DECRETO Nº 58, DE 25 DE FEVEREIRO DE 2026.

Institui a Política de Segurança de Dados (PSD) no âmbito da Administração Pública Municipal de Canoas e estabelece suas diretrizes.

O PREFEITO MUNICIPAL, no uso das atribuições conferidas pelo inciso IV do art. 66 da Lei Orgânica Municipal,

Considerando a necessidade de proteger os ativos de informação do Município de Canoas contra ameaças internas e externas, garantindo a continuidade dos serviços públicos essenciais;

Considerando a importância de estabelecer diretrizes e responsabilidades claras para a segurança de dados no âmbito da Administração Pública Municipal;

Considerando as exigências legais relativas à proteção de dados pessoais e ao acesso à informação pública, Leis Federais nº 12.527, de 18 de novembro de 2011 - Lei de Acesso à Informação (LAI), nº 12.965, de 23 de abril de 2014 - Marco Civil da Internet, nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados (LGPD);

Considerando a necessidade de proteger dados sob a guarda do Município, assegurar a continuidade dos serviços públicos e observar a legislação aplicável em matéria de transparência e proteção de dados, especialmente a que se refere à Lei Federal nº 13.709, de 2018; e Considerando o disposto no processo SEI protocolado sob o nº 26.0.000006856-9, de 3 de fevereiro de 2026,

DECRETA:

CAPÍTULO I
DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a Política de Segurança de Dados (PSD) da Administração Pública Municipal de Canoas, com diretrizes para proteção, tratamento e governança de dados, em todos os órgãos e entidades municipais.

Art. 2º São objetivos da PSD:

I - proteger dados contra acessos, usos, alterações, divulgações e destruições não autorizados;

II - reduzir riscos operacionais e legais e assegurar a continuidade dos serviços públicos;

III - harmonizar transparência e proteção de dados, conforme legislação aplicável;

IV - estabelecer papéis, responsabilidades, controles e processos para o ciclo de vida dos dados;

...

V - promover a melhoria contínua e a responsabilização institucional.

Art. 3º A presente política aplica-se a:

I - todos os órgãos e entidades municipais;

II - servidores, empregados públicos, estagiários, terceirizados e colaboradores;

III - fornecedores e parceiros que tratem dados em nome do Município;

IV - dados em qualquer meio e formato, inclusive cópias de segurança.

CAPÍTULO II
PRINCÍPIOS E DEFINIÇÕES

Art. 4º A PSD observará os princípios:

I - legalidade, finalidade, necessidade e proporcionalidade;

II - confidencialidade, integridade, disponibilidade e autenticidade;

III - prevenção, segurança por padrão e por desenho;

IV - transparência e prestação de contas (*accountability*);

V - qualidade e minimização de dados.

Art. 5º Para os fins deste Decreto, consideram-se as seguintes definições essenciais:

I - dado: qualquer representação de fatos, conceitos ou instruções;

II - dado pessoal: informação relativa a pessoa natural identificada ou identificável;

III - dado pessoal sensível: dado pessoal sujeito a proteção reforçada, a exemplo de saúde, biometria, convicções;

IV - dado sigiloso: informação protegida por sigilo legal;

V - tratamento: toda operação realizada com dados;

VI - incidente de segurança: evento adverso que comprometa confidencialidade, integridade, disponibilidade ou autenticidade;

VII - controlador: Município de Canoas;

VIII - operador: terceiro que realiza tratamento em nome do controlador;

IX - proprietário da informação/dado: gestor responsável pelo conjunto de dados em sua unidade;

X - logs: registros cronológicos de eventos e acessos.

CAPÍTULO III
CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO

Art. 6º Os dados informações serão classificados, no mínimo como:

I - públicos;

II - internos;

III - confidenciais;

IV - sigilosos;

...

V - pessoais;

VI - pessoais sensíveis.

§1º A classificação orientará rotulagem, acesso, armazenamento, compartilhamento, retenção e descarte.

§º Dados pessoais e sensíveis observarão a proteção reforçada e base legal adequada.

§3º O detalhamento dos critérios de classificação constará em ato complementar do órgão central de Tecnologia da Informação (TI) e do Comitê de Governança.

CAPÍTULO IV
GOVERNANÇA E RESPONSABILIDADES

Art. 7º A governança da PSD observará a seguinte estrutura:

I - Comitê de Segurança da Informação e Proteção de Dados (CSIPD): instância colegiada de diretrizes, priorização de riscos, deliberação sobre normas complementares e monitoramento;

II - encarregado de proteção de dados (DPO): ponto focal com titulares e autoridade competente;

III - gestor de segurança da informação (GSI): coordenação técnica da segurança e interface com o CSIPD;

IV - órgão central de tecnologia da informação: implementação e operação dos controles técnicos;

V - gestores de unidade: custódia e conformidade no âmbito de suas áreas;

VI - usuários: cumprimento das regras e reporte de incidentes;

VII - operadores/fornecedores: observância contratual dos requisitos de segurança e privacidade.

§1º A composição e atribuições detalhadas serão definidas em ato próprio.

§2º Poderão ser instituídos grupos de trabalho para temas específicos (incidentes, classificação, contratos).

CAPÍTULO V
MEDIDAS DE SEGURANÇA PARA PROTEÇÃO DE DADOS

Art. 8º O Município adotará medidas proporcionais ao risco, incluindo:

I - gestão de identidades e acessos (mínimo privilégio, revisão periódica, desligamentos;

II - autenticação forte e, quando aplicável, multifator;

III - criptografia em trânsito e em repouso, com gestão segura de chaves;

...

IV - segmentação de redes e proteção de *endpoints*;

V - *hardening*, aplicação tempestiva de correções e gestão de vulnerabilidades;

VI - trilhas de auditoria, sincronização de tempo e monitoramento contínuo;

VII - segregação de ambientes (produção, teste, desenvolvimento) e mascaramento de dados;

VIII - *backups* regulares, testados e protegidos, inclusive cópias externas/imutáveis, quando cabível.

CAPÍTULO VI
COMPARTILHAMENTO E USO DE DADOS

Art. 9º O compartilhamento de dados obedecerá:

I - finalidade pública legítima, base legal adequada e minimização;

II - avaliação de risco e de impacto quando pertinente;

III- formalização por instrumento específico com cláusulas de segurança e privacidade;

IV - anonimização ou pseudonimização quando destinado a transparência ativa ou *analytics*;

V - restrições a dados sigilosos e pessoais conforme legislação aplicável.

§1º Pedidos de acesso via transparência observarão teste de interesse público e técnica de anonimização ou restrição quando envolverem dados pessoais ou sigilosos.

§2º O compartilhamento com terceiros exigirá equivalência de controles e auditoria.

CAPÍTULO VII
ARMAZENAMENTO, RETENÇÃO E DESCARTE

Art. 10. O armazenamento e a retenção de dados seguirão:

I - tabelas de temporalidade e requisitos legais ou regulatórios;

II - princípios de minimização e limitação de finalidade;

III - requisitos de segurança do ambiente de guarda, com controles de acesso e criptografia.

Art. 11. O descarte observará:

I - eliminação irrecuperável para dados que não demandem guarda permanente;

II - registro do processo de eliminação;

III - preservação de cadeias de custódia quando houver obrigação de guarda.

...

CAPÍTULO VIII
INCIDENTES DE SEGURANÇA DE DADOS

Art. 12. A gestão de incidentes seguirá processo formal:
I - detecção e registro;
II - análise e classificação de severidade;
III - contenção, erradicação e recuperação;
IV - comunicação à autoridade competente e aos titulares, quando exigido;
V - lições aprendidas e atualização de controles.
§1º Todo usuário deverá reportar suspeitas de incidente pelos canais oficiais.
§2º O GSI coordenará a resposta com o DPO e o órgão central de TI.

CAPÍTULO IX
MONITORAMENTO, AVALIAÇÃO E AUDITORIA

Art. 13. A PSD será monitorada por indicadores e auditorias:
I - métricas de incidentes, tempos de detecção e resposta, conformidade de acessos, status de correções e capacitação;
II - auditorias internas e, quando aplicável, externas;
III - relatórios periódicos ao CSIPD e à Alta Administração.
§1º A revisão da PSD ocorrerá ao menos anualmente ou diante de mudanças relevantes.
§2º As unidades deverão manter registros de conformidade e planos de ação.

CAPÍTULO X
DISPOSIÇÕES COMPLEMENTARES

Art. 14. As contratações de bens e serviços incluirão requisitos de segurança e privacidade, due diligence, direitos de auditoria e penalidades por descumprimento.
Art. 15. Casos excepcionais ou de inviabilidade técnica serão formalizados com análise de risco, prazo e aprovação do CSIPD.
Art. 16. A Secretaria Municipal de Transparência, Controladoria e Governo Digital (SMTCGD) em conjunto com a Fundação Municipal de Tecnologia da Informação e Comunicação de Canoas – CANOASTEC, editarão normas e procedimentos complementares no prazo de 90 (noventa) dias a contar da publicação deste Decreto.

...

CAPÍTULO XI
DISPOSIÇÕES FINAIS

Art. 17. Este Decreto entra em vigor na data de sua publicação, aplicando-se a todos os órgãos e fundações municipais.

MUNICÍPIO DE CANOAS, em vinte e cinco de fevereiro de dois mil e vinte e seis (25.2.2026).

Airton Souza
Prefeito Municipal