos agentes de tratamento e do(s) Encarregado(s);
- A natureza, escopo, contexto e finalidade do tratamento;
- A identificação e avaliação do nível dos riscos (probabilidade e impacto); e
- As medidas para tratar os riscos.

Este relatório deve ser elaborado antes de iniciar qualquer novo tratamento de dados pessoais de alto risco e ser revisado e atualizado periodicamente.

Situação	Realizada
Periodicidade	Revisado anualmente, no mês de dezembro

9.2.4 Implementação de Medidas de Segurança

A segurança dos dados pessoais é um pilar da LGPD. O LNCC deve adotar medidas técnicas e administrativas robustas para proteger os dados pessoais de acessos não autorizados, destruição, perda, alteração ou difusão ilícita, conforme o Art. 46 da LGPD. Estas medidas podem incluir:

- A implementação de políticas de acesso, garantindo que apenas pessoal autorizado possa acessar dados específicos, com base no princípio do menor privilégio;
- A utilização de técnicas de criptografia para proteger dados sensíveis em

trânsito e em repouso;

- O estabelecimento de procedimentos claros para backup regular e recuperação de dados, garantindo a resiliência em caso de incidentes; e
- A adoção de padrões e frameworks de segurança da informação reconhecidos, como ABNT NBR ISO/IEC 27001, 27002, 27005, 27701 e PPSI.

Situação	Atualizada
Periodicidade	Revisadas anualmente
Observações	O LNCC possui a certificação ABNT NBR ISSO/IEC 27001

9.2.5 Revisão e Adequação de Cláusulas Contratuais

Todos os contratos existentes e futuros que envolvam o tratamento de dados pessoais devem ser revisados e adequados à LGPD, a fim de que as cláusulas sejam claras e objetivas, abordando:

- As obrigações e responsabilidades do LNCC e dos terceiros em relação ao tratamento de dados, e qual é o papel de cada um como Agente de Tratamento;
- A finalidade e bases legais para o tratamento realizado a partir do objeto do contrato/convênio;
- As medidas técnicas e organizacionais de segurança e controle, que devem ser adotadas para proteger os dados pessoais; e
- As penalidades, especificando sanções em caso de descumprimento das obrigações contratuais relacionadas à proteção de dados.

Situação	Programada - com conclusão prevista para julho de 2026
-----------------	--

9.2.6 Implementação de Termos de Uso

O LNCC deve elaborar e implementar termo de uso para seus serviços e plataformas. O Termo de Uso descreve as condições e regras do serviço, enquanto a Política de Privacidade detalha como os dados pessoais são tratados. Ambos devem informar claramente aos titulares:

- A finalidade da coleta de dados.
- Os direitos dos titulares (acesso, retificação, eliminação, etc.).
- Os dados de contato do Encarregado para solicitações ou esclarecimentos.

Situação	Programada - com conclusão prevista para julho de 2026
Periodicidade	Revisados anualmente

9.3 Fase 3: Monitoramento e Melhoria Contínua

Esta fase garante que o PGP seja dinâmico, eficaz e constantemente aprimorado, respondendo a novas ameaças e requisitos legais.

9.3.1 Monitoramento de Indicadores de Desempenho (KPIs)

Para monitorar a eficácia do PGP, o LNCC deve acompanhar regularmente os seguintes indicadores de desempenho:

- Índice de maturidade - iPriv;
- Número de incidentes de segurança envolvendo dados pessoais;
- Tempo de resposta a solicitações dos titulares;
- Índice de processos/atividades que tratam dados pessoais inventariados;
- Índice de conscientização (participação e engajamento dos colaboradores em treinamentos e ações de sensibilização sobre privacidade);

Situação	Programado - 1º relatório em março de 2026
Periodicidade	Relatório anual, elaborado nos meses de março

9.3.2 Gestão de Incidentes

Para manter um processo robusto de gestão de incidentes o LNCC deve

implementar procedimentos para:

- Identificar, registrar e analisar rapidamente incidentes de segurança da informação e privacidade;
- Lidar com violações de dados, incluindo a coleta/preservação de evidências e a análise de causa-raiz;
- Informar a ANPD e os titulares de dados afetados, conforme exigido pela LGPD, em prazos adequados;
- Mitigar os impactos dos incidentes e evitar reincidências.

Situação	Ação contínua, já em execução
Observações	O LNCC possui estabelecido um Procedimento de Tratamento de Incidente de Segurança envolvendo Dados Pessoais (66-PTISDP), que deve ser revisado anualmente.

9.3.3 Relatórios e Comunicação

A transparência é um princípio fundamental, por isso, o LNCC deve elaborar relatórios regulares sobre o desempenho do PGP e comunicar os resultados à alta administração e às partes interessadas. Isso não só garante a prestação de contas, mas também reforça a cultura de privacidade e demonstra o valor do programa. Os relatórios devem ser claros e concisos, destacando o progresso, os desafios e as melhorias realizadas.

Situação	Programado - 1º relatório em março de 2026
Periodicidade	Relatório anual, elaborado nos meses de março

10. CONSIDERAÇÕES FINAIS

A implementação deste Programa de Governança em Privacidade para o LNCC é uma jornada contínua que exige comprometimento, colaboração e adaptação. Ao seguir estas diretrizes, o LNCC não apenas estará em conformidade com a LGPD, mas também reforçará sua reputação como uma instituição que preza pela segurança e privacidade das informações, elemento fundamental em um cenário cada vez mais digitalizado e preocupado com a proteção de dados.

11. ANÁLISE CRÍTICA E REVISÃO DO DOCUMENTO

Este "Programa de Governança em Privacidade" será revisado criticamente pelo menos a cada 12 meses ou sempre que houver mudanças significativas na legislação, nos processos internos do LNCC ou na identificação de necessidades de melhoria, visando garantir sua eficácia e atualização contínua.

12. HISTÓRICO DA REVISÃO E QUADRO DE APROVAÇÃO

Versão	Data	Itens Revisados
1.0	23/10/2025	Documento inicial.

Quadro de Aprovação		
	Nome	Atribuição
Elaborado por:	Diógenes Souza Freitas	Coordenador da Comissão de Privacidade e Proteção de Dados Pessoais
	Marcia Aparecida Almeida Pereira	Analista em C&T
Verificado por:	Luís Rodrigo Oliveira Gonçalves	Presidente do Comitê de Privacidade e Segurança da Informação, Comunicações e Segurança Física do LNCC
Aprovado por:	Wagner Vieira Léo	Diretor Substituto do LNCC



Documento assinado eletronicamente por **Luis Rodrigo De Oliveira Gonçalves, Gestor de Segurança da Informação**, em 23/10/2025, às 15:58 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Diógenes Souza Freitas, Analista em Ciência e Tecnologia**, em 23/10/2025, às 16:30 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Wagner Vieira Léo, Diretor do Laboratório Nacional de Computação Científica substituto**, em 23/10/2025, às 16:37 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Márcia Aparecida Almeida Pereira, Analista em Ciência e Tecnologia**, em 23/10/2025, às 17:24 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site <https://sei.mcti.gov.br/verifica.html>, informando o código verificador **13251234** e o código CRC **671C0541**.