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

Política de Mascaramento e Tarjamento de Dados Pessoais			
CÓDIGO	**VERSÃO**	**TIPO DE ACESSO**	**NÍVEL DE ACESSO**
81-PMTDP	1.0	Externo	Público
CONTROLES DA ABNT NBR ISO/IEC 27001:2022			**PUBLICADO EM**
A.8.11 – Mascaramento de Dados			03/02/2026

SUMÁRIO

1. OBJETIVO

Esta política estabelece orientações para a aplicação de mascaramento e tarjamento de dados pessoais em sistemas, bancos de dados, arquivos e documentos físicos e digitais. O objetivo é viabilizar o uso e o compartilhamento seguro de informações — seja para fins de testes, análises, colaboração entre setores ou atendimento a pedidos de acesso à informação (LAI) — protegendo dados sensíveis, pessoais e sigilosos contra visualização não autorizada, em conformidade com a LGPD e a ISO/IEC 27001:2022.

2. CAMPO DE APLICAÇÃO

As diretrizes aplicam-se a todas as unidades organizacionais do LNCC e abrange:

I - Dados Estruturados: bancos de dados de sistemas (CPD, SSD, administrativos) usados em desenvolvimento, testes ou produção.

II - Dados não Estruturados: documentos digitais (PDFs, planilhas, textos), físicos e comunicações que contenham dados sensíveis e precisem ser compartilhados interna ou externamente.

III - Processos de Negócio: atividades que envolvam transferência de arquivos entre setores ou respostas a cidadãos e órgãos de controle.

3. RESPONSABILIDADE

São responsabilidades do:

I - Gestor de Segurança da Informação: supervisionar a aplicação da política e apoiar na definição de ferramentas homologadas para mascaramento seguro.

II - Servidores e colaboradores proprietários ou curadores dos dados: identificar, antes de realizar operações, os documentos ou dados que requerem mascaramento ou tarjamento e realizá-los, quando aplicável.

III - Encarregado pelo Tratamento de Dados Pessoais (DPO): divulgar esta política e orientar os servidores e colaboradores quanto a sua aplicação.

4. DOCUMENTOS DE REFERÊNCIA

Lei nº 13.709/2018	Lei Geral de Proteção de Dados Pessoais (LGPD)
ABNT NBR ISO/IEC 27001:2022	Sistema de Gestão de Segurança da Informação - Requisitos (Controle A.8.11)
Cartilha de Orientações e Boas Práticas de Proteção de Dados Pessoais	Cartilha publicada pelo MCTI que contém orientações sobre mascaramento e tarjamento de dados pessoais (https://www.gov.br/mcti/pt-br/acesso-a-informacao/lei-geral-de-protecao-de-dados-pessoais-lgpd/09-2025_boas-praticas.pdf)

5. DOCUMENTOS COMPLEMENTARES

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

Lei nº 12.527/2011	Lei de Acesso à Informação (LAI)
Decreto nº 7.724/2012	Regulamenta a LAI
31-PTIS	Procedimento para Tratamento de Incidentes de Segurança da Informação
66-PTISDP	Procedimento para Tratamento de Incidentes de Segurança envolvendo Dados Pessoais

6. SIGLAS

DPO: Encarregado pelo Tratamento de Dados Pessoais

LAI: Lei de Acesso à Informação

LGPD: Lei Geral de Proteção de Dados Pessoais;

OCR: Optical Character Recognition (Reconhecimento Óptico de Caracteres)

SGSI: Sistema de Gestão 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 e em conceitos de segurança da informação, adaptados para facilitar a compreensão do público externo:

Mascaramento	Técnica de modificação do dado, que altera o valor original para uma versão fictícia, mas mantém o formato e a integridade referencial para que o dado continue sendo útil em contextos como testes, desenvolvimento ou pesquisas científicas.
Tarjamento	Técnica de mascaramento irreversível aplicada a documentos (físicos ou digitais), onde informações sensíveis são cobertas ou removidas visualmente para permitir a divulgação do restante do documento.

8. DIRETRIZES GERAIS

Todo compartilhamento de informação classificada como "Restrita", "Confidencial" ou que contenha dados pessoais para um destinatário com nível de acesso inferior ou externo ao LNCC deve passar por análise de mascaramento ou tarjamento

É vedado o compartilhamento de bases de dados ou documentos contendo dados pessoais excessivos (não necessários à finalidade) sem o devido mascaramento.

9. TÉCNICAS DE MASCARAMENTO E TARJAMENTO

Técnica	**Descrição**	**Exemplos**
Substituição	Troca de valores reais por fictícios	Marta Pereira Silva → Lucia Freitas Lemos
Ocultação parcial	Exibição apenas de parte do dado, ocultando o restante com símbolos	**CPF**: 123.456.789-00 → ***.456.***-** **Matrícula**: 12345678 → *****678
Tarjamento	Técnica irreversível aplicada a documentos (físicos ou digitais), onde informações sensíveis são cobertas visualmente para permitir a divulgação do restante do	O servidor [redacted], de matrícula [redacted], compareceu à consulta médica em 15/10/2020...

	documento.	

10. MASCARAMENTO EM DOCUMENTOS E COMPARTILHAMENTOS

Compartilhamento Intersetorial: ao enviar planilhas, documentos ou relatórios para outros setores que não necessitam visualizar dados pessoais específicos, o remetente deve excluir, mascarar ou tarjar esses dados antes do envio, de forma que o receptor não consiga reverter a ocultação de tais dados.

Documentos Digitalizados e PDFs: para documentos que serão publicados ou enviados externamente, deve-se utilizar ferramentas de edição de PDF homologadas, divulgadas na página web do SGSI, que realizem a remoção definitiva da informação, sem que seja possível realizar a extração por OCR.

Documentos Físicos: o tarjamento deve ser feito de forma a impedir a leitura contra a luz ou através do verso da folha.

11. APLICAÇÃO EM SISTEMAS E BANCO DE DADOS

Ambientes de Teste e Homologação : dados reais devem ser mascarados (substituídos ou embaralhados) antes de serem copiados para ambientes de desenvolvimento.

Mascaramento Dinâmico: em sistemas de produção, o dado deve ser apresentado mascarado na tela para usuários sem permissão de visualização total (ex.: atendentes visualizam apenas alguns dígitos do CPF).

12. ATENDIMENTO DE REQUISIÇÃO DE ACESSO À INFORMAÇÃO (LAI)

Em cumprimento à LAI e à LGPD, documentos públicos que contenham informações pessoais **relativas à intimidade, vida privada, honra e imagem** devem ter esses trechos tarjados antes do fornecimento ao requerente.

O documento deve ser fornecido na íntegra, exceto pelas partes tarjadas, garantindo a transparência do ato administrativo sem violar a privacidade de terceiros.

A justificativa para o tarjamento deve ser registrada no processo de atendimento à solicitação.

13. FERRAMENTAS E PROCEDIMENTOS SEGUROS

Deve-se utilizar ferramentas homologadas pela COTIC ou MCTI para realizar o mascaramento, tarjamento e a sanitização de arquivos digitais.

Antes de publicar ou compartilhar um documento tarjado digitalmente, deve-se verificar se os metadados e camadas ocultas do arquivo foram devidamente removidos.

14. EXCEÇÕES

Situações em que a ocultação do dado impeça a finalidade legal ou o cumprimento de obrigação regulatória devem ser analisadas pelo DPO ou pela assessoria jurídica.

15. CONSCIENTIZAÇÃO E TREINAMENTO

Todos os colaboradores, especialmente os que manipulam documentos administrativos e atendem a solicitações externas, devem ser orientados sobre como aplicar o mascaramento e o tarjamento de forma segura e eficaz, evitando vazamentos acidentais por falha técnica na edição de documentos.

16. CONFORMIDADE

A aderência a esta política será auditada periodicamente. O compartilhamento indevido de dados não mascarados ou tarjados será tratado como incidente de segurança, conforme as normas 31-PTIS e 66-PTISDP.

O grau de efetividade do mascaramento e tarjamento poderão ser passíveis de aferimento por critérios de qualidade de privacidade, como o K-anonymity, l-diversity e t-closeness.

17. ANÁLISE CRÍTICA

Este documento deve ser analisado criticamente, quanto à sua eficácia e adequação ao SGSI do LNCC, ao menos, uma vez ao ano.

18. HISTÓRICO DA REVISÃO E QUADRO DE APROVAÇÃO

Revisão	Data	Itens Revisados
1.0	03/02/2026	Documento Inicial.

Quadro de Aprovação		
	Nome	**Atribuição**
Elaborado por:	Diógenes Souza Freitas	Analista em Ciência e Tecnologia
Verificado por:	Luís Rodrigo de Oliveira Goncalves	Gestor de Segurança da Informação
Aprovado por:	Wagner Vieira Léo	Diretor substituto do LNCC

Documento assinado eletronicamente por **Diógenes Souza Freitas**, **Analista em Ciência e Tecnologia**, em 03/02/2026, às 13:17 (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 Cientifica substituto**, em 03/02/2026, às 15:11 (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 **Luis Rodrigo De Oliveira Gonçalves**, **Gestor de Segurança da Informação**, em 03/02/2026, às 16:04 (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 **13494056** e o código CRC **FCA36A89**.