Guia Prático

Controladoria-Geral do Estado
de Mato Grosso do Sul

Crédito Imagem: Pixabay – Geralt

PROTEÇÃO DE DADOS PESSOAIS

LGPD NA CGE-MS

VERSÃO: Setembro 2025

Controladoria-Geral do Estado
de Mato Grosso do Sul

Carlos Eduardo Girão de Arruda
Controlador Geral do Estado

Marina Hiraoka Gaidarji
Controladora-Geral Adjunta do Estado

Elaboração:
Rosely Pereira Maia
Encarregada pelo Tratamento de Dados Pessoais
contato: encarregadolgpd@cge.ms.gov.br

Identidade Visual
Diagramação
Thalita Vieira

Controladoria-Geral do Estado
de Mato Grosso do Sul

SUMÁRIO

APRESENTAÇÃO

A Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018) estabelece normas sobre como os dados pessoais devem ser coletados, armazenados e compartilhados. Para os órgãos públicos, isso significa a responsabilidade de adotar práticas que respeitem a privacidade dos cidadãos. Por meio dessas ações, os servidores contribuem diretamente para fortalecer a confiança da sociedade no uso responsável das informações pessoais sob a guarda do órgão.

Na Controladoria-Geral do Estado de Mato Grosso do Sul (CGE/MS), a implementação da LGPD trouxe a necessidade de repensar a forma como lidamos com os dados pessoais. Para nós, servidores,significa adotar uma nova postura, com mais cuidado, atenção e responsabilidade no tratamento das informações pessoais. Essa mudança demonstra o compromisso do órgão com a ética, a transparência e a integridade na gestão pública.

Dando continuidade ao trabalho iniciado na CGE/MS em 2021, percebemos a necessidade de elaborar este novo material, não com a intenção de esgotar o tema, mas sim de oferecer orientações úteis que possam ajudar no dia a dia, com foco nas boas práticas em proteção de dados pessoais.

Rosely Pereira Maia
Encarregada pelo Tratamento de Dados Pessoais na CGE/MS

CGE

Controladoria-Geral do Estado
de Mato Grosso do Sul

LGPD EM POUCAS PALAVRAS

A Lei Geral de Proteção de Dados Pessoais (Lei Federal nº 13.709/2018) é a norma que disciplina a coleta, a utilização, o armazenamento e o compartilhamento de dados pessoais no Brasil. Em vigor desde setembro de 2020, a LGPD tem como objetivo principal proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da pessoa natural.

A LGPD é aplicável a todas as organizações, públicas ou privadas, que tratam dados pessoais, independentemente do porte, abrangendo também o ambiente digital.

A lei utiliza a nomenclatura **"tratamento"** todas as vezes em que se refere a qualquer operação realizada com dados pessoais, como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, difusão ou extração.

Para assegurar que o tratamento dos dados pessoais ocorra de forma ética, segura e transparente, respeitando os direitos dos titulares, a LGPD estabelece **princípios** que formam a base para práticas corretas e seguras. Todos são importantes, mas alguns se destacam por sua aplicação prática e impacto direto na proteção dos dados pessoais, como a finalidade, a necessidade, a transparência, a segurança e a responsabilização.

"A LGPD é aplicável a todas as organizações, públicas ou privadas, que tratam dados pessoais, independentemente do porte, abrangendo também o ambiente digital."

ENTENDENDO DO INÍCIO: O QUE SÃO DADOS PESSOAIS?

A Lei Geral de Proteção de Dados (LGPD), em seu artigo 5º, define dado pessoal como qualquer informação que identifique ou possa identificar uma pessoa física. Explicando melhor, informações como CPF, Carteira de Identidade Nacional (antigo RG), gênero, data e local de nascimento, e-mail, endereço residencial, endereço de IP e, até mesmo, um histórico de serviço podem ser classificadas como dados pessoais — desde que, isoladamente ou combinadas com outros elementos, permitam reconhecer alguém direta ou indiretamente.

Por exemplo, palavras como "Auditor do Estado", "sexo masculino", "trabalha na Auditoria-Geral do Estado", "nascido em Bonito/MS" podem, separadamente, não dizer muita coisa.

No entanto, se apenas um servidor corresponder a esse conjunto de características, a combinação dessas referências é suficiente para identificá-lo. Nesse caso, a informação passa a ser considerada um dado pessoal.

[Crédito imagem: Pixabay (Geralt)]

A LGPD também define uma categoria especial que requer tratamento mais criterioso: os **dados pessoais sensíveis**.

O uso inadequado desses dados pode resultar em discriminação, violação de direitos fundamentais, danos materiais e morais, sanções legais e, inclusive, na perda de confiança dos cidadãos na instituição responsável pelo seu tratamento.

Dados pessoais sensíveis englobam:

- Origem racial ou étnica
- Convicção religiosa
- Opinião política
- Filiação a sindicato ou organização de caráter religioso, filosófico ou político
- Dados referentes à saúde ou à vida sexual
- Dados genéticos ou biométricos

ATENÇÃO: É importante observar que um **dado pessoal comum pode se tornar um dado pessoal sensível** quando expuser informações mais vulneráveis, capazes de afetar a privacidade e direitos fundamentais de um indivíduo.

Exemplo: O nome do servidor é um dado pessoal comum, mas se divulgado em um documento sobre reuniões sindicais, passa a ser sensível, por revelar filiação a sindicato.

TITULAR DE DADOS: O PROTAGONISTA DA PROTEÇÃO DE DADOS PESSOAIS

CGE
Controladoria-Geral do Estado
de Mato Grosso do Sul

A LGPD confere uma série de direitos ao titular.

Você, servidor público da CGE/MS, também possui esses direitos.

E deve, sobretudo, resguardar os direitos das pessoas cujos dados estão sob a responsabilidade da CGE/MS, em razão de execução de política pública ou das atribuições legais ou regulatórias exercidas pelo órgão.

Assim, manifestantes, beneficiários, usuários de serviços públicos, fornecedores e prestadores de serviço, entre outros, têm seus direitos assegurados pela LGPD. Entre essas prerrogativas, destacam-se: a confirmação da existência de tratamento; o acesso aos dados pessoais; a correção de dados incompletos, inexatos ou desatualizados e a faculdade de saber com quais entidades públicas e privadas seus dados foram compartilhados.

Esses direitos têm como objetivo fortalecer a autonomia do cidadão sobre seus dados, assegurando mais transparência e controle. Eles podem ser exercidos a qualquer tempo, por meio da plataforma: https://falabr.cgu.gov.br.

A proteção adequada dos dados pessoais vai muito além da preocupação em evitar sanções aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável por regulamentar e fiscalizar a Lei Geral de Proteção de Dados (LGPD) no Brasil. Trata-se, acima de tudo, de garantir a privacidade e os direitos fundamentais dos cidadãos.

Nesse contexto, é essencial que os servidores da CGE/MS estejam atentos às boas práticas relacionadas à proteção de dados pessoais. O descumprimento dessas diretrizes pode gerar consequências sérias, inclusive a responsabilização de agentes públicos, conforme previsto no artigo 42 da LGPD.

Compete ao Encarregado pelo Tratamento de Dados Pessoais orientar os servidores do órgão quanto às condutas adequadas no tratamento de dados pessoais. Por esse motivo, apresentamos a seguir um conjunto de procedimentos recomendados, com o objetivo de reforçar a proteção nas rotinas de trabalho que envolvem informações pessoais sob a responsabilidade desta CGE/MS.

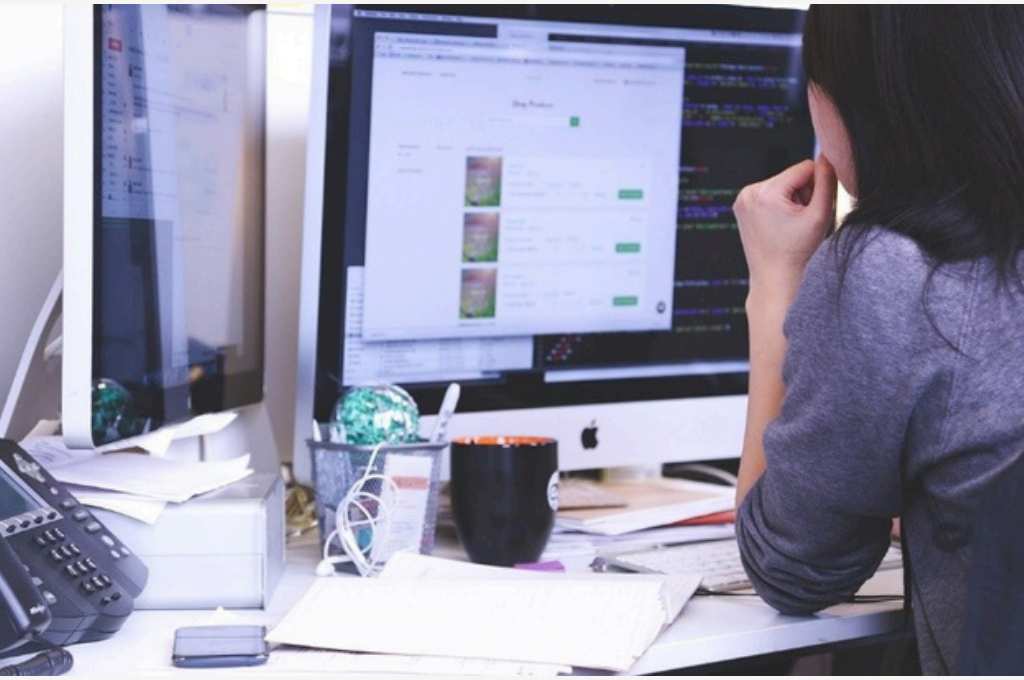
BOAS PRÁTICAS AO UTILIZAR COMPUTADORES E NOTEBOOKS

- Sempre bloquear a estação de trabalho ao se ausentar da mesa, utilizando as teclas Ctrl + Alt + Del ou Windows + L, a fim de prevenir o acesso de pessoas não autorizadas a informações restritas;

- Evitar a captura e compartilhamento de imagens, como prints, fotos ou vídeos, com dados pessoais, principalmente por meio de canais de comunicação não oficiais;

- Não realizar o download de arquivos pessoais no computador ou notebook de trabalho, pois podem conter malwares que comprometem a segurança dos sistemas institucionais;

- Efetuar a formatação completa do dispositivo antes de seu descarte, doação ou transferência, garantindo a remoção definitiva de todos os dados sensíveis nele armazenados.



(Crédito Imagem: Pixaby –Startup Stock)

BOAS PRÁTICAS AO USAR IMPRESSORAS E SCANNERS

- Cadastrar uma senha para impressão para que os documentos só sejam liberados com a presença do usuário, evitando o acesso indevido a informações sigilosas ou pessoais;
- Retirar os documentos da impressora imediatamente, caso não haja senha de impressão, especialmente se contiverem dados pessoais;
- Imprimir apenas o estritamente necessário, evitando a reprodução de documentos que contenham dados pessoais comuns ou sensíveis, como CPF, RG ou atestados médicos, por exemplo;
- Armazenar arquivos digitalizados em pastas seguras da rede institucional;
- Excluir cópias temporárias ou arquivos que ficam na pasta padrão do scanner;
- Após o escaneamento, se for necessário o descarte do documento físico, utilizar meio seguro (fragmentadora).

(Crédito Imagem: Pixabay – Claudio Henrique)

(Crédito Imagem: Pixabay – Geralt)

BOAS PRÁTICAS AO ACESSAR O CORREIO ELETRÔNICO

- Acessar o webmail digitando a URL diretamente no navegador e, ao enviar dados pessoais, utilizar os meios institucionais de comunicação;

- Evitar acessar o e-mail corporativo em computadores de terceiros e, em caso de necessidade, utilizar o modo de navegação anônima para proteger os dados;

- Identificar e-mails suspeitos de spam, golpe ou solicitação de dados pessoais, promoções e sorteios falsos, não respondê-los e encaminhar para o endereço www.denunciespam@fazenda.ms.gov.br;

- Consultar o Catálogo de Fraudes da Rede Nacional de Pesquisa (https://catalogodefraudes.rnp.br/) ao suspeitar de alguma mensagem, para identificar os principais golpes em circulação na internet;

- Verificar cuidadosamente o endereço antes de clicar em links recebidos, evitar abrir links suspeitos e preferir acessar sites oficiais diretamente pelo navegador;

- Abster-se de abrir arquivos de fontes não confiáveis, mesmo após o uso de antivírus, especialmente os executáveis ou compactados, pois podem conter ameaças disfarçadas;

- Evitar o armazenamento de e-mails contendo dados pessoais por tempo indeterminado, promovendo a exclusão periódica de mensagens desnecessárias.

BOAS PRÁTICAS NO TRATAMENTO DE DADOS PESSOAIS NO SISTEMA e-MS

- Ao criar processos no Sistema Eletrônico de Processo Administrativo e-MS, definir o nível de acesso, tornando-o restrito em casos de tratamento de dados pessoais comuns ou sensíveis, conforme o art. 31 da Lei Federal nº 12.527/2011 e art. 3º, IV, da Lei Estadual nº 4.416/2013, ambas referentes à Lei de Acesso à Informação;

- Gerar documentos públicos no Sistema e-MS com o mínimo de dados pessoais e, sempre que possível, descaracterizar informações como o CPF para evitar exposições indevidas, salvo quando houver previsão legal para sua divulgação;

- Em caso de exigência para disponibilizar processos ou documentos a usuários externos, verificar previamente se é necessária a anonimização de dados pessoais.

BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

Controladoria-Geral do Estado de Mato Grosso do Sul

- Aplicar a Política de Segurança da Informação, visando limitar riscos e assegurar a confidencialidade, integridade e disponibilidade dos dados;
- Limitar a coleta e o uso de informações ao estritamente necessário, especificar a finalidade e aplicar medidas técnicas, restringindo o acesso a dados sensíveis somente a usuários essenciais;
- Implementar Controle de Acesso Lógico, permitindo que apenas usuários habilitados utilizem o sistema, com o propósito de mitigar riscos de acesso não autorizado;
- Revisar os acessos aos sistemas sempre que um servidor for exonerado, aposentado ou remanejado para outra área ou unidade;
- Obter a assinatura de Termo de Confidencialidade, Responsabilidade e Sigilo de todos os servidores, especialmente de estagiários e trainees, bem como de terceirizados que atuem em suporte e manutenção de TI;
- Não realizar downloads de softwares sem o conhecimento da Assessoria de Tecnologia da Informação;
- Salvar os arquivos no servidor S134 ou, quando necessário, na estação de trabalho local, conforme as diretrizes institucionais.

(Crédito Imagem: Pixabay – The digital artist)

BOAS PRÁTICAS EM GOVERNANÇA DE DADOS E COMPLIANCE

(Crédito Imagem: Pixabay – Geralt)

- Mapear todos os dados pessoais tratados, registrar no Inventário de Dados Pessoais, avaliar e mitigar os riscos e impactos à privacidade, quando aplicável (RIPD);

- Promover a capacitação de servidores e colaboradores por meio de treinamentos e ações de conscientização.

(Crédito Imagem: Pixabay – Jarmoluk)

BOAS PRÁTICAS NA UTILIZAÇÃO DE DOCUMENTOS FÍSICOS

- Realizar o Controle de Acesso Físico a documentos com dados pessoais, armazenando-os em locais seguros, como armários trancados, e utilizando barreiras físicas (chaves, fechaduras, etc.), quando necessário;

- Avaliar a real necessidade de manter documentos físicos com dados pessoais, eliminando os desnecessários e protegendo os essenciais em ambientes compartilhados;

- Mapear fluxos de trabalho que envolvam dados pessoais em meios físicos, definindo procedimentos seguros e lembrando que arquivos físicos também estão sujeitos à LGPD.

BOAS PRÁTICAS NO USO COMPARTILHADO DE DADOS

- Abster-se de compartilhar arquivos com dados pessoais a terceiros alheios às atividades da CGE/MS, sem autorização prévia;

- Formalizar o compartilhamento de dados pessoais, definindo claramente a finalidade, base legal, prazo do tratamento, medidas de segurança, regras de transparência e responsabilidades entre as partes, segundo as normas do Guia Orientativo de Tratamento de Dados Pessoais pelo Poder Público, da ANPD (Autoridade Nacional de Proteção de Dados Pessoais.

BOAS PRÁTICAS NO DESCARTE DE PAPÉIS E MÍDIAS

- Descartar documentos físicos, com segurança, utilizando fragmentadoras ou trituradores;
- Realizar a exclusão de mídias como HDs, pen drives, CDs ou DVDs utilizando softwares de eliminação segura de dados ou danificando-as fisicamente antes do descarte, de forma a assegurar que os dados não possam ser recuperados por terceiros;
- Reutilizar a mídia somente apenas após a formatação segura, garantindo que não haja vestígios de dados anteriores, caso não seja realizada a destruição física;
- Promover gestão documental, conforme orientações da Comissão Setorial de Avaliação de Documentos de Arquivo da CGE/MS – CADA, responsável pela elaboração e atualização da Tabela de Temporalidade de Documentos, evitando manter dados pessoais além do prazo legal previsto.

BOAS PRÁTICAS NAS ROTINAS DE TRABALHO

(Crédito Imagem: Pixabay – RosZie)

- Consultar o Encarregado pelo Tratamento de Dados Pessoais em todas as questões relacionadas à proteção de dados pessoais;

- Evitar a publicação ou divulgação externa de documentos que contenham dados pessoais, como o CPF, salvo nos casos em que houver obrigação legal ou regulatória, ou quando necessários à execução de políticas públicas previstas em leis e regulamentos. Nessas hipóteses, deve-se preservar essas informações por meio de anonimização, pseudonimização ou outras medidas adequadas antes de qualquer compartilhamento;

- Proteger dados pessoais e informações sensíveis quando os documentos ficarem temporariamente sobre a mesa, virando o anverso das folhas para baixo, por exemplo;

- Realizar revisão periódica dos arquivos digitais para eliminar documentos digitalizados que contenham dados pessoais de manifestantes, fornecedores ou colaboradores;

- Não utilizar aplicativos de mensagens, seja por números corporativos ou pessoais, para tramitação de arquivos que contenham dados pessoais;

- Abster-se de imprimir documentos de caráter pessoal em equipamentos institucionais, como impressoras do ambiente de trabalho.

BOAS PRÁTICAS NO TELETRABALHO

(Crédito Imagem: Pixaby – Aleksandr Pridvanyi)

- Utilizar o e-mail corporativo exclusivamente para tratar de assuntos de trabalho, evitando o uso de contas pessoais;

- Salvar os documentos de trabalho exclusivamente no servidor S134, conforme as diretrizes de segurança da informação;

- Desconectar-se de sistemas e plataformas ao finalizar o expediente, reduzindo riscos de acesso não autorizado.

CGE
Controladoria-Geral do Estado de Mato Grosso do Sul

BOAS PRÁTICAS NA UTILIZAÇÃO DE CELULAR INSTITUCIONAL

- Abster-se de utilizar o celular institucional para fins pessoais, incluindo a instalação de aplicativos pessoais e o armazenamento de fotos particulares;
- Aguardar autorização prévia antes de responder a mensagens SMS que solicitem dados ou informações relacionadas ao trabalho;
- Não conectar o aparelho a redes Wi-Fi públicas ou não seguras durante o exercício das atividades profissionais;
- Não compartilhar o aparelho com terceiros, mesmo que familiares ou colegas.

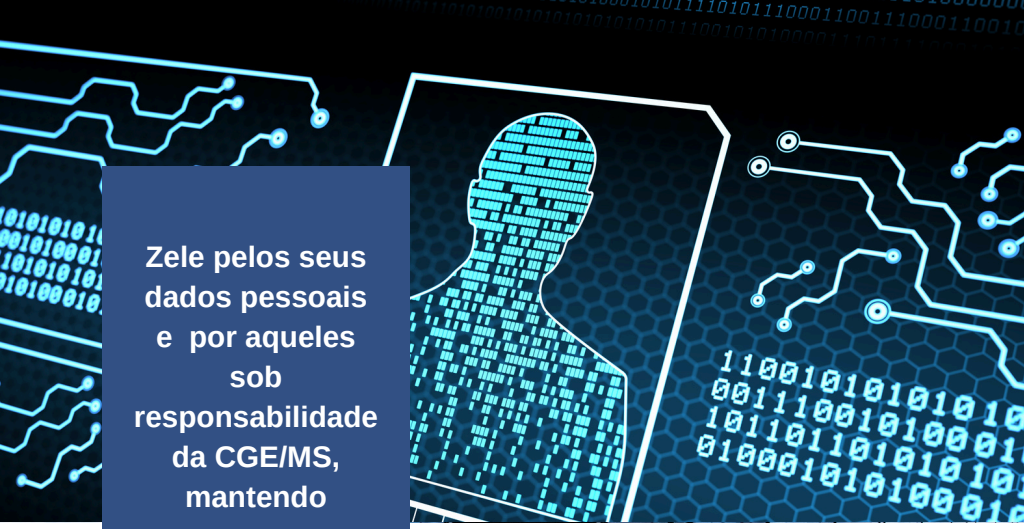
BOAS PRÁTICAS NA APLICAÇÃO DA INTELIGÊNCIA ARTIFICIAL

- Seguir as normas da LGPD e assegurar conformidade com a Política de Segurança da Informação, ao acessar ferramentas de inteligência artificial no ambiente de trabalho;
- Abster-se de inserir dados pessoais, tais como nome completo, CPF, RG, endereço e telefone, bem como dados de terceiros (colegas, familiares, manifestantes, beneficiários de políticas públicas, etc), ao interagir com tecnologias baseadas em inteligência artificial, sem observar as recomendações de segurança e boas práticas definidas pela Assessoria de Tecnologia da Informação – ASTI;
- Não inserir dados financeiros (contas bancárias, senhas), informações médicas, de saúde, ou qualquer dado confidencial, ao utilizar plataformas digitais automatizadas, visto a necessidade de preservar a privacidade dos dados pessoais sensíveis, sem observar as recomendações de segurança e boas práticas definidas pela Assessoria de Tecnologia da Informação – ASTI;
- Evitar o uso de soluções de Inteligência Artificial em versões gratuitas, a fim de prevenir o compartilhamento de dados que possam ser utilizados para o treinamento dos algoritmos.
- Verificar o conteúdo com atenção antes do envio, eliminando ou anonimizando quaisquer dados que possam ser classificados como pessoais.

CGE

Controladoria-Geral do Estado
de Mato Grosso do Sul

PROTEJA SEUS DADOS PESSOAIS



Zele pelos seus dados pessoais e por aqueles sob responsabilidade da CGE/MS, mantendo sempre o controle e contribuindo ativamente na proteção dessas informações!

Seus dados pessoais são valiosos e podem ser utilizados de forma indevida por terceiros mal-intencionados. Além de seguir as recomendações que listamos neste Guia nas suas atividades de trabalho, é essencial tomar cuidados simples ao navegar na internet ou preencher formulários online, com o objetivo de preservar sua privacidade e segurança.

Sempre é bom restringir a exposição de informações pessoais em redes sociais, desconfiar de ofertas excessivamente vantajosas e jamais cadastrar seu e-mail institucional em sites de venda ou similares.

O CPF é um dos principais documentos de identificação do cidadão e, por isso, é muito suscetível a fraude e golpes.

Para verificar se o seu CPF está sendo indevidamente utilizado, é possível consultar serviços fornecidos por órgãos oficiais:

No endereço eletrônico do Banco Central (www.bcb.gov.br/meubc/registrato), é possível verificar a existência de contas bancárias, empréstimos e demais serviços registrados em seu nome;
·Acessando a Redesim, do Governo Federal (https://consultacnpj.redesim.gov.br/minhas-empresas), na opção “Meu CNPJ -Minhas Empresas”, podem ser consultados os CNPJs vinculados ao seu CPF e a situação cadastral das respectivas empresas.

CGE
Controladoria-Geral do Estado de Mato Grosso do Sul