DECRETO Nº 32, DE 28 DE JANEIRO DE 2026.

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

O PREFEITO MUNICIPAL, no uso das atribuições que lhe confere o inciso IV do artigo 66 da Lei Orgânica;

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 da informação 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); e

Considerando o disposto no processo SEI protocolado sob o nº 25.0.000086595-0, de 3 de novembro de 2025,

DECRETA:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES E PRINCÍPIOS GERAIS

Art. 1º Fica instituída, no âmbito da Administração Pública Municipal de Canoas, a Política de Segurança da Informação (PSI), que estabelece as diretrizes e responsabilidades para a proteção dos ativos de informação do Município.

Art. 2º A Política de Segurança da Informação observará os seguintes princípios gerais:

I - confidencialidade: garantia de que a informação seja acessível somente por pessoas, entidades ou processos autorizados;

II - integridade: garantia da exatidão e completude da informação e dos métodos de seu processamento, protegendo-a contra alterações indevidas ou não autorizadas;

III - disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;

IV - autenticidade: garantia de que a informação é genuína e que a identidade do remetente ou da fonte é verdadeira;

V - legalidade: conformidade com a legislação aplicável, incluindo as normas de proteção de dados pessoais e acesso à informação;

VI - necessidade e proporcionalidade: tratamento de informações e dados estritamente ao necessário para o cumprimento das finalidades legais e institucionais;

VII - responsabilidade e prestação de contas (*Accountability*): demonstração da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de segurança da informação;

…

VIII - prevenção: adoção de medidas proativas para evitar incidentes de segurança;

IX - melhoria contínua: aprimoramento constante dos processos, controles e tecnologias de segurança da informação.

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

I - todos os órgãos e entidades da Administração Pública Municipal de Canoas;

II - todos os servidores públicos, empregados públicos, estagiários e colaboradores que, a qualquer título, desempenhem funções ou prestem serviços ao Município;

III - todos os fornecedores e prestadores de serviços que, em razão de suas atividades, tenham acesso ou tratem ativos de informação do Município;

IV - todos os ativos de informação, em qualquer formato (físico, digital, voz, imagem), incluindo sistemas, dados, equipamentos, redes e serviços de comunicação.

Art. 4º Para os fins deste Decreto, consideram-se as seguintes definições essenciais:

I - ativo de informação: qualquer informação ou sistema que possua valor para o Município e, portanto, necessita de proteção;

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

III - dado pessoal sensível: dado pessoal sobre 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 à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

IV - incidente de segurança da informação: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos ativos de informação que possa comprometer a confidencialidade, integridade, disponibilidade ou autenticidade;

V - controle de acesso: mecanismo para garantir que apenas pessoas, sistemas ou processos autorizados possam acessar ativos de informação;

VI - proprietário da informação: agente público responsável pela criação, manutenção, uso e descarte de um conjunto de informações ou sistema;

VII - operador/terceiro: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - registro de log: registro cronológico de eventos e atividades em sistemas de informação.

CAPÍTULO II
GOVERNANÇA E RESPONSABILIDADES

Art. 5º A governança da Segurança da Informação e Proteção de Dados no Município de Canoas será estabelecida por meio da seguinte estrutura:

I - Comitê de Segurança da Informação e Proteção de Dados (CSIPD): órgão colegiado com a finalidade de deliberar sobre as diretrizes, riscos, políticas, normas e padrões de segurança da informação e proteção de dados, bem como de monitorar sua implementação;

…

II - gestor de segurança da informação (GSI): agente público designado, responsável pela coordenação, implementação e gestão das atividades de segurança da informação e pela assessoria ao CSIPD;

III - órgão central de tecnologia da informação: responsável pela implementação e manutenção dos controles técnicos e operacionais de segurança da informação;

IV - encarregado geral de proteção de dados (DPO): agente público responsável por atuar como canal de comunicação entre o controlador, os titulares dos dados e a autoridade nacional de proteção de dados;

V - gestores de unidade: responsáveis por garantir a aplicação das políticas e normas de segurança da informação em suas respectivas áreas, bem como pela custódia e uso adequado dos ativos de informação sob sua responsabilidade;

VI - usuários: todos os que acessam ou utilizam os ativos de informação do Município, responsáveis por cumprir as normas e diretrizes de segurança.

§1º A composição e as atribuições detalhadas do CSIPD e do GSI serão definidas em ato normativo próprio.

§2º O DPO poderá ser o mesmo GSI, desde que não haja conflito de interesses.

CAPÍTULO III
CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO

Art. 6º As informações do Município serão classificadas para determinar o nível de proteção adequado, de acordo com seu valor, sensibilidade e requisitos legais.

§1º As informações serão categorizadas, no mínimo, em:

I - pública: informação cujo acesso é irrestrito e que pode ser divulgada sem quaisquer restrições;

II - interna: informação de uso restrito à Administração Pública Municipal e que não deve ser divulgada sem autorização;

III - confidencial: informação cujo acesso é restrito a indivíduos ou grupos específicos dentro da organização, e cuja divulgação não autorizada pode causar danos ao Município ou a terceiros;

IV - sigilosa: informação protegida por legislação específica de sigilo, cuja divulgação não autorizada pode acarretar graves sanções ou danos.

§ 2º A classificação de informações pessoais e sensíveis deverá seguir as diretrizes da legislação aplicável à proteção de dados.

§3º Serão estabelecidas regras de rotulagem, armazenamento, compartilhamento, retenção e descarte seguro para cada categoria de informação, conforme seu grau de criticidade e sensibilidade.

CAPÍTULO IV
CONTROLES E MEDIDAS DE SEGURANÇA

Art. 7º O Município implementará controles e medidas de segurança da informação para proteger seus ativos, conforme a classificação de cada informação e a avaliação de riscos.

Art. 8º O acesso aos ativos de informação será regido pelos seguintes princípios:

I - princípio do mínimo privilégio: os usuários e sistemas terão acesso apenas às informações e recursos estritamente necessários para o desempenho de suas funções;

II - gestão de identidades e acessos (IAM): será implementado um processo formal para gerenciar as identidades digitais dos usuários e seus respectivos perfis de acesso, com revisão periódica;

III - autenticação multifator (MFA): será exigida a autenticação multifator para acesso a sistemas e informações de alta criticidade ou sensibilidade, sempre que tecnicamente viável;

IV - segregação de funções: as funções e atribuições serão distribuídas de modo a evitar que uma única pessoa possa executar uma transação completa ou atividade crítica sem supervisão.

Art. 9º A segurança será incorporada em todas as etapas do ciclo de vida dos sistemas e serviços:

I - segurança em desenvolvimento: os projetos de desenvolvimento e aquisição de sistemas deverão incorporar requisitos de segurança desde as fases iniciais, utilizando práticas de desenvolvimento seguro;

II - gestão de mudanças: todas as alterações em sistemas, redes e infraestrutura deverão ser planejadas, testadas e documentadas, com impacto na segurança avaliado previamente;

III - gestão de vulnerabilidades: será implementado um processo contínuo de identificação, avaliação e tratamento de vulnerabilidades em sistemas e aplicações, incluindo a aplicação tempestiva de patches e atualizações;

IV - reforço da segurança (*Hardening*): os sistemas e equipamentos serão configurados de forma segura, removendo funcionalidades desnecessárias e fortalecendo as proteções padrão.

Art. 10. O Município adotará medidas para garantir a continuidade de seus serviços e a recuperação de suas informações:

I - continuidade de negócios e recuperação de desastres: serão elaborados e testados Planos de Continuidade de Negócios (PCN) e Planos de Recuperação de Desastres (PRD), definindo os Tempos de Recuperação Objetivo (RTO) e Pontos de Recuperação Objetivo (RPO) para sistemas críticos;

II - backup e restauração: serão realizados backups regulares e testados dos dados e sistemas críticos, com cópias armazenadas em locais seguros e, quando aplicável, utilizando soluções de backup imutáveis ou externas para maior resiliência.

…

Parágrafo único. O Município estimulará que as informações e dados do Município sejam hospedados e armazenados em infraestrutura própria e geridos pela Fundação Municipal de Tecnologia da Informação e Comunicação de Canoas - CANOASTEC, garantindo segurança digital, autonomia tecnológica e proteção das informações públicas e pessoais.

Art. 11. A gestão de incidentes de segurança e de dados será um processo formalizado:

I - será estabelecido um processo para detecção, análise, contenção, erradicação, recuperação e lições aprendidas de incidentes de segurança da informação e de dados;

II - a comunicação de incidentes às autoridades competentes e aos titulares de dados afetados será realizada em conformidade com a legislação aplicável, nos prazos e formas exigidos.

Art. 12. A presente política harmoniza os princípios da transparência pública e da proteção de dados com as seguintes premissas:

I - o acesso à informação pública será garantido em conformidade com a legislação aplicável, resguardando-se as informações classificadas como sigilosas ou pessoais;

II - na divulgação de informações públicas que contenham dados pessoais, serão priorizadas técnicas de anonimização ou pseudonimização, buscando o equilíbrio entre o direito de acesso e à proteção da privacidade;

III - a publicidade dos dados seguirá a avaliação do interesse público, visando sempre a minimização da exposição de dados pessoais e sensíveis.

CAPÍTULO V
DISPOSIÇÕES FINAIS

Art. 13. As contratações de bens e serviços com terceiros deverão contemplar requisitos de segurança da informação e proteção de dados:

I - os contratos, convênios e instrumentos congêneres deverão incluir cláusulas específicas que estabeleçam as responsabilidades do contratado em relação à segurança da informação e à proteção de dados;

II - será realizada a devida diligência (*due diligence*) para avaliar a capacidade dos fornecedores em cumprir os requisitos de segurança do Município;

III - as penalidades contratuais serão aplicadas em caso de descumprimento das obrigações de segurança e proteção de dados por parte dos contratados.

Art. 14. O Município promoverá a conscientização e o treinamento contínuos em segurança da informação:

I - serão desenvolvidos programas de conscientização e treinamento periódicos, adaptados aos diferentes perfis de usuários, sobre as políticas, normas e melhores práticas de segurança da informação e proteção de dados;

II - o descumprimento das normas e diretrizes estabelecidas neste Decreto e em atos complementares poderá acarretar responsabilização administrativa, civil e criminal, conforme a legislação vigente.

Art. 15. A eficácia da PSI será continuamente monitorada e auditada:

I - serão estabelecidos indicadores de desempenho (KPIs) para a segurança da informação, com monitoramento regular e reporte à alta administração;

II - serão realizadas auditorias internas e externas periódicas para verificar a conformidade com a PSI e identificar oportunidades de melhoria.

Art. 16. Casos omissos ou exceções à aplicação desta política deverão ser formalizados, submetidos à análise de risco e aprovados pelo CSIPD, com prazos definidos para sua revisão.

Art. 17. Este Decreto, bem como a PSI e proteção de dados, será revisado, no mínimo, anualmente ou sempre que houver mudanças significativas na legislação, nos processos de negócio ou na tecnologia, que impactem

Art. 18 Fica a CANOASTEC responsável por elaborar, no prazo de 90 (noventa) dias a contar da publicação deste Decreto, as normas complementares, procedimentos operacionais e padrões técnicos necessários para a efetivação desta Política, especialmente relacionados às normas complementares de:

I - norma para classificação de informação;

II - norma para credenciais e senhas;

III - norma para padrões de segurança da informação;

IV - norma para plano de resposta de incidentes;

V - norma para procedimentos de backup e armazenamento e hospedagem em nuvens;

VI - norma para repositório oficial de arquivos;

VII - norma para uso de e-mails e mensagens;

VIII - norma para uso de equipamentos e software; e

IX - normas para utilização do SEI.

Art. 19. Este Decreto entra em vigor na data de sua publicação.

MUNICÍPIO DE CANOAS, em vinte e oito de janeiro de dois mil e vinte e seis (28.1.2026).

Airton Souza
Prefeito Municipal