



CÂMARA MUNICIPAL DE CUIABÁ

CANAIS E DISPOSITIVOS COM SEGURANÇA

Orientação para WhatsApp, e-mail e equipamentos pessoais

Boas práticas para o cotidiano parlamentar

Curso: LGPD na prática parlamentar
Data: 5 de agosto de 2026 | 9h às 12h
Edição: 2026



Portal LGPD

Material educativo institucional. A aplicação concreta deve considerar a legislação vigente, as normas internas e a orientação do Encarregado.

1. Princípios de uso

- Preferência institucional: utilize contas, equipamentos, sistemas e armazenamento fornecidos ou aprovados pela Câmara.
- Mínimo necessário: envie apenas o dado indispensável e apenas a quem precisa atuar.
- Temporalidade: aplicativo de mensagem não deve ser o único arquivo de uma atividade institucional.
- Rastreabilidade: preserve registros necessários em sistema ou processo oficial.
- Segurança proporcional: dados sensíveis, documentos de identificação e informações de vulnerabilidade exigem canal mais protegido.
- Separação de finalidades: não misture atendimento institucional com uso pessoal, partidário ou eleitoral.

2. WhatsApp e aplicativos de mensagem

Antes de enviar

- ☐ Confirme identidade e número do destinatário.
- ☐ Pergunte se o documento completo é necessário ou se bastam dados mínimos.
- ☐ Evite grupos; prefira conversa direta com o responsável.
- ☐ Remova informações que não sejam necessárias para o encaminhamento.
- ☐ Considere e-mail institucional, protocolo ou sistema quando houver documento formal.

Configurações recomendadas

- ☐ Ative autenticação em dois fatores e PIN do aplicativo.
- ☐ Use bloqueio forte e biometria do aparelho, sem compartilhar credenciais.
- ☐ Desative prévia de conteúdo sensível na tela bloqueada.
- ☐ Revise dispositivos conectados ao WhatsApp Web e encerre sessões desconhecidas.
- ☐ Revise backups automáticos e evite cópia de documentos institucionais em nuvem pessoal.
- ☐ Mantenha sistema e aplicativo atualizados.

Durante e depois

- ☐ Não encaminhe para grupos amplos “só para localizar quem resolve”.
- ☐ Não exponha números de cidadãos em grupos ou listas abertas.
- ☐ Transfira o registro necessário ao ambiente institucional.
- ☐ Elimine cópias locais conforme a política e os prazos aplicáveis; não destrua evidência de incidente.
- ☐ Em envio incorreto, tente conter e comunique imediatamente.

3. E-mail

- ☐ Use o endereço institucional para assuntos da Câmara.
- ☐ Confira destinatário, domínio e preenchimento automático.
- ☐ Abra e revise o anexo correto antes de enviar.
- ☐ Use CCO quando destinatários de comunicação coletiva não precisarem conhecer os demais contatos.
- ☐ Não encaminhe cadeias antigas sem revisar dados e anexos anteriores.
- ☐ Evite colocar dado sensível no assunto do e-mail, que pode aparecer em notificações.
- ☐ Para arquivo protegido, envie a senha por canal diferente e não use senha óbvia.
- ☐ Desconfie de urgência, alteração de conta, pedido de senha ou link inesperado; confirme por canal conhecido.
- ☐ Não use e-mail pessoal como arquivo paralelo ou para contornar limite de sistema.

Exemplo de assunto seguro

Em vez de “LAUDO DE HIV - João da Silva”, use “Documentação para análise - atendimento nº 2026/...” e restrinja o conteúdo a quem precisa atuar.

4. Dispositivos pessoais**Regra geral**

O uso de aparelho pessoal para atividade institucional deve ser excepcional e obedecer às normas e orientações internas. Conveniência não elimina responsabilidade.

- ☐ Ative criptografia, bloqueio automático, localização e apagamento remoto quando disponíveis.
- ☐ Mantenha cópia de segurança pessoal separada de documentos institucionais.
- ☐ Não permita uso do aparelho por terceiros com contas de trabalho abertas.
- ☐ Não instale aplicativos de origem duvidosa ou que peçam permissões excessivas.
- ☐ Evite redes Wi-Fi públicas para acessar sistemas ou documentos sensíveis; use conexão confiável e recursos institucionais.
- ☐ Não salve senha em notas, mensagens ou fotos.
- ☐ Antes de vender, doar ou enviar para assistência, faça backup autorizado, remova contas e apague dados com segurança.
- ☐ Comunique perda, roubo ou acesso suspeito quando houver conteúdo ou credenciais institucionais.

5. Computador, tela e impressão

- ☐ Bloqueie a tela ao se afastar.
- ☐ Não compartilhe usuário ou senha.
- ☐ Evite salvar documentos em Área de Trabalho compartilhada ou pasta pública.
- ☐ Recolha imediatamente impressões e não reutilize rascunhos com dados pessoais.
- ☐ Guarde documentos físicos em local controlado e use descarte seguro.
- ☐ Não conecte pen drive desconhecido ou pessoal sem autorização.
- ☐ Revise permissões de pastas e links periodicamente.

6. Reuniões on-line, áudio e gravações

- ☐ Informe gravação e finalidade quando houver.
- ☐ Evite exibir notificações, e-mails ou documentos durante compartilhamento de tela.
- ☐ Compartilhe apenas a janela necessária, não a área de trabalho inteira.
- ☐ Controle participantes e links; não publique gravações sem análise da finalidade e do conteúdo.
- ☐ Revise transcrições automáticas, que também podem conter dados pessoais.

7. Resposta rápida a erros

1. Interrompa o compartilhamento ou revogue o link, se possível.
2. Não apague evidências relevantes.
3. Registre o que ocorreu, quando e com quais dados.
4. Comunique imediatamente à chefia e ao Encarregado.
5. Siga as orientações de Tecnologia e das áreas responsáveis.

ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS

Hermes Teseu Bispo Freire Júnior

lgpd@camaracuiaba.mt.gov.br | (65) 3617-1527

Portal: <https://www.camaracuiaba.mt.gov.br/lgpd>



Canal LGPD