

LGPD MPM

**CARTILHA DE PROTEÇÃO
DE DADOS PESSOAIS
E PRIVACIDADE**





CLAURO ROBERTO DE BORTOLLI
Procurador-Geral de Justiça Militar

JORGE AUGUSTO CAETANO DE FARIAS

Encarregado pelo Tratamento de Dados Pessoais do MPM
Promotor de Justiça Militar

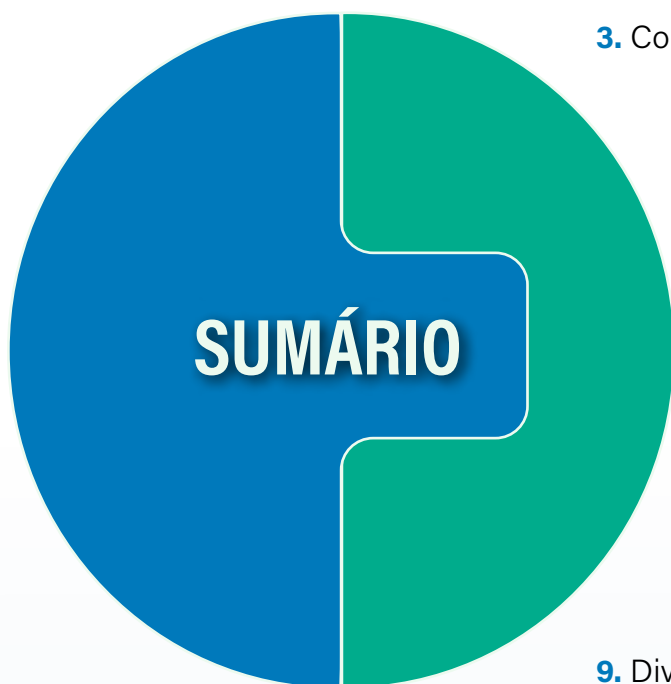
ORGANIZAÇÃO E COORDENAÇÃO

Assessoria de Proteção de Dados Pessoais e Privacidade (ASSPRO)

ESCRITÓRIO DE PROTEÇÃO DE DADOS PESSOAIS

Coautoria (LGPD no SEI):
Coordenadoria de Gestão Documental (CGD)

e-mail: encarregado.lgpd@mpm.mp.br



1. Apresentação 4

2. Fundamentos da Proteção de Dados 5

3. Conceitos Importantes 6

4. Principais Atores na LGPD 10

5. Princípios da Proteção de Dados 12

6. Direitos dos Titulares 14

7. Boas Práticas 15

8. Identificação do Titular 16

9. Divulgação de Dados Pessoais 15

10. LGPD no SEI 18

11. Conclusão 33



CARTILHA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Este é um guia prático de consulta em suas atividades cotidianas, elaborado de forma clara e didática, para que membros, servidores e colaboradores do MPM possam assimilar os principais conceitos, fundamentos e princípios de proteção de dados pessoais.

Nosso objetivo é promover boas práticas de proteção de dados dentro da Instituição.

LGPD + **CNMP**

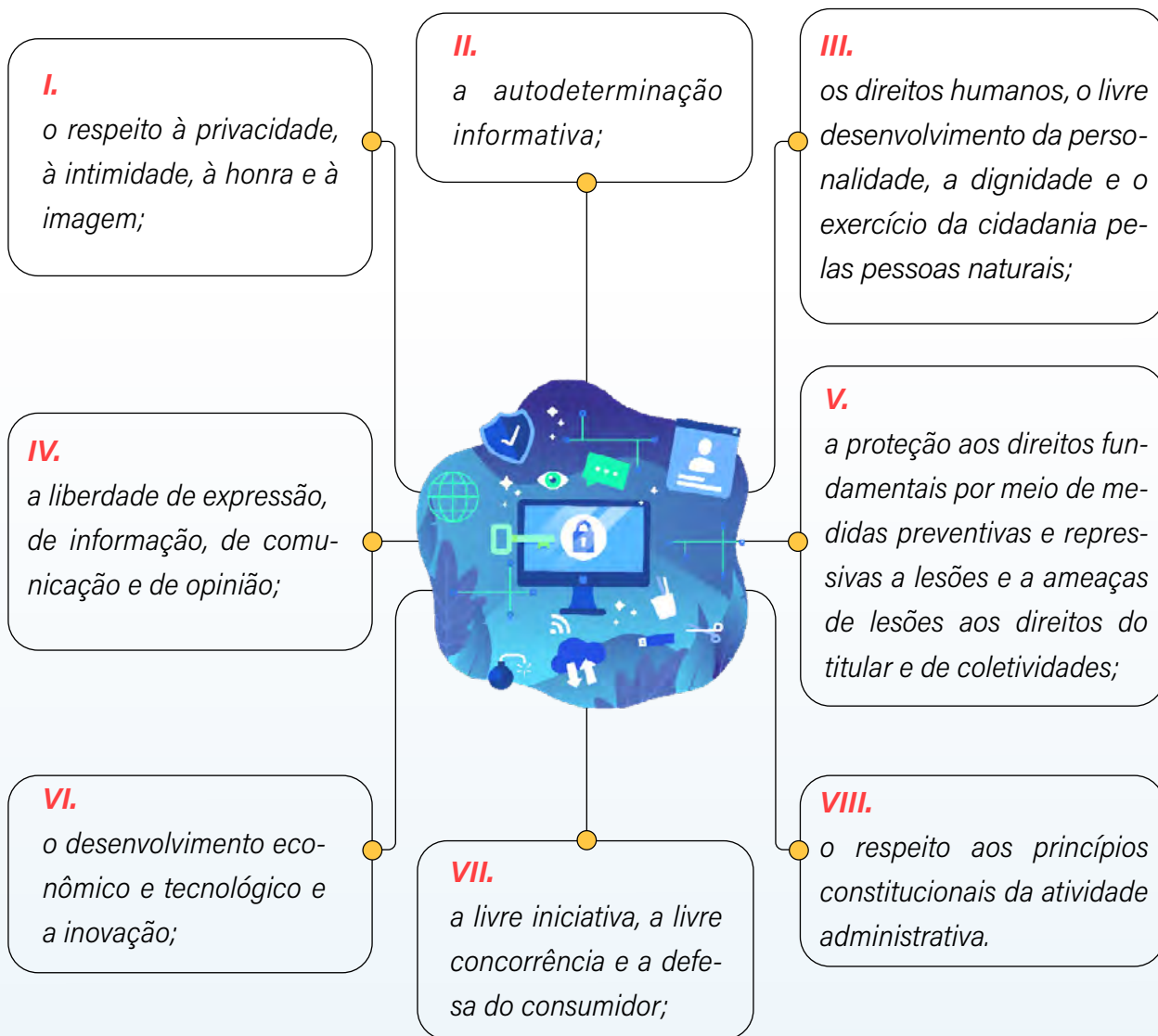
A **Constituição Federal (art. 5, inciso LXXIX)** e a **Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei n 13.709/2018** protegem os direitos fundamentais de liberdade, privacidade, proteção de dados pessoais e o livre desenvolvimento da personalidade, inclusive nos meios digitais.

Para regulamentar a atividade finalística e administrativa do Ministério Público nessa matéria, o CNMP editou a **Resolução n. 281/2023**.

Com regras, diretrizes e princípios bem definidos, toda essa normativa tem como objetivo garantir que os dados pessoais sejam protegidos, assegurando a privacidade e a segurança de todos.

[Acesse o site](#)

A LGPD e a Resolução nº281/2023 do CNMP, ambas em seu art. 2º, estabelecem os fundamentos para a proteção de dados pessoais, que são essenciais para orientar todas as ações relacionadas ao seu tratamento.



3

CONCEITOS IMPORTANTES

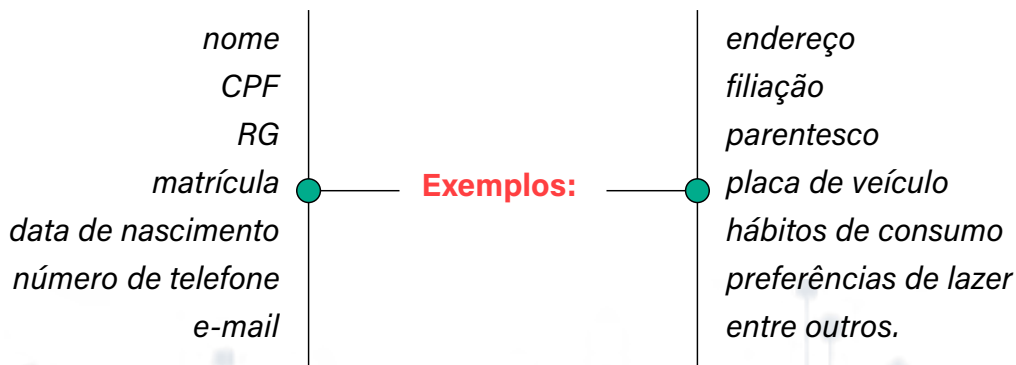
*Conceituar os termos na **Lei Geral de Proteção de Dados (LGPD)** é essencial para garantir clareza e precisão na aplicação da lei. Isso ajuda a estabelecer o escopo das responsabilidades de quem trata dados pessoais e a proteger os direitos dos titulares.*

Sem uma compreensão clara dos conceitos, pode haver interpretações errôneas que comprometam a eficácia da lei. Além disso, ao conceituar os termos, a sociedade passa a ter um entendimento mais claro sobre seus dados pessoais, seus direitos e como exercê-los, promovendo uma cultura de proteção de dados mais robusta e consciente.

1. DADO PESSOAL:



Informação relacionada a pessoa natural que esteja viva e permite identificá-la direta ou indiretamente.



2. DADO PESSOAL SENSÍVEL:



Dado vinculado a pessoa natural, que **revela características particulares** e que quando expostas podem gerar discriminação ou causar prejuízo ao indivíduo.

Exemplos:

- 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 vida sexual;
- dado genético ou biométrico.

3. DADO ANONIMIZADO:



Dado do titular que **não pode ser identificado**, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do seu tratamento.

A anonimização deve seguir preceitos da segurança da informação, os quais estão sob responsabilidade do Departamento de Tecnologia da Informação e da Secretaria de Polícia Institucional, ambos do MPM.

ATENÇÃO!

Se o processo de anonimização puder ser revertido então será considerado dado pessoal e, portanto, estará sujeito às diretrizes da LGPD.

4. CONCEITOS IMPORTANTES:

PSEUDONIMIZAÇÃO



Dado pessoal que perde a possibilidade de associação a um indivíduo, direta ou indireta, somente mediante o uso de informação adicional mantida de forma segregada pelo controlador, em ambiente controlado e seguro.

São **exemplos de técnicas aplicáveis** para fins de pseudonimização ou ocultação de dados pessoais:

- Omitir, tarjar ou mascarar dados pessoais, de modo a impedir a sua exposição direta.
- Suprimir o dado pessoal, substituindo-o pela expressão em latim [omissis], grafada entre colchetes e em itálico.

- Substituir nomes próprios por iniciais, pseudônimos ou expressões genéricas que descrevam o papel da pessoa na relação fática ou processual (por exemplo: investigado, denunciado, réu, vítima, testemunha, representante).

.....

- Aplicar técnicas de generalização, como indicar apenas a categoria do cargo, a idade aproximada, o ano de nascimento, a cidade ou o estado de domicílio, ou a apresentação de valores totais em lugar de itens específicos.

.....

- Suprimir caracteres sensíveis, mantendo apenas parte da informação essencial (por exemplo: CPF *.127.783-).

.....

5. TRATAMENTO DE DADOS PESSOAIS:

Qualquer operação realizada com dados pessoais, por pessoas físicas ou por empresas, órgãos e entidades públicas.

As operações de tratamento estão previstas no **art. 5º, X, da LGPD e no art. 4º, XXXV, da Resolução nº 281/2023/CNMP**, tais como:

- coleta;
- recepção;
- utilização;
- acesso;
- compartilhamento;
- armazenamento;
- avaliação ou controle da
- informação; entre outros.





ATENÇÃO!

DADOS PESSOAIS

DE CRIANÇAS

E ADOLESCENTES

Os dados pessoais de crianças e adolescentes **gozam de maior grau de proteção**, e só devem ser divulgados em situações excepcionais (maior ônus argumentativo).

Nesses casos, o tratamento deve ser feito **sempre para a proteção** e no melhor interesse desses titulares; e, a depender das circunstâncias, será necessário o consentimento dos responsáveis.

Além do **uso de iniciais** em lugar do nome, podem ser adotadas outras medidas de proteção, como a **restrição de acesso** a determinados usuários e a imposição de sigilo ao expediente. Também devem ser resguardados dados de eventuais vítimas e testemunhas.



4

PRINCIPAIS ATORES NA LGPD

*Na **Lei Geral de Proteção de Dados (LGPD)**, os atores são indivíduos ou entidades que desempenham papéis cruciais no tratamento de dados pessoais, sendo responsáveis por assegurar a proteção e o uso adequado das informações.*

Os principais atores:

Titular dos dados

Controlador

Operador

Encarregado

ANPD

*Cada um desses atores desempenha um papel fundamental para a **segurança e privacidade dos dados pessoais**. A compreensão dessas funções é essencial para garantir que a LGPD seja aplicada de forma eficaz.*





I. CONTROLADOR

Pessoa natural ou jurídica, de direito público ou privado, responsável pelas decisões referentes ao tratamento de dados pessoais.



TITULAR DOS DADOS PESSOAIS

Pessoa natural identificada ou identificável, independente da sua nacionalidade ou do local da sua residência.

No MPM, os titulares podem ser cidadãos, terceirizados, membros, servidores, estagiários, representantes de empresas contratadas, entre outros.



II. OPERADOR

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador.



III. ANPD - AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS

Agência Reguladora vinculada ao Ministério da Justiça e Segurança Pública, que tem como missão zelar pela proteção de dados pessoais e é o órgão central de interpretação da Lei Geral de Proteção de Dados (LGPD).



IV. APDP/MP - AUTORIDADE DE PROTEÇÃO DE DADOS PESSOAIS NO MINISTÉRIO PÚBLICO

Responsável por zelar, implementar e fiscalizar a proteção de dados pessoais no Ministério Público brasileiro, por meio da sua Unidade Especial de Proteção de Dados Pessoais (UEPDAP), vinculada à Comissão de Preservação da Autonomia do Ministério Público (CPAMP).

IV. ENCARREGADO

*Pessoa **indicada pelo Controlador** para atuar como canal de comunicação entre o MPM, titulares dos dados, ANPD e APDP/MP.*



5

PRINCÍPIOS DA PROTEÇÃO DE DADOS

O tratamento de dados pessoais deve observar os princípios estabelecidos no **artigo 6º da LGPD** e **artigo 3º da Resolução nº 281/2023 do CNMP**, quais sejam:

1. FINALIDADE:



Realização de tratamento de dados pessoais com fins legítimos, explícitos, específicos e informados aos titulares.

4. LIVRE ACESSO E TRANSPARÊNCIA:

Direito de consulta facilitada e precisa sobre os dados pessoais necessários para a tutela de direitos fundamentais, observadas as hipóteses constitucionais de reserva jurisdicional prévia ao acesso.

2. BOA-FÉ E ADEQUAÇÃO:



Compatibilidade do tratamento de dados com as finalidades informadas ao titular de dados pessoais.



3. NECESSIDADE:



Limitação do tratamento ao mínimo necessário para atendimento à finalidade informada ao titular.

5. QUALIDADE DOS DADOS:



Os dados pessoais devem ser tratados com clareza, precisão, de forma atualizada e completa.

6. SEGURANÇA E PREVENÇÃO:



Ação de medidas de proteção para garantir a disponibilidade, inviolabilidade e confidencialidade dos dados.

9. PROPORCIONALIDADE E RAZOABILIDADE:



Os dados devem ser tratados de maneira proporcional e razoável, observada a finalidade informada ao titular.

7. NÃO DISCRIMINAÇÃO:



O tratamento de dados pessoais não deve ser realizado com fins ilícitos, abusivos ou discriminatórios.

10. NA TUTELA DOS DIREITOS FUNDAMENTAIS:



Dever de proteção suficiente dos direitos fundamentais, como o direito à privacidade e proteção de dados pessoais.

8. RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS:



Aplicação da responsabilidade de cumprimento das normas de proteção de dados aos agentes de tratamento, com comprovação da eficácia das medidas adotadas.



Como
proprietário
dos seus dados
pessoais, o
titular possui
direitos e
garantias, tais
como:

- 1 Confirmação da **existência do tratamento e acesso** aos seus dados pessoais;
- 2 Solicitação de **correção de dados incompletos, inexatos ou desatualizados**;
- 3 **Anonimização**, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade;
- 4 **Oposição ao tratamento** em casos específicos e de descumprimento da lei;
- 5 **Revogação do consentimento**, a qualquer momento, por meio de procedimento facilitado e gratuito;
- 6 **Revisão de decisões** tomadas unicamente com base em tratamento automatizado que afetem seus interesses;
- 7 **Restrição do tratamento**, por meio da recusa em fornecer o consentimento, quando este for necessário, em casos específicos e quando a base legal para o tratamento for exclusivamente de consentimento;
- 8 Pedido de **esclarecimento e realização de reclamação** perante a ANPD e a APDP/MP contra o Controlador em casos de irregularidade.



Proteja os dados pessoais com cuidado.



Use senhas fortes e exclusivas, com troca periódica sempre que solicitado.

Colete apenas informações necessárias.

Realize o tratamento de dados na medida de suas atribuições.

Busque usar os dados pessoais de maneira exata e atualizada.

Observe se há uma finalidade específica e legítima para o tratamento.

Elimine dados que não possuem mais justificativa de manutenção.

Guarde os dados pelo tempo necessário para a finalidade do tratamento.

Utilize os meios institucionais para o compartilhamento de informações.

Bloqueie a tela do computador quando ausente do seu local de trabalho.

Mantenha a mesa organizada para evitar a exposição de dados pessoais.

Utilize somente ferramentas homologadas pelo Departamento de TI.

Verifique se os destinatários do E-mail necessitam dos dados compartilhados.

Observe as orientações e normas internas de proteção de dados do MPM.



Não compartilhe suas senhas e restrinja o número de logins simultâneos.

Não tire foto ou filme documentos que contenham dados pessoais.

Não utilize equipamentos institucionais para fins pessoais.

Não insira dados em plataformas desconhecidas (ex: IA, editor de texto).

**PRECISO
UTILIZAR TODAS
AS INFORMAÇÕES
PESSOAIS DOS
TITULARES DE DADOS
PARA IDENTIFICÁ-
LOS EM PEÇAS
PROCESSUAIS**



A legislação exige que peças processuais contenham a qualificação completa das pessoas envolvidas (investigados, réus, testemunhas, vítimas etc.).

Porém, para outras finalidades — como divulgação ou consulta pública — nem sempre é necessário expor todos os dados pessoais.

Nesses casos, as informações podem ser pseudonimizadas, com versões diferentes do mesmo documento conforme a finalidade de uso.

ATENÇÃO!**CUIDADO COM****A DIVULGAÇÃO****DE DADOS****PESSOAIS!**

Quando houver necessidade de divulgar informações por meio da **Secretaria de Comunicação Social do MPM (SECOM)**, o setor demandante deve definir quais dados pessoais são realmente de interesse público e adotar medidas para proteger os demais — especialmente dados sensíveis, de crianças e adolescentes, vítimas e testemunhas.

Por isso, ao enviar peças, vídeos, áudios ou outros documentos para divulgação, **eles devem chegar previamente tratados**, conforme as regras do Sistema de Comunicação Social do MPM (**Portaria nº 152/PGJM, de 14 de julho de 2025**). Cabe ao sistema verificar se as medidas de proteção de dados foram corretamente aplicadas.

O Sistema Eletrônico de Informações (SEI) é a ferramenta adotada pelo Ministério Público Militar **para produzir e tramitar documentos**, preferencialmente relacionados aos atos administrativos.

Todos os integrantes da instituição (membros, servidores, estagiários, residentes e voluntários) **têm acesso ao SEI** e produzem documentos diariamente.

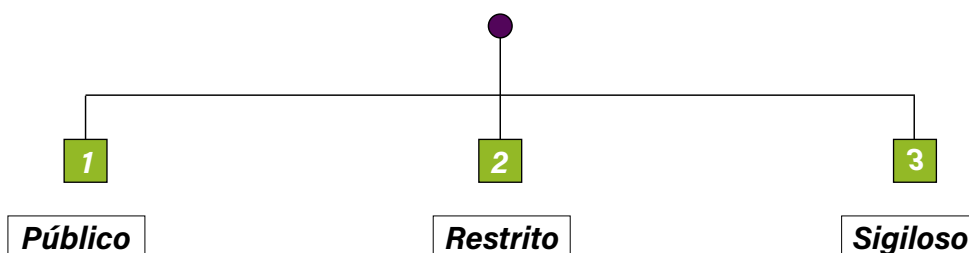
É necessário utilizar os registros observando os normativos existentes, incluindo a LGPD.

Algumas operações específicas do Sistema exigem atenção dos usuários para não comprometer a segurança das informações, a imagem e a intimidade das pessoas.

Diante desse cenário, esta Cartilha apresentará os pontos críticos do uso do SEI, relacionando-os com a exposição de dados pessoais.



O **SEI** disponibiliza três opções de níveis de acesso aos processos e documentos, quais sejam:

**ATENÇÃO!**

Ao criar processos e produzir documentos, é essencial **selecionar cuidadosamente o nível de acesso adequado**.

Isso se aplica tanto a documentos internos (produzidos no SEI) quanto externos (digitalizados ou capturados de outros softwares e inseridos no SEI).

Uma escolha mal fundamentada pode ter implicações significativas.

A escolha do Nível de Acesso influencia diretamente a realização de pesquisas no Sistema e no Portal da Transparência, **determinando quem poderá acessar os conteúdos**.

A seguir, serão detalhados os Níveis de Acesso disponibilizados pelo SEI, com suas respectivas categorizações.

ATENÇÃO!

Cabe ao usuário do Sistema (membro, servidor, residente, estagiário ou voluntário), máxima **atenção quanto à escolha do Nível de Acesso**, bem como **à retificação/alteração**, se encontrar processo ou documento produzido com parâmetros incorretos.

1 DOCUMENTAÇÃO PÚBLICA

Não possui restrição de acesso.

Pode ser localizada e ter seu conteúdo lido integralmente.

INFORMAÇÕES DETALHADAS:

Conforme a **Lei de Acesso à Informação, nº 12.527, de 18 de novembro de 2011**, em seu **Art. 6º, inciso I**, **cabe ao órgão público a “gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação”.**

Seguindo esse princípio, é necessário **produzir e manter registros públicos, permitindo sua consulta, localização e leitura.**

Essa ideia é **reforçada por normativo interno**, que define informações ostensivas

como aquelas que “não possuem restrição de acesso, ou seja, são consideradas públicas ou franqueadas”.

Um processo ou documento público é aquele cujo acesso é plenamente franqueado ao usuário interno, por meio de pesquisa no SEI, e aos cidadãos, por meio do Portal da Transparência.

Um registro definido como público no SEI é passível de pesquisa e apresentado de forma íntegra ao usuário, permitindo a leitura de todo o teor.

Essa mesma lógica não se aplica às Minutas (documentos internos não assinados). As Minutas ficam disponíveis para leitura apenas às pessoas lotadas na unidade produtora desses registros.

2 DOCUMENTAÇÃO RESTRITA:

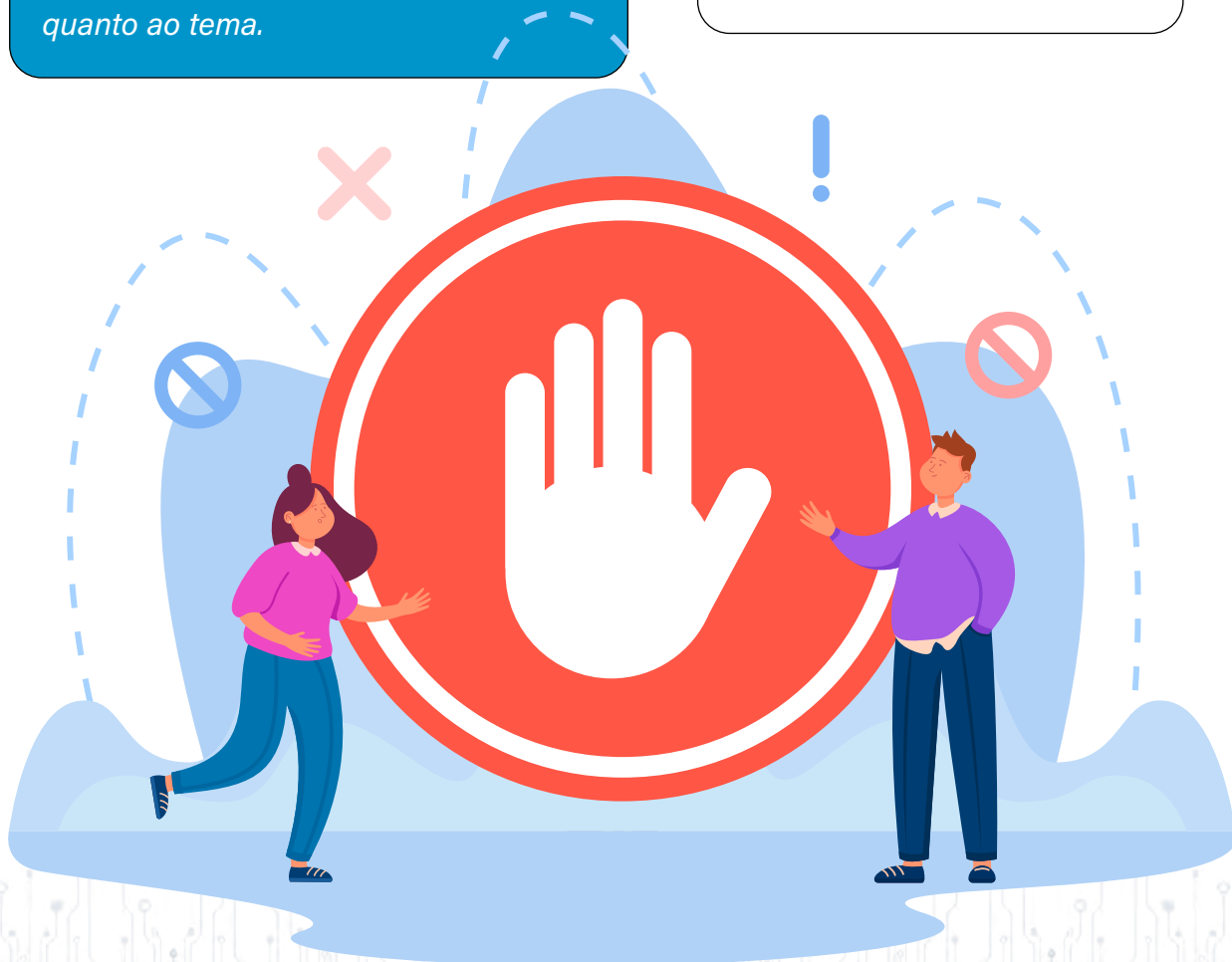
É aquela disponível para leitura apenas para os usuários da unidade produtora e para os que acessam caixas por onde o processo tramitou.

Trata-se de documentação, cujo teor não deva ser de amplo conhecimento, sendo necessário manter os registros passíveis de plena utilização apenas às partes que tenham alguma tratativa ou atuação quanto ao tema.

ATENÇÃO!

Alguns exemplos práticos:

formulários, nos quais existam campos relativos aos documentos pessoais; relatórios de saúde; avaliações de desempenho; processos nos quais constem cópias de documentos pessoais, entre outros.



INFORMAÇÕES DETALHADAS:

Dada a subjetividade da aplicação do Nível de Acesso restrito, um relevante apoio é a **Portaria nº 201/PGJM, de 8 de novembro de 2017.**

O **Art. 4º** é um norteador para o uso do **SEI**, embora também possa ser aplicado a outros sistemas e aos documentos físicos.

Art. 4º O Ministério Público Militar manterá, independentemente de classificação, acesso restrito em relação às informações e documentos sob seu controle e sua posse, mantidos em qualquer suporte, relacionadas a:

I – informações pessoais relativas à intimidade, à vida privada, à honra e à imagem das pessoas;

II – informações e documentos caracterizados em normas específicas como sendo de natureza sigilosa, tais como sigilo fiscal, patrimonial ou bancário;

III – processos judiciais sob segredo de justiça e procedimentos relativos a qualquer espécie de ação de natureza investigativa;

IV – identificação do denunciante, até que se conclua o procedimento investigativo;



V– documentos e informações de natureza técnica, produzidos por outros órgãos e entidades, em poder do Ministério Público Militar sem a característica de custódia;

VI – relatórios e notas técnicas decorrentes de investigações, perícias e fiscalizações, e outros documentos relativos a ações na área de competência do Ministério Público Militar, quando ainda não concluídos os respectivos procedimentos.

TRANSPARÊNCIA X NÍVEL DE ACESSO NO SEI

O Portal da Transparência, disponível no site do MPM, oferece acesso específico aos processos gerados no SEI por meio do 'Módulo de Pesquisa Pública do SEI'.

Nesse módulo, qualquer cidadão pode pesquisar livremente a documentação institucional, podendo localizar e ler sobre diversos temas.

As exceções são os documentos classificados como Restritos e Sigilosos.

ATENÇÃO!

É essencial escolher cuidadosamente o Nível de Acesso dos processos e documentos.

O objetivo é garantir transparência à sociedade, sem expor desnecessariamente temas sensíveis que não devem ser de domínio público.

INFORMAÇÕES DETALHADAS:

Mesmo que um processo esteja configurado como **Restrito**, ele **será recuperado na busca do cidadão**, permitindo a visualização de uma lista de links dos documentos. No entanto, **a leitura do conteúdo dos arquivos não será possível**.

Para **processos Públicos**, nos quais os documentos são Públicos, o cidadão terá acesso completo ao teor do processo, podendo ler integralmente todos os documentos.

Nos processos **Públicos** que **contêm documentos Públicos e Restritos**, a visualização mostrará claramente a diferença entre eles.

Documentos Públicos serão acessíveis, enquanto os Restritos não terão links ou qualquer forma de acesso ao conteúdo. O cidadão verá uma mensagem indicando a restrição de acesso.

Processos e documentos Sigilosos não são recuperados pela busca do Módulo.

[Pesquisa pública do SEI.](#)



É a documentação que possui restrição provisória de acesso público, devido à sua importância para a segurança da sociedade e do Estado, de forma geral.

No entanto, ao aplicar o conceito de forma mais específica, entende-se que a documentação sigilosa é aquela que pode colocar em risco os envolvidos em programas, projetos, planos e operações do MPM.

Isso inclui outras instituições e pessoas físicas, sejam elas parte do quadro funcional do órgão ou não.

ATENÇÃO!

Documentação sigilosa só pode ser consultada pelo indivíduo que a produziu e por aqueles com permissão, ou seja, usuários com Credencial de Acesso.

Os processos não são recuperados pela Pesquisa e não são visíveis para outras pessoas na mesma unidade do agente com a Credencial.

INFORMAÇÕES DETALHADAS:

Os graus de sigilo dos registros (reservado, secreto e ultrassecreto) são visualizados no SEI, na tela de cadastro do processo, na opção Hipótese Legal.

Registros ultrassecretos

São aqueles cujo acesso às informações possa colocar em risco a defesa e a soberania nacionais ou a integridade do território nacional e de suas instituições.

Registros secretos

São aqueles cujo conhecimento não autorizado possa acarretar graves danos à segurança dos autores e envolvidos.

Registros reservados

São aqueles cujo conhecimento por pessoas não autorizadas possa frustrar os objetivos e dificultar os trâmites e o desenvolvimento de ações pelo MPM.

É importante esclarecer que **a produção de processos sigilosos segue um critério hierárquico**, não sendo adequada para qualquer integrante da instituição. **Conforme a Portaria nº 201/PGJM, de 2017, no Art. 8º**, a classificação do sigilo de informações no âmbito do MPM é de competência:

No grau ultrassecreto:

do Procurador-Geral de Justiça Militar, existindo a hipótese de delegação;

No grau secreto:

do Diretor-Geral e dos Membros, no exercício de função administrativa;

No grau reservado:

das autoridades mencionadas anteriormente e dos ocupantes de cargos em comissão CC-3 a CC-5, na respectiva área de atuação.

Relação entre o Nível de Acesso e a consulta:

Consulta Nível de Acesso	Público interno (membros, servidores, estagiários, residentes e voluntários, ou seja, pessoas com cadastro no SEI).	Público externo (aceso pelo Portal da Transparência).
Processo público (documentos públicos)	Todas as pessoas de todas as unidades do órgão. Acesso integral: recuperação por meio da Pesquisa e leitura de todo o conteúdo.	Todos os cidadãos. Acesso integral: recuperação por meio da Pesquisa e leitura de todo o conteúdo.
Processo público (documentos públicos e restritos)	Todas as pessoas lotadas na unidade de origem do processo ou naquelas por onde o processo tramitou. Para as demais, é possível recuperar o processo por meio da Pesquisa, contudo, apenas as árvores dos processos são expostas, não sendo possível ler os conteúdos.	O cidadão recupera por meio da Pesquisa, mas não visualiza integralmente o conteúdo. Os itens públicos poderão ser acessados e lidos normalmente. Os itens restritos serão exibidos, mas não será possível abrí-los.
Processo restrito (documentos restritos)	Todas as pessoas lotadas na unidade de origem do processo ou naquelas por onde o processo tramitou. Para as demais, é possível recuperar o processo por meio da Pesquisa, contudo, apenas as árvores dos processos são expostas, não sendo possível ler os conteúdos.	O cidadão recupera por meio da Pesquisa, mas não visualiza o conteúdo. Há uma mensagem, na qual é explicado que o conteúdo é restrito e há um contato para dúvidas.
Processo restrito (documentos públicos e restritos)	Todas as pessoas lotadas na unidade de origem do processo ou naquelas por onde o processo tramitou. Para as demais, é possível recuperar o processo por meio da Pesquisa, contudo, apenas as árvores dos processos são expostas, não sendo possível ler os conteúdos.	O cidadão recupera por meio da Pesquisa, mas não visualiza o conteúdo. Há uma mensagem, na qual é explicado que o conteúdo é restrito e há um contato para dúvidas.
Processo sigiloso	Apenas usuários específicos, credenciados pelo criador do processo ou por outros usuários, que já tenham acesso ao processo. Um usuário que receba a credencial também consegue concedê-la a uma outra pessoa e assim sucessivamente. Os processos não são recuperados por meio da Pesquisa. Administradores do SEI podem consultar os números (apenas os números, sem acesso aos conteúdos), por meio de função específica, com o intuito de auxiliar as unidades.	Os processos não são recuperados. Não é feita qualquer referência à documentação sigilosa.

8.2 ALTERAÇÃO DO NÍVEL DE ACESSO

A Retificar/alterar o Nível de Acesso de um PROCESSO

Para realizar a mudança do Nível de Acesso de um processo, basta selecioná-lo e clicar no botão Consultar/Alterar Processo.

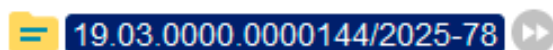
Selecione o processo;

Clique no botão "Consultar/Alterar Processo";

Altere o Nível e salve.

Alteração de Nível de Acesso de um processo pode ser feita por qualquer usuário da unidade produtora ou das unidades por onde o processo tramitou, exceto para processos sigilosos.

1



2



3

B Retificar/alterar o Nível de Acesso de um DOCUMENTO

Para realizar a mudança do Nível de Acesso de um documento, basta selecioná-lo e clicar no botão Consultar/Alterar Documento.

1 *Selecione o documento;*

2 *Clique no botão “Consultar/Alterar Documento”;*

3 *Altere o Nível e salve.*

1

 DGP - Relatório de Trabalho Híbrido _março (1623145)

2



3

Nível de Acesso

 Sigiloso

 Restrito

 Público

Salvar

A alteração do Nível de Acesso de um documento está limitada aos usuários da unidade produtora. Mesmo que o processo esteja aberto em várias unidades, a mudança só é possível para aqueles que utilizam a caixa onde o arquivo foi inserido.

POR QUE É TÃO IMPORTANTE OBSERVAR RIGOROSAMENTE O NÍVEL DE ACESSO?

A principal questão é evitar riscos e exposições desnecessárias, pois informações sensíveis podem ser localizadas e usadas de forma prejudicial. A LGPD também aborda situações específicas relacionadas a dados pessoais. Alguns exemplos incluem processos com relatórios médicos e outras informações de saúde.

1 MUDANÇA DE LOTAÇÃO

Um aspecto importante relacionado à segurança da informação é a manutenção dos usuários em cada unidade do Sistema. Quando alguém muda de lotação, espera-se o rápido desligamento dessa pessoa da unidade do SEI anteriormente utilizada. Cada gestor deve verificar se os integrantes da equipe correspondem aos que estão acessando a unidade.

ATENÇÃO!

Um usuário indevido numa unidade pode ler todos os conteúdos na tela inicial (Controle de Processos), realizar pesquisas em Blocos Internos e Acompanhamentos Especiais, e utilizar os resultados da Pesquisa, que está relacionada aos Níveis de Acesso.

INFORMAÇÕES DETALHADAS:

Uma forma simples de realizar a conferência é simular uma Atribuição de Processos.

Ao selecionar um processo e clicar no botão Atribuição de Processos, o gestor verá um combo com os nomes de todos os usuários daquela caixa do SEI.

Se houver ajustes necessários, o Suporte SEI deve ser acionado.

O botão está na primeira página da Intranet, na coluna à esquerda da tela.

É importante manter apenas o mínimo de pessoas necessárias em cada unidade para evitar a disponibilização indevida de informações.

Sugere-se manter na unidade apenas o chefe, o chefe substituto e as pessoas que realizam operações ou consultas diretamente relacionadas às pautas da caixa.

8.3

DISPONIBILIZAÇÃO DE DOCUMENTOS PARA USUÁRIOS EXTERNOS

Diversas unidades do MPM relacionam-se com outras instituições, disponibilizando documentos para usuários externos.

Sugere-se disponibilizar apenas o documento específico a ser analisado ou assinado pelo representante da outra organização, evitando consulta livre ao teor completo do processo.

INFORMAÇÕES DETALHADAS:

A disponibilização de documentos para usuários externos ocorre por meio do botão **"Gerenciar Liberações para Assinatura Externa"**.



O usuário pode selecionar os documentos a serem disponibilizados usando a opção **"Selecionar Protocolos para Acesso Externo"** (ícone da lupa no canto direito).

Gerenciar Assinaturas Externas

E-mail da Unidade:
PGJME-mail da Coordenadoria de Gestão Documental <dg.cgd@mpm.mp.br>

Liberar Assinatura Externa para:
ELIANE ALVES ALÍPIO (elialpio@yahoo.com.br)

☒ Som visualização integral do processo

Protocolos adicionais disponibilizados para consulta (clique na lupa para selecionar):

☐ Permitir inclusão de documentos

Validade (dias): Senha:

As publicações no Boletim de Serviço Eletrônico (BSe) são irreversíveis.

Não é possível excluir ou cancelar uma publicação. O sistema permite apenas agendá-las, republicá-las, retificá-las ou apostilá-las.

Em caso de agendamento, é possível cancelar a ação para evitar a publicação do documento. Republicações, retificações e apostilamentos geram publicações relacionadas, ou seja, a publicação original sempre estará associada àquela feita posteriormente e vice-versa.

Na prática, isso significa que ao consultar uma publicação retificada ou apostilada, a outra publicação sempre aparecerá como resultado da pesquisa.

Quanto à Retificação, é importante explicar que não funciona como a edição de um documento.

A Retificação gera uma nova publicação, vinculada àquela que precisa de correção. Mesmo utilizando esse recurso, a primeira publicação nunca será apagada.

ATENÇÃO!

O uso do BSe é extremamente sensível.

Antes da publicação, é necessário verificar se o documento não fere questões da LGPD, LAI e outros normativos, dado seu caráter permanente e considerando que fará parte da base de pesquisa do SEI para usuários internos e externos (no Sistema e no Portal da Transparência).

Questões que envolvam debates éticos, situações de exposição ou constrangimento, informações de interesse particular, entre outras, NÃO DEVEM SER PUBLICADAS NO BOLETIM.

INFORMAÇÕES DETALHADAS:

Uma sugestão para o fluxo das atividades é sempre revisar o texto antes de clicar no botão de Publicação.

Para dúvidas operacionais sobre o uso do Boletim, a Coordenadoria de Gestão Documental (CGD) oferece o suporte necessário.

É importante lembrar que o objetivo principal do Boletim é divulgar os atos da Administração, sem gerar desgaste ou implicações negativas.

Os documentos devem ser objetivos, curtos, diretos e simplificados, com textos claros e de fácil compreensão.

Para situações específicas e delicadas, como sindicâncias, apenas a manifestação da autoridade decisora deve constar no Boletim, de forma sintética. Não cabe publicar detalhes, mencionar análises ou discorrer sobre ações do processo. O intuito é publicizar apenas o resultado, sem explicitar os caminhos adotados para alcançá-lo, da maneira mais breve possível.

Isso também se aplica a documentos sobre saúde, condutas inadequadas de integrantes do órgão, situações de risco, entre outros.

O SEI não permite a publicação de qualquer tipo de documento no BSe, funcionando como um bloqueio inicial para evitar publicações indevidas. No entanto, todos os usuários devem ter extrema atenção e zelo ao usar a ferramenta, fazendo uma crítica apurada quanto ao teor do que será publicado.

É sempre oportuno avaliar eventuais danos ou dissabores antes de efetivar a publicação.

CONCLUSÃO

O Ministério Público Militar trata dados pessoais garantindo transparência e proteção da privacidade, em atenção ao seu papel na defesa do regime democrático e da ordem jurídica.

As medidas de privacidade e proteção de dados estão em constante revisão para assegurar os direitos fundamentais de liberdade, privacidade e proteção dos dados pessoais, além do desenvolvimento da personalidade.

O público interno do MPM deve proteger os dados pessoais sob sua responsabilidade.

Esta cartilha reforça boas práticas e governança conforme os princípios da LGPD, da Resolução CNMP nº 281/2023 e demais atos normativos sobre a matéria, aplicáveis ao ciclo de vida dos dados pessoais.

Além de orientar, a cartilha promove a cultura de proteção de dados e alerta sobre riscos, indicando formas de minimizá-los.

Cumprir as normativas resguarda nossos direitos.

Vamos juntos fortalecer essa iniciativa!

ESSE COMPROMISSO É DEVER DE TODOS!

