



Câmara Municipal de Bodoquena

Mato Grosso do Sul
GABINETE DA PRESIDENCIA

Protocolo nº	RESOLUÇÃO 007/2026	APROVADO ☐
Recebido/...../.....		REJEITADO ☐
Protocolista		Carimbo da Presidência
AUTOR: Presidência da Câmara		

“Institui a Política de Segurança da Informação - PSI da Câmara Municipal de Bodoquena/MS e estabelece diretrizes para governança, classificação, tratamento, acesso, compartilhamento, proteção, continuidade e resposta a incidentes de segurança da informação”.

O Presidente da Câmara Municipal de Bodoquena, Estado de Mato Grosso do Sul, Vereador Ayrton Ferreira Marques, no uso de suas atribuições que lhe confere a Lei Orgânica Municipal e o Regimento Interno dessa Casa de Leis, faz saber que o soberano Plenário aprovou e ele sanciona e promulga a presente Resolução:

CONSIDERANDO a necessidade de assegurar a confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade e proteção das informações produzidas, recebidas, armazenadas, transmitidas ou custodiadas pela Câmara Municipal;

CONSIDERANDO a Lei Federal nº 12.527/2011 - Lei de Acesso à Informação, especialmente a necessidade de proteger informações pessoais e informações submetidas a restrição de acesso, sem prejuízo da transparência pública;

CONSIDERANDO a Lei Federal nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais - LGPD, especialmente os deveres de segurança e prevenção aplicáveis ao tratamento de dados pessoais;

CONSIDERANDO a Resolução nº 005/2026 da Câmara Municipal de Bodoquena/MS, que institui a Política Institucional de Governança em Proteção de Dados Pessoais e expressamente prevê a adoção de Política de Segurança da Informação de caráter geral;

CONSIDERANDO a Portaria nº 068/2026, que aprova o Aviso de Privacidade Institucional da Câmara Municipal de Bodoquena/MS;



Câmara Municipal de Bodoquena

Mato Grosso do Sul
GABINETE DA PRESIDENCIA

RESOLVE:

CAPÍTULO I DAS DISPOSIÇÕES GERAIS

Art. 1º. Fica instituída a Política de Segurança da Informação - PSI da Câmara Municipal de Bodoquena/MS, como instrumento geral de governança destinado à proteção das informações institucionais, independentemente do meio físico ou digital em que se encontrem.

Art. 2º. São objetivos da PSI:

- I - proteger as informações contra acesso, uso, divulgação, alteração, destruição, perda ou indisponibilidade não autorizados;
- II - preservar a confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade das informações;
- III - estabelecer critérios proporcionais ao risco para acesso, tratamento, armazenamento, compartilhamento, transmissão, retenção e descarte;
- IV - assegurar a continuidade das atividades legislativas e administrativas;
- V - reduzir os riscos identificados no ROPA, nas matrizes de risco e em avaliações posteriores;
- VI - integrar segurança da informação, proteção de dados pessoais, transparência, gestão documental, gestão de contratos e continuidade de serviços; e
- VII - promover cultura institucional de prevenção e responsabilidade no uso da informação.

Art. 3º. Esta Política aplica-se aos vereadores, servidores efetivos e comissionados, estagiários, colaboradores, prestadores de serviços, fornecedores, operadores, assessorias e demais pessoas que utilizem recursos tecnológicos ou tenham acesso a informações, documentos, sistemas, ambientes ou ativos da Câmara.

Art. 4º. A aplicação desta PSI observará, de forma integrada, a Resolução nº 005/2026 de Governança em Proteção de Dados Pessoais, o Aviso de Privacidade Institucional.

Parágrafo único. Em caso de informação que contenha dado pessoal, além da classificação de segurança prevista nesta PSI, deverão ser observadas as regras específicas da LGPD.

CAPÍTULO II DOS PRINCÍPIOS E DA GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO



Câmara Municipal de Bodoquena

Mato Grosso do Sul
GABINETE DA PRESIDENCIA

Art. 5º. A segurança da informação observará os princípios da legalidade, finalidade, necessidade, proporcionalidade, prevenção, menor privilégio, segregação de funções, necessidade de conhecer, rastreabilidade, continuidade, responsabilidade e gestão baseada em risco.

Art. 6º. A governança da segurança da informação será exercida de forma proporcional à estrutura da Câmara, com participação da Presidência, Administração, Tecnologia da Informação, unidades responsáveis pelos ativos e, quando houver dados pessoais, do Encarregado pelo Tratamento de Dados Pessoais.

Art. 7º. Compete à unidade ou responsável por Tecnologia da Informação, no âmbito de suas atribuições:

- I - administrar usuários, credenciais, perfis e privilégios de acesso;
- II - manter inventário mínimo dos ativos tecnológicos críticos;
- III - implementar e acompanhar rotinas de backup, restauração, atualização, proteção e continuidade;
- IV - registrar, quando tecnicamente viável, eventos, acessos privilegiados e intervenções remotas;
- V - apoiar a gestão de incidentes de segurança;
- VI - orientar sobre aquisição, contratação, implantação e descarte seguro de recursos tecnológicos; e
- VII - apoiar avaliações de risco de novos sistemas, serviços em nuvem, ferramentas de inteligência artificial e integrações.

Art. 8º. O Encarregado pelo Tratamento de Dados Pessoais atuará, quando o evento, processo ou medida de segurança envolver dados pessoais, nas atribuições de orientação previstas na LGPD e na Resolução nº 005/2026, sem assumir funções operacionais incompatíveis com sua autonomia.

CAPÍTULO III

DA CLASSIFICAÇÃO E DO TRATAMENTO DA INFORMAÇÃO

Art. 9º. Para fins operacionais de segurança, as informações serão classificadas conforme sua necessidade de proteção, sem prejuízo das hipóteses e procedimentos formais de restrição de acesso previstos na Lei de Acesso à Informação.

Art. 10. Adotam-se as seguintes categorias de tratamento:



Câmara Municipal de Bodoquena

Mato Grosso do Sul
GABINETE DA PRESIDENCIA

I - Pública: informação destinada à divulgação ou cujo acesso seja franqueado por lei, como atos legislativos, leis, projetos, atas e informações de transparência, ressalvados dados que devam ser protegidos ou minimizados;

II - Uso Interno: informação necessária às atividades da Câmara, cujo acesso deve se limitar às pessoas e unidades envolvidas no processo, embora não possua sigilo legal específico;

III - Restrita: informação cujo acesso indevido possa causar prejuízo a pessoas, à Câmara ou à continuidade dos serviços, incluindo dados pessoais, dados bancários, credenciais, documentos funcionais, informações contratuais não públicas e documentos administrativos em elaboração;

IV - Restrita Sensível: informação que demande controles reforçados, incluindo dados pessoais sensíveis, documentos de saúde, senhas e chaves de autenticação, registros de segurança, configurações críticas, cópias de segurança e informações protegidas por sigilo legal.

§ 1º. A classificação deverá considerar o conteúdo, a finalidade, o contexto, o impacto de eventual divulgação indevida e a necessidade de acesso.

§ 2º. A classificação operacional desta PSI não transforma informação pública em sigilosa nem substitui os procedimentos legais de classificação de sigilo previstos na LAI.

Art. 11. A informação deverá receber proteção compatível com sua classificação durante todo o ciclo de vida: criação ou recebimento, uso, armazenamento, compartilhamento, arquivamento, retenção e descarte.

Art. 12. Documentos físicos classificados como restritos ou restritos sensíveis deverão ser mantidos, sempre que possível, em armários, arquivos ou ambientes com controle de acesso compatível com o risco.

Art. 13. Documentos digitais classificados como restritos ou restritos sensíveis deverão permanecer em sistemas, pastas, contas ou ambientes institucionais com controle de acesso, evitando-se cópias desnecessárias e armazenamento disperso.

CAPÍTULO IV DO CONTROLE DE ACESSO E DA AUTENTICAÇÃO

Art. 14. O acesso a sistemas, pastas, documentos e ambientes será concedido segundo os princípios do menor privilégio e da necessidade de conhecer, limitado ao necessário ao desempenho das atribuições do usuário.



Câmara Municipal de Bodoquena

Mato Grosso do Sul
GABINETE DA PRESIDENCIA

Art. 15. A concessão, alteração e revogação de acessos deverá observar procedimento institucional que contemple ingresso, mudança de função, afastamento, substituição e desligamento.

Art. 16. É vedado o compartilhamento de senhas, credenciais, certificados digitais, tokens ou mecanismos individuais de autenticação.

Art. 17. As contas deverão ser individualizadas sempre que o sistema permitir, e os perfis de acesso deverão ser revistos periodicamente, com prioridade para sistemas críticos e acessos privilegiados.

Art. 18. A Câmara adotará requisitos mínimos de senha definidos em procedimento técnico, considerando comprimento, complexidade, bloqueio contra tentativas indevidas e proteção contra reutilização ou exposição.

Parágrafo único. A alteração de senha será exigida imediatamente em caso de suspeita de comprometimento e poderá ser estabelecida periodicamente quando tecnicamente recomendável para o sistema ou risco envolvido.

Art. 19. A autenticação multifator - MFA será priorizada para e-mail institucional, redes sociais, contas administrativas, acessos remotos e sistemas críticos, sempre que tecnicamente disponível.

Art. 20. Acessos administrativos ou privilegiados deverão ser limitados às pessoas formalmente autorizadas e, quando tecnicamente possível, registrados e auditáveis.

CAPÍTULO V DO USO ACEITÁVEL DOS RECURSOS TECNOLÓGICOS

Art. 21. Os recursos tecnológicos da Câmara destinam-se prioritariamente às atividades institucionais e deverão ser utilizados de forma responsável, segura e compatível com a legislação e com esta Política.

Art. 22. É vedado, salvo autorização institucional e justificativa técnica:

- I - instalar ou utilizar software não licenciado, não homologado ou de origem desconhecida;
- II - desabilitar mecanismos de proteção, antivírus, atualizações, bloqueios ou controles de segurança;
- III - acessar conteúdo ou sítios sabidamente maliciosos ou incompatíveis com a atividade institucional;



Câmara Municipal de Bodoquena

Mato Grosso do Sul
GABINETE DA PRESIDENCIA

IV - armazenar documentos ou dados institucionais em contas pessoais de e-mail, nuvens pessoais ou serviços não homologados;

V - compartilhar credenciais ou permitir o uso de conta institucional por terceiro não autorizado;

VI - conectar dispositivos ou mídias externas de origem desconhecida quando houver risco à rede ou aos dados; e

VII - inserir informações restritas ou dados pessoais em ferramentas públicas de inteligência artificial sem avaliação prévia e autorização institucional.

Art. 23. O uso de e-mail institucional deverá observar cautela com links, anexos, remetentes desconhecidos, solicitações urgentes de credenciais ou pagamentos e demais sinais de phishing ou engenharia social.

Art. 24. O uso de dispositivos móveis e aplicativos de mensagens para atividades institucionais deverá priorizar equipamentos, contas e canais institucionais.

§ 1º. O uso excepcional de dispositivo ou canal pessoal não autoriza armazenamento permanente de informação institucional e deverá observar as salvaguardas definidas pela Câmara.

§ 2º. Documentos oficiais, documentos com dados pessoais, informações financeiras, documentos de licitação, atestados e informações restritas não deverão ser encaminhados por WhatsApp pessoal quando houver canal institucional adequado.

Art. 25. Impressoras e documentos impressos deverão ser utilizados de modo a evitar abandono de documentos restritos em bandejas, mesas, salas compartilhadas ou locais de livre circulação.

CAPÍTULO VI

DO COMPARTILHAMENTO INTERNO E EXTERNO

Art. 26. O compartilhamento interno de informações deverá ocorrer apenas entre pessoas e unidades que necessitem dos dados para executar suas atribuições, observando finalidade, minimização, classificação e canal adequado.

Art. 27. Os fluxos internos de maior risco ou recorrência deverão ser formalizados, especialmente aqueles envolvendo RH e Financeiro, Secretaria, Contabilidade, Licitações, Compras, Gabinete, Controladoria, Frota, Recepção e demais unidades identificadas no ROPA.

Art. 28. O compartilhamento externo deverá:



Câmara Municipal de Bodoquena

Mato Grosso do Sul
GABINETE DA PRESIDENCIA

- I - possuir finalidade institucional e fundamento legal ou contratual adequado;
- II - limitar-se às informações necessárias à finalidade;
- III - utilizar canal compatível com a classificação da informação;
- IV - ser dirigido ao destinatário correto, com conferência prévia de endereço eletrônico, conta, sistema ou identificação;
- V - observar, quando aplicável, os registros e deveres de transparência previstos na Política de Governança em Proteção de Dados; e
- VI - preservar evidência ou rastreabilidade quando a natureza do processo exigir.

Art. 29. O envio de informações restritas ou restritas sensíveis por e-mail deverá utilizar conta institucional e, quando o risco justificar, medidas adicionais de proteção, como arquivo protegido, limitação de acesso ou outro mecanismo tecnicamente disponível.

Art. 30. A publicação em Portal da Transparência, Diário Oficial, site, redes sociais, atas, transmissões e outros meios públicos deverá observar a legislação de transparência e, simultaneamente, a minimização de dados pessoais prevista na Resolução nº 005/2026 e no Aviso de Privacidade.

Art. 31. Compartilhamentos com Tribunal de Contas, Receita Federal, e Social, INSS, BodoPrev, Ministério Público, instituições financeiras, Prefeitura e demais órgãos públicos deverão utilizar, preferencialmente, sistemas oficiais ou canais institucionais próprios.

CAPÍTULO VII

DA SEGURANÇA DE SISTEMAS, REDES, BACKUPS E ACESSOS REMOTOS

Art. 32 Os sistemas e equipamentos deverão ser mantidos atualizados e protegidos de acordo com sua criticidade e capacidade técnica, com mecanismos de prevenção contra códigos maliciosos, acessos indevidos e perda de informação.

Art. 33. A Câmara manterá rotinas de backup compatíveis com a criticidade dos serviços, contemplando, progressivamente:

- I - definição dos dados e sistemas abrangidos;
- II - frequência de execução;
- III - responsabilidade pela rotina;
- IV - controle de acesso às cópias;



Câmara Municipal de Bodoquena

Mato Grosso do Sul
GABINETE DA PRESIDENCIA

V - prazo ou critério de retenção;

VI - proteção contra alteração ou exclusão indevida; e

VII - testes periódicos de restauração.

Art. 34. Os acessos remotos de empresas de sistemas, assessorias e suporte técnico deverão ser limitados ao necessário, preferencialmente autorizados, temporários e registráveis, observando as regras contratuais e de proteção de dados.

Art. 35. A contratação ou utilização de serviço em nuvem dependerá de avaliação prévia quanto à finalidade, segurança, controle de acesso, backup, disponibilidade, retenção, localização ou transferência de dados, encerramento do serviço e responsabilidades do fornecedor.

Art. 36. A utilização de ferramentas de inteligência artificial em atividades institucionais deverá observar ato ou orientação específica, sendo vedada a inserção de informação restrita, restrita sensível ou dado pessoal em ferramenta não previamente avaliada para essa finalidade.

CAPÍTULO VIII

DA SEGURANÇA FÍSICA, AMBIENTAL E DO DESCARTE

Art. 37. Ambientes que abriguem servidores, equipamentos de rede, backups, arquivos documentais ou outros ativos críticos deverão possuir acesso limitado às pessoas autorizadas.

Art. 38. A Câmara adotará, conforme avaliação técnica e disponibilidade estrutural, medidas de proteção ambiental e continuidade, incluindo proteção contra incêndio, falhas elétricas, calor, umidade e outras condições capazes de comprometer equipamentos e documentos.

Art. 39. Documentos em papel contendo informação restrita ou restrita sensível deverão ser descartados por fragmentação, trituração ou método equivalente que impeça sua reconstrução.

Art. 40. Mídias, computadores, celulares, discos e demais dispositivos deverão ter seus dados eliminados de forma segura antes de descarte, devolução, transferência, alienação ou reutilização, quando tecnicamente aplicável.



Câmara Municipal de Bodoquena

Mato Grosso do Sul
GABINETE DA PRESIDENCIA

Art. 41. O Patrimônio e a Tecnologia da Informação deverão manter fluxo coordenado para a baixa e destinação de equipamentos que possam conter dados institucionais.

CAPÍTULO IX DA GESTÃO DE INCIDENTES DE SEGURANÇA

Art. 42. Todo usuário deverá comunicar imediatamente qualquer suspeita ou ocorrência de incidente de segurança ao responsável pela Tecnologia da Informação ou responsável técnico de TI formalmente designado pela Câmara e, quando o evento envolver ou puder envolver dados pessoais, também ao Encarregado pelo Tratamento de Dados Pessoais. A comunicação deverá ocorrer mesmo quando ainda não houver confirmação de vazamento, dano ou acesso indevido.

Art. 43. A gestão dos incidentes de segurança será coordenada operacionalmente pelo responsável pela Tecnologia da Informação ou responsável técnico de TI formalmente designado, com participação do Encarregado sempre que houver dados pessoais envolvidos, e apoio da Administração, da unidade responsável pelo processo, do Jurídico e da Presidência, conforme a natureza e a gravidade do evento. O Plano de Resposta a Incidentes de Segurança deverá contemplar, no mínimo:

- I - canal institucional para recebimento do relato, triagem inicial e registro do incidente pelo responsável pela TI;
- II- classificação do incidente quanto à natureza, criticidade, ativos, sistemas, documentos, serviços e informações afetados;
- III- adoção, pela TI ou por quem detenha competência técnica, das medidas de contenção, isolamento, bloqueio, preservação de evidências e prevenção de agravamento;
- IV - avaliação do impacto, da extensão e da causa provável do incidente, com participação da unidade responsável pelo processo afetado;
- V - medidas de erradicação, recuperação, restauração e continuidade dos serviços, inclusive acionamento de backups quando necessário;
- VI - comunicação interna e escalonamento à Administração e à Presidência nos incidentes relevantes, críticos ou que possam comprometer a continuidade institucional;
- VII - avaliação, pelo Encarregado, quando houver dados pessoais, da natureza e das categorias de dados afetados, dos riscos aos titulares, das medidas de mitigação e das providências previstas na legislação de proteção de dados;
- VIII - avaliação conjunta, quando cabível, das comunicações legalmente exigidas à Autoridade Nacional de Proteção de Dados - ANPD, aos titulares, às autoridades competentes, aos fornecedores ou a terceiros envolvidos; e



Câmara Municipal de Bodoquena

Mato Grosso do Sul
GABINETE DA PRESIDENCIA

IX - documentação das providências adotadas, encerramento do incidente, registro de lições aprendidas e definição de medidas corretivas e preventivas.

Art. 44. Para fins deste Capítulo, compete ao responsável pela Tecnologia da Informação ou responsável técnico de TI coordenar as providências técnicas e operacionais de resposta, contenção, preservação de evidências, recuperação e restabelecimento dos serviços. Compete ao Encarregado, quando houver dados pessoais envolvidos, orientar quanto às obrigações da LGPD, avaliar os riscos aos direitos dos titulares, acompanhar o registro do incidente e subsidiar a decisão sobre eventual comunicação à ANPD e aos titulares, preservada sua autonomia e sem lhe atribuir a execução operacional das atividades de TI.

Art. 45. Os incidentes deverão ser registrados em repositório de acesso restrito. Os registros técnicos ficarão sob a guarda da área ou responsável pela TI, e os registros relacionados à proteção de dados pessoais serão acompanhados pelo Encarregado, observados os prazos e critérios de retenção aplicáveis. As informações deverão ser preservadas pelo período necessário à apuração, à prestação de contas, ao cumprimento de obrigações legais ou contratuais e ao aperfeiçoamento dos controles de segurança.

CAPÍTULO X

DA GESTÃO DE FORNECEDORES E CONTRATOS

Art. 46. Contratações que envolvam acesso a sistemas, rede, equipamentos, documentos ou informações institucionais deverão prever requisitos de segurança proporcionais ao risco.

Art. 47. Sem prejuízo das cláusulas de proteção de dados previstas na Resolução nº 005/2026, os instrumentos contratuais deverão contemplar, quando aplicável:

- I - confidencialidade e dever de sigilo;
- II - regras de controle de acesso e credenciais;
- III - procedimentos de suporte e acesso remoto;
- IV - registro de intervenções técnicas;
- V - medidas mínimas de segurança e continuidade;
- VI - backup, recuperação e disponibilidade quando integrantes do serviço;
- VII - comunicação imediata de incidentes;
- VIII - subcontratação e acesso por terceiros;
- IX - devolução, portabilidade, eliminação ou preservação das informações ao término do contrato; e



Câmara Municipal de Bodoquena

Mato Grosso do Sul
GABINETE DA PRESIDENCIA

X - responsabilidades pela segurança das informações e cooperação em auditorias ou apurações

CAPÍTULO XI

DAS RESPONSABILIDADES E CONSEQUÊNCIAS

Art. 48. Todos os abrangidos por esta Política são responsáveis por cumprir as medidas de segurança aplicáveis às atividades que desempenham e por comunicar situações que possam comprometer informações ou ativos da Câmara.

Art. 49. O descumprimento desta Política poderá ensejar apuração de responsabilidade administrativa, civil e penal, conforme a natureza do vínculo, a legislação aplicável, o Estatuto dos Servidores, os contratos, os deveres funcionais e demais normas pertinentes, assegurados o contraditório e a ampla defesa quando cabíveis.

CAPÍTULO XII

DAS DISPOSIÇÕES FINAIS

Art. 50. A Presidência poderá expedir normas, procedimentos e padrões complementares para execução desta PSI, especialmente sobre controle de acessos, senhas, backup, resposta a incidentes, continuidade, uso aceitável, acesso remoto, nuvem, inteligência artificial, classificação da informação e descarte seguro.

Art. 51. Os procedimentos técnicos poderão ser atualizados por ato administrativo próprio, sem necessidade de alteração desta Resolução, desde que preservadas suas diretrizes.

Art. 52. A PSI será revista periodicamente e sempre que houver alteração relevante na estrutura, nos sistemas, nos riscos, na legislação ou nos processos da Câmara.

Art. 53. Os casos omissos serão resolvidos pela Presidência ou Mesa Diretora, conforme suas competências, com apoio técnico da Administração, Tecnologia da Informação, Jurídico e, quando houver dados pessoais, do Encarregado.

Art. 54. Esta Resolução entra em vigor na data de sua publicação.

Câmara Municipal de Bodoquena MS., 14 de outubro de 2.026.



Ayrton Ferreira Marques
Presidente/CMB



Câmara Municipal de Bodoquena

Mato Grosso do Sul
GABINETE DA PRESIDENCIA

ANEXO

MATRIZ INSTITUCIONAL DE CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO

Categoria	Exemplos	Acesso	Compartilhamento	Proteção mínima
Pública	Leis, projetos, atos, atas e informações de transparência, após avaliação de dados protegidos.	Livre, conforme legislação.	Canais oficiais de publicidade.	Integridade, versão oficial e minimização de dados pessoais.
Uso Interno	Rotinas administrativas, documentos de trabalho e comunicações internas sem sigilo específico.	Pessoas/unidades envolvidas.	Canais institucionais.	Controle de acesso compatível e armazenamento institucional.
Restrita	Dados pessoais, dados bancários, documentos funcionais, contratos não públicos, documentos administrativos em elaboração.	Necessidade de conhecer.	Somente destinatários necessários e canal adequado.	Credencial individual, controle físico/digital, minimização e descarte seguro.
Restrita Sensível	Dados de saúde, senhas, chaves, backups, registros de segurança e configurações críticas.	Estritamente necessário.	Excepcional e controlado.	Acesso reforçado, MFA quando disponível, registro de acesso quando possível, guarda restrita e descarte seguro.



Câmara Municipal de Bodoquena

Mato Grosso do Sul
GABINETE DA PRESIDENCIA

Nota: a classificação operacional acima orienta os controles de segurança e não substitui a classificação formal de sigilo prevista na Lei de Acesso à Informação.

Resolução nº007/2026

"Institui a Política de Segurança da Informação - PSI da Câmara Municipal de Bodoquena/MS e estabelece diretrizes para governança, classificação, tratamento, acesso, compartilhamento, proteção, continuidade e resposta a incidentes de segurança da informação".

O Presidente da Câmara Municipal de Bodoquena, Estado de Mato Grosso do Sul, Vereador Ayrton Ferreira Marques, no uso de suas atribuições que lhe confere a Lei Orgânica Municipal e o Regimento Interno dessa Casa de Leis, faz saber que o soberano Plenário aprovou e ele sanciona e promulga a presente Resolução:

CONSIDERANDO a necessidade de assegurar a confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade e proteção das informações produzidas, recebidas, armazenadas, transmitidas ou custodiadas pela Câmara Municipal;

CONSIDERANDO a Lei Federal nº 12.527/2011 - Lei de Acesso à Informação, especialmente a necessidade de proteger informações pessoais e informações submetidas a restrição de acesso, sem prejuízo da transparência pública;

CONSIDERANDO a Lei Federal nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais - LGPD, especialmente os deveres de segurança e prevenção aplicáveis ao tratamento de dados pessoais;

CONSIDERANDO a Resolução nº 005/2026 da Câmara Municipal de Bodoquena/MS, que institui a Política Institucional de Governança em Proteção de Dados Pessoais e expressamente prevê a adoção de Política de Segurança da Informação de caráter geral;

CONSIDERANDO a Portaria nº 068/2026, que aprova o Aviso de Privacidade Institucional da Câmara Municipal de Bodoquena/MS;

RESOLVE:

CAPÍTULO I**DAS DISPOSIÇÕES GERAIS**

Art. 1º. Fica instituída a Política de Segurança da Informação - PSI da Câmara Municipal de Bodoquena/MS, como instrumento geral de governança destinado à proteção das informações institucionais, independentemente do meio físico ou digital em que se encontrem.

Art. 2º. São objetivos da PSI:

I - proteger as informações contra acesso, uso, divulgação, alteração, destruição, perda ou indisponibilidade não autorizados;

II - preservar a confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade das informações;

III - estabelecer critérios proporcionais ao risco para acesso, tratamento, armazenamento, compartilhamento, transmissão, retenção e descarte;

IV - assegurar a continuidade das atividades legislativas e administrativas;

V - reduzir os riscos identificados no ROPA, nas matrizes de risco e em avaliações posteriores;

VI - integrar segurança da informação, proteção de dados pessoais, transparência, gestão documental, gestão de contratos e continuidade de serviços; e

VII - promover cultura institucional de prevenção e responsabilidade no uso da informação.

Art. 3º. Esta Política aplica-se aos vereadores, servidores efetivos e comissionados, estagiários, colaboradores, prestadores de serviços, fornecedores, operadores, assessorias e demais pessoas que utilizem recursos tecnológicos ou tenham acesso a informações, documentos, sistemas, ambientes ou ativos da Câmara.

Art. 4º. A aplicação desta PSI observará, de forma integrada, a Resolução nº 005/2026 de Governança em Proteção de Dados Pessoais, o Aviso de Privacidade Institucional.

Parágrafo único. Em caso de informação que contenha dado pessoal, além da classificação de segurança prevista nesta PSI, deverão ser observadas as regras específicas da LGPD.

CAPÍTULO**DOS PRINCÍPIOS E DA GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO****II**

Art. 5º. A segurança da informação observará os princípios da legalidade, finalidade, necessidade, proporcionalidade, prevenção, menor privilégio, segregação de funções, necessidade de conhecer, rastreabilidade, continuidade, responsabilidade e gestão baseada em risco.

Art. 6º. A governança da segurança da informação será exercida de forma proporcional à estrutura da Câmara, com participação da Presidência, Administração, Tecnologia da Informação, unidades responsáveis pelos ativos e, quando houver dados pessoais, do Encarregado pelo Tratamento de Dados Pessoais.

Art. 7º. Compete à unidade ou responsável por Tecnologia da Informação, no âmbito de suas atribuições:

I - administrar usuários, credenciais, perfis e privilégios de acesso;

II - manter inventário mínimo dos ativos tecnológicos críticos;

III - implementar e acompanhar rotinas de backup, restauração, atualização, proteção e continuidade;

IV - registrar, quando tecnicamente viável, eventos, acessos privilegiados e intervenções remotas;

V - apoiar a gestão de incidentes de segurança;

VI - orientar sobre aquisição, contratação, implantação e descarte seguro de recursos tecnológicos; e

VII - apoiar avaliações de risco de novos sistemas, serviços em nuvem, ferramentas de inteligência artificial e integrações.

Art. 8º. O Encarregado pelo Tratamento de Dados Pessoais atuará, quando o evento, processo ou medida de segurança envolver dados pessoais, nas atribuições de orientação previstas na LGPD e na Resolução nº 005/2026, sem assumir funções operacionais incompatíveis com sua autonomia.

CAPÍTULO III

DA CLASSIFICAÇÃO E DO TRATAMENTO DA INFORMAÇÃO

Art. 9º. Para fins operacionais de segurança, as informações serão classificadas conforme sua necessidade de proteção, sem prejuízo das hipóteses e procedimentos formais de restrição de acesso previstos na Lei de Acesso à Informação.

Art. 10. Adotam-se as seguintes categorias de tratamento:

I - Pública: informação destinada à divulgação ou cujo acesso seja franqueado por lei, como atos legislativos, leis, projetos, atas e informações de transparência, ressalvados dados que devam ser protegidos ou minimizados;

II - Uso Interno: informação necessária às atividades da Câmara, cujo acesso deve se limitar às pessoas e unidades envolvidas no processo, embora não possua sigilo legal específico;

III - Restrita: informação cujo acesso indevido possa causar prejuízo a pessoas, à Câmara ou à continuidade dos serviços, incluindo dados pessoais, dados bancários, credenciais, documentos funcionais, informações contratuais não públicas e documentos administrativos em elaboração;

IV - Restrita Sensível: informação que demande controles reforçados, incluindo dados pessoais sensíveis, documentos de saúde, senhas e chaves de autenticação, registros de segurança, configurações críticas, cópias de segurança e informações protegidas por sigilo legal.

§ 1º. A classificação deverá considerar o conteúdo, a finalidade, o contexto, o impacto de eventual divulgação indevida e a necessidade de acesso.

§ 2º. A classificação operacional desta PSI não transforma informação pública em sigilosa nem substitui os procedimentos legais de classificação de sigilo previstos na LAI.

Art. 11. A informação deverá receber proteção compatível com sua classificação durante todo o ciclo de vida: criação ou recebimento, uso, armazenamento, compartilhamento, arquivamento, retenção e descarte.

Art. 12. Documentos físicos classificados como restritos ou restritos sensíveis deverão ser mantidos, sempre que possível, em armários, arquivos ou ambientes com controle de acesso compatível com o risco.

Art. 13. Documentos digitais classificados como restritos ou restritos sensíveis deverão permanecer em sistemas, pastas, contas ou ambientes institucionais com controle de acesso, evitando-se cópias desnecessárias e armazenamento disperso.

CAPÍTULO IV**DO CONTROLE DE ACESSO E DA AUTENTICAÇÃO**

Art. 14. O acesso a sistemas, pastas, documentos e ambientes será concedido segundo os princípios do menor privilégio e da necessidade de conhecer, limitado ao necessário ao desempenho das atribuições do usuário.

Art. 15. A concessão, alteração e revogação de acessos deverá observar procedimento institucional que contemple ingresso, mudança de função, afastamento, substituição e desligamento.

Art. 16. É vedado o compartilhamento de senhas, credenciais, certificados digitais, tokens ou mecanismos individuais de autenticação.

Art. 17. As contas deverão ser individualizadas sempre que o sistema permitir, e os perfis de acesso deverão ser revistos periodicamente, com prioridade para sistemas críticos e acessos privilegiados.

Art. 18. A Câmara adotará requisitos mínimos de senha definidos em procedimento técnico, considerando comprimento, complexidade, bloqueio contra tentativas indevidas e proteção contra reutilização ou exposição.

Parágrafo único. A alteração de senha será exigida imediatamente em caso de suspeita de comprometimento e poderá ser estabelecida periodicamente quando tecnicamente recomendável para o sistema ou risco envolvido.

Art. 19. A autenticação multifator - MFA será priorizada para e-mail institucional, redes sociais, contas administrativas, acessos remotos e sistemas críticos, sempre que tecnicamente disponível.

Art. 20. Acessos administrativos ou privilegiados deverão ser limitados às pessoas formalmente autorizadas e, quando tecnicamente possível, registrados e auditáveis.

CAPÍTULO V**DO USO ACEITÁVEL DOS RECURSOS TECNOLÓGICOS**

Art. 21. Os recursos tecnológicos da Câmara destinam-se prioritariamente às atividades institucionais e deverão ser utilizados de forma responsável, segura e compatível com a legislação e com esta Política.

Art. 22. É vedado, salvo autorização institucional e justificativa técnica:

I - instalar ou utilizar software não licenciado, não homologado ou de origem desconhecida;

II - desabilitar mecanismos de proteção, antivírus, atualizações, bloqueios ou controles de segurança;

III - acessar conteúdo ou sítios sabidamente maliciosos ou incompatíveis com a atividade institucional;

IV - armazenar documentos ou dados institucionais em contas pessoais de e-mail, nuvens pessoais ou serviços não homologados;

V - compartilhar credenciais ou permitir o uso de conta institucional por terceiro não autorizado;

VI - conectar dispositivos ou mídias externas de origem desconhecida quando houver risco à rede ou aos dados; e

VII - inserir informações restritas ou dados pessoais em ferramentas públicas de inteligência artificial sem avaliação prévia e autorização institucional.

Art. 23. O uso de e-mail institucional deverá observar cautela com links, anexos, remetentes desconhecidos, solicitações urgentes de credenciais ou pagamentos e demais sinais de phishing ou engenharia social.

Art. 24. O uso de dispositivos móveis e aplicativos de mensagens para atividades institucionais deverá priorizar equipamentos, contas e canais institucionais.

§ 1º. O uso excepcional de dispositivo ou canal pessoal não autoriza armazenamento permanente de informação institucional e deverá observar as salvaguardas definidas pela Câmara.

§ 2º. Documentos oficiais, documentos com dados pessoais, informações financeiras, documentos de licitação, atestados e informações restritas não deverão ser encaminhados por WhatsApp pessoal quando houver canal institucional adequado.

Art. 25. Impressoras e documentos impressos deverão ser utilizados de modo a evitar abandono de documentos restritos em bandejas, mesas, salas compartilhadas ou locais de livre circulação.

CAPÍTULO VI

DO COMPARTILHAMENTO INTERNO E EXTERNO

Art. 26. O compartilhamento interno de informações deverá ocorrer apenas entre pessoas e unidades que necessitem dos dados para executar suas atribuições, observando finalidade, minimização, classificação e canal adequado.

Art. 27. Os fluxos internos de maior risco ou recorrência deverão ser formalizados, especialmente aqueles envolvendo RH e Financeiro, Secretaria, Contabilidade, Licitações, Compras, Gabinete, Controladoria, Frota, Recepção e demais unidades identificadas no ROPA.

Art. 28. O compartilhamento externo deverá:

I - possuir finalidade institucional e fundamento legal ou contratual adequado;

II - limitar-se às informações necessárias à finalidade;

III - utilizar canal compatível com a classificação da informação;

IV - ser dirigido ao destinatário correto, com conferência prévia de endereço eletrônico, conta, sistema ou identificação;

V - observar, quando aplicável, os registros e deveres de transparência previstos na Política de Governança em Proteção de Dados; e

VI - preservar evidência ou rastreabilidade quando a natureza do processo exigir.

Art. 29. O envio de informações restritas ou restritas sensíveis por e-mail deverá utilizar conta institucional e, quando o risco justificar, medidas adicionais de proteção, como arquivo protegido, limitação de acesso ou outro mecanismo tecnicamente disponível.

Art. 30. A publicação em Portal da Transparência, Diário Oficial, site, redes sociais, atas, transmissões e outros meios públicos deverá observar a legislação de transparência e, simultaneamente, a minimização de dados pessoais prevista na Resolução nº 005/2026 e no Aviso de Privacidade.

Art. 31. Compartilhamentos com Tribunal de Contas, Receita Federal, e Social, INSS, BodoPrev, Ministério Público, instituições financeiras, Prefeitura e demais órgãos públicos deverão utilizar, preferencialmente, sistemas oficiais ou canais institucionais próprios.

CAPÍTULO VII

DA SEGURANÇA DE SISTEMAS, REDES, BACKUPS E ACESSOS REMOTOS

Art. 32. Os sistemas e equipamentos deverão ser mantidos atualizados e protegidos de acordo com sua criticidade e capacidade técnica, com mecanismos de prevenção contra códigos maliciosos, acessos indevidos e perda de informação.

Art. 33. A Câmara manterá rotinas de backup compatíveis com a criticidade dos serviços, contemplando, progressivamente:

I - definição dos dados e sistemas abrangidos;

II - frequência de execução;

III - responsabilidade pela rotina;

IV - controle de acesso às cópias;

V - prazo ou critério de retenção;

VI - proteção contra alteração ou exclusão indevida; e

VII - testes periódicos de restauração.

Art. 34. Os acessos remotos de empresas de sistemas, assessorias e suporte técnico deverão ser limitados ao necessário, preferencialmente autorizados, temporários e registráveis, observando as regras contratuais e de proteção de dados.

Art. 35. A contratação ou utilização de serviço em nuvem dependerá de avaliação prévia quanto à finalidade, segurança, controle de acesso, backup, disponibilidade, retenção, localização ou transferência de dados, encerramento do serviço e responsabilidades do fornecedor.

Art. 36. A utilização de ferramentas de inteligência artificial em atividades institucionais deverá observar ato ou orientação específica, sendo vedada a inserção de informação restrita, restrita sensível ou dado pessoal em ferramenta não previamente avaliada para essa finalidade.

CAPÍTULO VIII

DA SEGURANÇA FÍSICA, AMBIENTAL E DO DESCARTE

Art. 37. Ambientes que abriguem servidores, equipamentos de rede, backups, arquivos documentais ou outros ativos críticos deverão possuir acesso limitado às pessoas autorizadas.

Art. 38. A Câmara adotará, conforme avaliação técnica e disponibilidade estrutural,

medidas de proteção ambiental e continuidade, incluindo proteção contra incêndio, falhas elétricas, calor, umidade e outras condições capazes de comprometer equipamentos e documentos.

Art. 39. Documentos em papel contendo informação restrita ou restrita sensível deverão ser descartados por fragmentação, trituração ou método equivalente que impeça sua reconstrução.

Art. 40. Mídias, computadores, celulares, discos e demais dispositivos deverão ter seus dados eliminados de forma segura antes de descarte, devolução, transferência, alienação ou reutilização, quando tecnicamente aplicável.

Art. 41. O Patrimônio e a Tecnologia da Informação deverão manter fluxo coordenado para a baixa e destinação de equipamentos que possam conter dados institucionais.

CAPÍTULO DA GESTÃO DE INCIDENTES DE SEGURANÇA

Art. 42. Todo usuário deverá comunicar imediatamente qualquer suspeita ou ocorrência de incidente de segurança ao responsável pela Tecnologia da Informação ou responsável técnico de TI formalmente designado pela Câmara e, quando o evento envolver ou puder envolver dados pessoais, também ao Encarregado pelo Tratamento de Dados Pessoais. A comunicação deverá ocorrer mesmo quando ainda não houver confirmação de vazamento, dano ou acesso indevido.

Art. 43. A gestão dos incidentes de segurança será coordenada operacionalmente pelo responsável pela Tecnologia da Informação ou responsável técnico de TI formalmente designado, com participação do Encarregado sempre que houver dados pessoais envolvidos, e apoio da Administração, da unidade responsável pelo processo, do Jurídico e da Presidência, conforme a natureza e a gravidade do evento. O Plano de Resposta a Incidentes de Segurança deverá contemplar, no mínimo:

- I - canal institucional para recebimento do relato, triagem inicial e registro do incidente pelo responsável pela TI;
- II- classificação do incidente quanto à natureza, criticidade, ativos, sistemas, documentos, serviços e informações afetados;
- III- adoção, pela TI ou por quem detenha competência técnica, das medidas de contenção, isolamento, bloqueio, preservação de evidências e prevenção de agravamento;
- IV - avaliação do impacto, da extensão e da causa provável do incidente, com participação da unidade responsável pelo processo afetado;
- V - medidas de erradicação, recuperação, restauração e continuidade dos serviços, inclusive acionamento de backups quando necessário;
- VI - comunicação interna e escalonamento à Administração e à Presidência nos incidentes relevantes, críticos ou que possam comprometer a continuidade institucional;
- VII - avaliação, pelo Encarregado, quando houver dados pessoais, da natureza e das categorias de dados afetados, dos riscos aos titulares, das medidas de mitigação e das providências previstas na legislação de proteção de dados;
- VIII - avaliação conjunta, quando cabível, das comunicações legalmente exigidas à Autoridade Nacional de Proteção de Dados - ANPD, aos titulares, às autoridades competentes, aos fornecedores ou a terceiros envolvidos; e
- IX - documentação das providências adotadas, encerramento do incidente, registro de lições aprendidas e definição de medidas corretivas e preventivas.

Art. 44. Para fins deste Capítulo, compete ao responsável pela Tecnologia da Informação ou responsável técnico de TI coordenar as providências técnicas e operacionais de resposta, contenção, preservação de evidências, recuperação e restabelecimento dos serviços. Compete ao Encarregado, quando houver dados pessoais envolvidos, orientar quanto às obrigações da LGPD, avaliar os riscos aos direitos dos titulares, acompanhar o registro do incidente e subsidiar a decisão sobre eventual comunicação à ANPD e aos titulares, preservada sua autonomia e sem lhe atribuir a execução operacional das atividades de TI.

Art. 45. Os incidentes deverão ser registrados em repositório de acesso restrito. Os registros técnicos ficarão sob a guarda da área ou responsável pela TI, e os registros relacionados à proteção de dados pessoais serão acompanhados pelo Encarregado, observados os prazos e critérios de retenção aplicáveis. As informações deverão ser preservadas pelo período necessário à apuração, à prestação de contas, ao cumprimento de obrigações legais ou contratuais e ao aperfeiçoamento dos controles de segurança.

CAPÍTULO X DA GESTÃO DE FORNECEDORES E CONTRATOS

Art. 46. Contratações que envolvam acesso a sistemas, rede, equipamentos, documentos ou informações institucionais deverão prever requisitos de segurança proporcionais ao risco.

Art. 47. Sem prejuízo das cláusulas de proteção de dados previstas na Resolução nº 005/2026, os instrumentos contratuais deverão contemplar, quando aplicável:

- I - confidencialidade e dever de sigilo;
- II - regras de controle de acesso e credenciais;
- III - procedimentos de suporte e acesso remoto;
- IV - registro de intervenções técnicas;
- V - medidas mínimas de segurança e continuidade;
- VI - backup, recuperação e disponibilidade quando integrantes do serviço;
- VII - comunicação imediata de incidentes;
- VIII - subcontratação e acesso por terceiros;
- IX - devolução, portabilidade, eliminação ou preservação das informações ao término do contrato; e
- X - responsabilidades pela segurança das informações e cooperação em auditorias ou apurações

CAPÍTULO XI DAS RESPONSABILIDADES E CONSEQUÊNCIAS

Art. 48. Todos os abrangidos por esta Política são responsáveis por cumprir as medidas de segurança aplicáveis às atividades que desempenham e por comunicar situações que possam comprometer informações ou ativos da Câmara.

Art. 49. O descumprimento desta Política poderá ensejar apuração de responsabilidade administrativa, civil e penal, conforme a natureza do vínculo, a legislação aplicável, o Estatuto dos Servidores, os contratos, os deveres funcionais e demais normas pertinentes, assegurados o contraditório e a ampla defesa quando cabíveis.

CAPÍTULO XII DAS DISPOSIÇÕES FINAIS

- Art. 50.** A Presidência poderá expedir normas, procedimentos e padrões complementares para execução desta PSI, especialmente sobre controle de acessos, senhas, backup, resposta a incidentes, continuidade, uso aceitável, acesso remoto, nuvem, inteligência artificial, classificação da informação e descarte seguro.
- Art. 51.** Os procedimentos técnicos poderão ser atualizados por ato administrativo próprio, sem necessidade de alteração desta Resolução, desde que preservadas suas diretrizes.
- Art. 52.** A PSI será revista periodicamente e sempre que houver alteração relevante na estrutura, nos sistemas, nos riscos, na legislação ou nos processos da Câmara.
- Art. 53.** Os casos omissos serão resolvidos pela Presidência ou Mesa Diretora, conforme suas competências, com apoio técnico da Administração, Tecnologia da Informação, Jurídico e, quando houver dados pessoais, do Encarregado.
- Art. 54.** Esta Resolução entra em vigor na data de sua publicação.
- Câmara Municipal de Bodoquena MS., 14 de outubro de 2.026.**

Ayrton Ferreira Marques
Presidente/CMB

ANEXO

MATRIZ INSTITUCIONAL DE CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO

Categoria	Exemplos	Acesso	Compartilhamento	Proteção mínima
Pública	Leis, projetos, atos, atas e informações de transparência, após avaliação de dados protegidos.	Livre, conforme legislação.	Canais oficiais de publicidade.	Integridade, versão oficial e minimização de dados pessoais.
Uso Interno	Rotinas administrativas, documentos de trabalho e comunicações internas sem sigilo específico.	Pessoas/unidades envolvidas.	Canais institucionais.	Controle de acesso compatível e armazenamento institucional.
Restrita	Dados pessoais, dados bancários, documentos funcionais, contratos não públicos, documentos administrativos em elaboração.	Necessidade de conhecer.	Somente destinatários necessários e canal adequado.	Credencial individual, controle físico/digital, minimização e descarte seguro.
Restrita Sensível	Dados de saúde, senhas, chaves, backups, registros de segurança e configurações críticas.	Estritamente necessário.	Excepcional e controlado.	Acesso reforçado, MFA quando disponível, registro de acesso quando possível, guarda restrita e descarte seguro.

Nota: a classificação operacional acima orienta os controles de segurança e não substitui a classificação formal de sigilo prevista na Lei de Acesso à Informação.

Matéria enviada por Leide Acosta Machado

