PREFEITURA MUNICIPAL DE IPUEIRA
DECRETO 002/2026

Institui a Política de Proteção de Dados Pessoais e Privacidade no âmbito do município de Ipueira/RN e dá outras providências.

O **PREFEITO DO MUNICÍPIO DE IPUEIRA**, no uso das atribuições que lhe confere a Lei Orgânica Municipal,

CONSIDERANDO o grau de indispensabilidade alcançado pela tecnologia da informação para a realização das funções institucionais e alcance dos objetivos estratégicos da Prefeitura Municipal;

CONSIDERANDO a crescente velocidade de processamento de dados e a elevada capacidade de armazenamento de informações proporcionadas pelos recursos tecnológicos atualmente utilizados pela Administração Pública;

CONSIDERANDO o grande volume de recursos humanos, financeiros e patrimoniais vinculados à operacionalização e manutenção de bens e serviços de tecnologia da informação do município;

CONSIDERANDO a necessidade de adequar as práticas de gestão, controle e tratamento de dados pessoais às diretrizes de boas práticas, governança e segurança da informação, em conformidade com padrões técnicos reconhecidos;

CONSIDERANDO a importância de se adotar abordagem institucional uniforme para a gestão de riscos relacionados à privacidade e à segurança da informação, com terminologia padronizada e procedimentos integrados entre as unidades administrativas;

CONSIDERANDO os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de proteção de dados pessoais e segurança da informação dentro do contexto da organização, bem como as normas para avaliação e tratamento de riscos;

CONSIDERANDO as diretrizes e normas que orientam a seleção, implementação e gerenciamento de controles de segurança da informação compatíveis com o ambiente de riscos da Administração Pública;

CONSIDERANDO que a Lei nº 12.527, de 18 de novembro de 2011, mais conhecida como Lei de Acesso à Informação (LAI), fixa como diretriz para a administração pública a observância da publicidade como preceito geral e do sigilo como exceção;

CONSIDERANDO que a Lei de Acesso à Informação (LAI) consigna que a administração pública deve pautar-se na utilização de meios de comunicação viabilizados pela tecnologia da informação;

CONSIDERANDO que a Lei nº 13.709, de 14 de agosto de 2018, também chamada de Lei Geral de Proteção de Dados Pessoais (LGPD), dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural;

CONSIDERANDO que a LGPD contém normas gerais sobre o tratamento de dados pessoais que são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios;

CONSIDERANDO que a Prefeitura Municipal de Ipueira deve construir uma cultura organizacional pautada na harmonização entre os preceitos da Lei de Acesso à Informação (LAI) e as normas sobre tratamento de dados pessoais constituídas pela Lei Geral de Proteção de Dados (LGPD);

CONSIDERANDO que se faz necessária a padronização do uso de recursos de Tecnologia da Informação, bem como para o armazenamento e tratamento de dados em meio digital, para que os processos de trabalho possuam o respaldo de medidas de segurança e privacidade compatíveis com o grau de relevância de que elas se revestem, em consonância com os princípios da LAI e da LGPD;

CONSIDERANDO que a proteção de dados pessoais, a privacidade e a segurança da informação e comunicação,

digital ou física, são temas de permanente acompanhamento e aperfeiçoamento, devendo ser constantemente revistos e atualizados, visando à melhoria contínua da qualidade dos processos internos e ao respeito aos direitos dos titulares de dados;

RESOLVE:

CAPÍTULO I

SEÇÃO I - Das Disposições Gerais

Art. 1º Fica instituída a Política de Proteção de Dados Pessoais e Privacidade no âmbito da Administração Direta e Indireta do Município de Ipueira, a qual observará os princípios, objetivos e diretrizes estabelecidos neste Decreto, bem como as disposições constitucionais e legais vigentes, especialmente a Lei nº 13.709/2018- Lei Geral de Proteção de Dados Pessoais (LGPD) e a Lei nº 12.527/2011– Lei de Acesso à Informação (LAI).

§ 1º Submetem-se às disposições desta Política os agentes públicos, servidores efetivos e comissionados, empregados públicos, estagiários, terceirizados, e quaisquer pessoas que tenham acesso a ativos de informação ou dados pessoais tratados pelo Município, sendo responsáveis por garantir a segurança, a integridade e a privacidade dos ativos físicos e lógicos a que tenham acesso no exercício de suas atribuições.

Art. 2º Nos casos não disciplinados expressamente neste Decreto, caberá aos agentes públicos e colaboradores da Administração Municipal adotar as medidas necessárias à preservação da segurança da informação, da privacidade e da proteção dos dados pessoais sob sua responsabilidade, em conformidade com a legislação aplicável e com os princípios desta Política.

Art. 3º É dever de todos aqueles que possuam acesso a ativos de informação ou dados pessoais do Município zelar pela proteção de dados, pela privacidade, pela confidencialidade, pela integridade e pela segurança das informações**.**

SEÇÃO II - Dos Princípios da Proteção de Dados Pessoais e Privacidade

Art. 4º A atividade de proteção de dados pessoais e de privacidade, no âmbito da Administração Direta e Indireta do Município de Ipueira, será desenvolvida em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), e com a Lei de Acesso à Informação (LAI), observando-se, entre outros, os seguintes princípios:

I – Proteção aos direitos humanos e respeito aos princípios constitucionais da Administração Pública, com especial atenção aos direitos fundamentais de liberdade, intimidade e privacidade dos titulares de dados;

II – Orientação das práticas institucionais pela ética, pela boa-fé, pela legalidade e pelos valores do Estado Democrático de Direito;

III – Atuação preventiva e proativa, com vistas à identificação, mitigação e neutralização de ameaças, vulnerabilidades e incidentes que possam comprometer a segurança e a privacidade dos dados pessoais;

IV – Integração e cooperação com outros órgãos e entidades públicas responsáveis pela proteção de dados, especialmente com a Autoridade Nacional de Proteção de Dados (ANPD);

V – Direcionamento das atividades à prevenção de riscos reais ou potenciais ao Município, aos agentes públicos e aos titulares de dados, inclusive aqueles decorrentes de falhas técnicas, humanas ou de eventos externos;

VI – Preservação da imagem institucional do Município, evitando exposições indevidas decorrentes de incidentes de segurança ou violação de privacidade;

VII – Incentivo à participação colaborativa e coordenada das unidades administrativas, visando à consolidação de cultura organizacional voltada à segurança da informação e à proteção de dados;

VIII – Gestão de riscos orientada à proteção dos ativos de informação do Município e, especialmente, dos dados pessoais tratados;

IX – Proteção da vida, do patrimônio público e do meio ambiente, considerados os impactos da segurança da informação nesses aspectos;

X – Finalidade, consistente na realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, vedado tratamento posterior incompatível com essas finalidades;

XI – Adequação, consistente na compatibilidade do tratamento com as finalidades informadas ao titular e com o contexto de

sua realização;
XII – Necessidade, mediante limitação do tratamento ao mínimo indispensável para o alcance de suas finalidades, com dados pertinentes, proporcionais e não excessivos;
XIII – Livre acesso, assegurando aos titulares consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados;
XIV – Qualidade dos dados, garantindo exatidão, clareza, relevância e atualização das informações, conforme a finalidade do tratamento;
XV – Transparência, com fornecimento de informações claras, precisas e acessíveis sobre o tratamento e os respectivos agentes, resguardados os sigilos legais;
XVI – Segurança, mediante adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
XVII – Prevenção, por meio da adoção de medidas destinadas a evitar a ocorrência de danos decorrentes do tratamento de dados pessoais;
XVIII – Não discriminação, vedado o tratamento para fins discriminatórios ilícitos ou abusivos;
XIX – Responsabilização e prestação de contas, com demonstração, pelos agentes de tratamento, da adoção de medidas eficazes para comprovar a observância das normas de proteção de dados pessoais.

SEÇÃO III - Dos Conceitos Fundamentais

Art. 5º Para efeitos deste Decreto, são considerados os seguintes conceitos:
I – Ativo de informação: todo recurso utilizado na produção, processamento, armazenamento, transmissão e recuperação da informação, compreendendo a própria informação, sistemas, redes, equipamentos de informática e telecomunicações, dispositivos móveis, mídias de armazenamento, softwares, bancos de dados, instalações físicas e as pessoas que tenham acesso a esses recursos;
II – Ciclo de vida da informação: conjunto de eventos relacionados à criação ou obtenção, à classificação, à distribuição, ao uso, ao armazenamento, ao descarte ou à guarda permanente da informação;
III – Informação: conjunto de dados registrados em meio físico ou eletrônico, produzidos, recebidos ou custodiados pelos órgãos e entidades da Administração Municipal, devendo ser classificada conforme o grau de sigilo e a necessidade de proteção;
IV – Classificação da informação: ação que define o grau de sigilo e os grupos de acesso atribuídos à informação, visando a garantir um nível adequado de proteção;
V – Autenticidade: assegura a correspondência entre o autor de determinada informação e a pessoa, processo ou sistema a quem se atribui a autoria;
VI – Confidencialidade: garantia de que a informação seja acessada somente pelos usuários ou processos autorizados;
VII – Disponibilidade: garantia de que usuários possam ter pronto acesso às informações segundo sua demanda e em conformidade com a política de proteção de dados e segurança;
VIII – Integridade: garantia de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental, inclusive quanto à origem, trânsito e destino;
IX – Não repúdio: garantia de que o emissor da mensagem não irá negar posteriormente a autoria da mensagem ou transação, permitindo a sua identificação;
X – Incidentes de Segurança da Informação e de Dados Pessoais: qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação da segurança de dados pessoais, como acessos não autorizados, acidentais ou ilícitos de destruição, perda, alteração, comunicação ou difusão de dados pessoais;
XI – Informação sigilosa: aquela abrangida pelas hipóteses legais de restrição de acesso ou a classificada como sigilosa, submetida temporariamente à restrição de acesso público, em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, ou para a proteção da privacidade e dados pessoais;
XII – Gestão de riscos de segurança da informação e privacidade: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar os riscos a que estão sujeitos os seus ativos de informação e dados pessoais, e equilibrá-los com os custos operacionais e financeiros envolvidos;

XIII – Usuário interno: agente público, servidor efetivo ou comissionado, empregado público, terceirizado, estagiário, ou qualquer pessoa, em razão de vínculo funcional ou contratual, tenha acesso às informações da Administração Pública Municipal;
XIV – Usuário externo: pessoa física ou jurídica que tenha acesso às informações produzidas ou custodiadas pelo Município, sem vínculo funcional direto com a Administração;
XV – Gestor da informação: autoridade ou servidor responsável pela produção, guarda, gerenciamento e uso das informações no âmbito de sua unidade administrativa;
XVI – Conta: registro individual que identifica o usuário por meio de credenciais próprias, conferindo permissão para utilização de recursos tecnológicos institucionais;
XVII – Dado Pessoal: informação relacionada a pessoa natural identificada ou identificável;
XVIII – 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;
XIX – Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
XX – Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
XXI – Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
XXII – Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
XXIII – Encarregado (DPO): pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
XXIV – Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
XXV – Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de ser associado, direta ou indiretamente, a um indivíduo;
XXVI – Pseudonimização: tratamento por meio do qual um dado é processado de tal forma que não possa mais ser atribuído a um titular sem o uso de informação adicional, desde que essa informação adicional seja mantida separadamente e sujeita a medidas técnicas e organizacionais adequadas para garantir que os dados pessoais não sejam atribuídos a uma pessoa natural identificada ou identificável.

SEÇÃO IV - Dos Objetivos da Política

Art. 6º A Política de Proteção de Dados Pessoais e Privacidade do Município de Ipueira tem como objetivos:
I – Garantir a autoria do responsável pelo envio e tratamento da informação e dos dados pessoais;
II – Assegurar que os ativos de informação, os dados pessoais e os recursos de processamento e armazenamento sejam protegidos contra acesso não autorizado, destruição, perda, alteração, comunicação, vazamento ou difusão indevida;
III – Garantir que as informações e dados institucionais estejam, sempre que possível e necessário, disponíveis ao solicitante, observadas as normas de transparência pública e de proteção de dados;
IV – Preservar a consistência, a integridade e a segurança das informações e dados pessoais armazenados ou transmitidos pelos órgãos e entidades da Administração Municipal;
V – Promover a conscientização e o comprometimento de agentes públicos, servidores, empregados públicos, terceirizados, estagiários e demais colaboradores quanto à confidencialidade, integridade, disponibilidade das informações, segurança das operações e proteção de dados pessoais;
VI – Assegurar a divulgação ativa de informações de interesse público, independentemente de solicitações, respeitados os limites legais de sigilo e proteção de dados pessoais;
VII – Incentivar o uso eficiente, seguro e responsável dos meios de comunicação e das tecnologias da informação, com

respeito à privacidade dos titulares;
VIII – Fomentar a cultura de transparência, governança, gestão de riscos e proteção de dados no âmbito da Administração Pública Municipal;
IX – Contribuir para o fortalecimento do controle social da administração pública, possibilitando aos cidadãos o exercício pleno de seus direitos como titulares de dados;
X – Garantir o exercício dos direitos dos titulares de dados pessoais, conforme previsto na LGPD.
XI – Instituir e manter a função de Encarregado pelo Tratamento de Dados Pessoais (DPO), como canal de comunicação entre o Município, os titulares de dados e a Autoridade Nacional de Proteção de Dados;
XII – Assegurar que o tratamento de dados pessoais seja realizado em estrita observância aos princípios da LGPD e demais legislações pertinentes.
Parágrafo único. Os objetivos da Política de Proteção de Dados Pessoais e Privacidade deverão estar alinhados ao planejamento estratégico do Município e ao Plano Diretor de Tecnologia da Informação, quando existente, bem como às diretrizes de governança e gestão pública.

CAPÍTULO II - DO TRATAMENTO DE INFORMAÇÕES E DADOS PESSOAIS

SEÇÃO I - Da Classificação da Informação

Art. 7º A classificação da informação e dos dados pessoais tem por objetivo assegurar que recebam um nível adequado de proteção.
Parágrafo único. As informações e os dados pessoais serão classificados para indicar a necessidade, as prioridades e o nível esperado de proteção durante todo o seu ciclo de vida, compreendendo criação, uso, armazenamento, compartilhamento, arquivamento e descarte.
Art. 8º A classificação da informação quanto ao grau de sigilo observará norma específica a ser editada pelo Poder Executivo Municipal, que disciplinará o acesso à informação e a aplicação da Lei de Acesso à Informação e da Lei Geral de Proteção de Dados Pessoais no âmbito dos órgãos e entidades da Administração Pública Municipal.
Parágrafo único. Poderá ser considerada sigilosa qualquer informação ou dado pessoal cuja divulgação irrestrita possa:
I – Gerar riscos à vida, à integridade física, à honra, à segurança ou à saúde da população ou dos titulares de dados;
II – Comprometer a segurança institucional, a defesa civil, a economia local, a ordem administrativa ou as relações federativas/municipais do Estado e do Município;
III – Ocasionar assimetria concorrencial, prejuízo econômico ou favorecimento indevido entre pessoas físicas ou jurídicas;
IV – Expor o Município a ataques, fraudes, incidentes de segurança ou responsabilização decorrente do descumprimento da legislação de proteção de dados;
V – Referir-se a autorizações, estudos, pareceres, processos administrativos, investigações, fiscalizações ou procedimentos internos ainda não concluídos, quando a divulgação puder prejudicar sua finalidade ou violar direitos dos titulares;
VI – Envolver denúncias, representações, apurações preliminares ou processos disciplinares em curso, quando o acesso puder comprometer a instrução processual, a apuração dos fatos ou a proteção da identidade do denunciante.
Art. 9º A unidade administrativa ou setor responsável, designado pelo Poder Executivo Municipal, será competente para classificar as informações e os dados pessoais sob sua responsabilidade, de acordo com o grau de sigilo, a sensibilidade e os riscos associados ao tratamento.
Art. 10. Para os fins deste Decreto, considera-se informação pessoal todo dado relacionado à pessoa natural identificada ou identificável, inclusive aqueles referentes à vida privada, à honra, à imagem e à intimidade, conforme definido na Lei Geral de Proteção de Dados Pessoais.
Parágrafo único. As disposições deste artigo aplicam-se, no que couber, às pessoas jurídicas, quando o tratamento de informações puder resultar na identificação de pessoas naturais a elas vinculadas.

SEÇÃO II - Das Obrigações do Gestor da Informação e dos Dados Pessoais

Art. 11. São responsabilidades dos gestores da informação e dos dados pessoais, no âmbito dos órgãos e entidades da Administração Pública Municipal, relativamente às informações e dados produzidos, recebidos ou custodiados sob sua gestão:

I – Manter atualizada a relação de usuários com acesso às informações e aos dados pessoais sob sua responsabilidade, indicando perfis, níveis de acesso e respectivas finalidades;
II – Coordenar as atividades de identificação, classificação e enquadramento das informações e dados pessoais, observando os princípios da LGPD;
III – Assegurar o cumprimento das normas, políticas e procedimentos relativos à proteção de dados pessoais, privacidade e segurança da informação;
IV - Definir procedimentos e grupos de acesso, observados os dispositivos legais e regimentais relativos ao sigilo, à LAI, à LGPD e a outros requisitos de segurança pertinentes;
V – Promover a conscientização e capacitação dos usuários internos quanto aos conceitos, deveres e boas práticas de proteção de dados pessoais, privacidade e segurança da informação;
VI – Adotar ou propor as medidas administrativas, técnicas e disciplinares cabíveis, inclusive ações corretivas e preventivas, sempre que verificado o comprometimento da segurança da informação ou de dados pessoais por parte de usuários internos ou terceiros vinculados à Administração Municipal;
VII – Classificar, rotular e sinalizar as informações sigilosas e os dados pessoais sensíveis sob sua responsabilidade, especialmente aqueles enquadrados em hipótese legal de restrição de acesso, segredo de justiça ou que demandem maior nível de proteção, assegurando tratamento compatível com sua natureza e grau de risco.

SEÇÃO III - Do Ciclo de Vida da Informação e dos Dados Pessoais

Art. 12. O ciclo de vida da informação e dos dados pessoais é composto pelas etapas de manuseio, armazenamento, transporte e descarte, assim caracterizadas:
I - Manuseio: momento em que a informação ou o dado pessoal é criado e manipulado, seja sob a forma física ou eletrônica, devendo ser observados os princípios da LGPD, especialmente finalidade, necessidade e segurança;
II - Armazenamento: fase em que há o armazenamento propriamente dito da informação ou do dado pessoal, seja em papel, arquivo físico, banco de dados ou qualquer outro tipo de mídia, exigindo medidas técnicas e administrativas de segurança para sua proteção;
III - Transporte: etapa em que a informação ou o dado pessoal é transportado, seja em papel, mídia ou por meio remoto em uma rede de computadores, devendo ser empregados mecanismos de segurança para prevenir acessos não autorizados;
IV - Descarte: momento em que a informação ou o dado pessoal é descartado, em formato físico ou eletrônico, de forma segura e irrecuperável, em conformidade com a legislação aplicável e com a LGPD, evitando vazamentos e acessos indevidos.
Art. 13. Caberá a cada gestor de informação e de dados pessoais tomar as devidas providências em relação ao ciclo de vida da informação e dos dados sob sua responsabilidade, que se encontrem em seu setor.

SEÇÃO IV - Do Tratamento dos Ativos de Informação e Dados Pessoais

Art. 14. As unidades administrativas que compõem a Administração Pública Municipal deverão atribuir a um ou mais servidores ou agentes públicos a responsabilidade pela classificação, registro e documentação de seus ativos de informação e dados pessoais, considerando seu valor, sensibilidade, criticidade e requisitos legais de proteção.
§ 1º A designação dos responsáveis deverá ocorrer de forma tempestiva, preferencialmente no momento da criação, recebimento ou transferência do ativo ou dado para a unidade administrativa.
§ 2º O prazo máximo para a atribuição dos responsáveis pela classificação e documentação dos ativos e dados pessoais será definido em norma específica.
Art. 15. Após a devida classificação, os ativos e dados pessoais deverão ser atribuídos a proprietários ou responsáveis pelo tratamento, que ficarão responsáveis pelo seu ciclo de vida e sua segurança e privacidade, mantendo a respectiva documentação atualizada, e revisando-a sempre que houver mudanças que justifiquem a sua atualização, nos termos definidos em norma complementar.
Parágrafo único. A atribuição de responsabilidade não confere direito de propriedade sobre o ativo ou os dados, limitando-se à

obrigação de gestão, proteção e conformidade legal.
Art. 16. As diretrizes, procedimentos e critérios para classificação, documentação, rotulagem, armazenamento, compartilhamento, descarte e demais formas de tratamento dos ativos de informação e dados pessoais serão disciplinados em norma específica.
Art. 17. A retirada de ativos de informação, equipamentos, documentos ou dados pessoais das dependências dos órgãos ou entidades municipais dependerá de autorização da chefia imediata, do gestor responsável ou do proprietário do ativo.
§ 1º A autorização somente será concedida quando necessária à continuidade das atividades institucionais, devendo ser asseguradas medidas adequadas de segurança da informação e proteção da privacidade dos titulares.
§ 2º Apenas servidores, empregados públicos ou agentes formalmente autorizados poderão realizar a retirada de ativos ou dados pessoais, observados os deveres de confidencialidade e responsabilidade funcional.
§ 3º O responsável deverá providenciar a devolução do ativo ou a restituição das informações ao órgão quando cessarem os motivos que justificaram a retirada ou quando do encerramento do vínculo funcional ou contratual, assegurando a integridade do material e a eliminação de cópias não autorizadas.
Art. 18. Os ativos de informação, os dados pessoais e os recursos de armazenamento e processamento deverão ser utilizados exclusivamente para fins institucionais, de forma ética, segura e em conformidade com a LGPD.

Art. 19. Norma complementar disciplinará as condições para utilização de dispositivos ou recursos computacionais pessoais por agentes públicos no ambiente institucional ou em regime de teletrabalho, garantindo a segurança das informações públicas e a proteção dos dados pessoais tratados pela Administração Municipal.

SEÇÃO V - Do Gerenciamento de Eventos e Incidentes
Art. 20. Deverão ser implementados e documentados procedimentos destinados à identificação, e tratamento de eventos relacionados aos ativos de informação, sistemas e equipamentos de armazenamento e processamento de dados, com o objetivo de prevenir a ocorrência de incidentes que possam comprometer a disponibilidade, integridade, confidencialidade ou privacidade das informações, dos serviços de tecnologia da informação e dos dados pessoais tratados pela Administração Pública Municipal.
Parágrafo único. A classificação dos eventos de acordo com a sua criticidade, bem como os procedimentos necessários para tratá-los de forma apropriada, serão definidos em norma específica, incluindo a comunicação à ANPD e aos titulares em caso de incidentes de dados pessoais.
Art. 21. A Unidade Responsável pela Tecnologia da Informação manterá um núcleo de gerenciamento de incidentes que deverá garantir a restauração dos serviços de TI de forma hábil, nos prazos e termos definidos em norma, minimizando eventuais efeitos negativos nos processos do órgão e nos direitos dos titulares de dados.

SEÇÃO VI - Do Gerenciamento de Problemas
Art. 22. A Unidade Responsável pela Tecnologia da Informação manterá um núcleo de gerenciamento de problemas, que visa minimizar a interrupção nos serviços de TI, buscando reduzir a quantidade de incidentes e evitar sua recorrência, especialmente aqueles que possam impactar a segurança e a privacidade dos dados pessoais.
§ 1º O núcleo de gerenciamento de problemas analisará as causas dos incidentes recorrentes ou de grande impacto para os serviços de TI e a proteção de dados pessoais.
§ 2º Será mantido um banco de dados de erros conhecidos que conterá todas as soluções produzidas pelo núcleo de gerenciamento de problemas.
§ 3º Os procedimentos necessários para analisar e tratar os problemas serão dispostos em norma específica.
SEÇÃO VII - Da Gestão de Riscos
Art. 23. O Município de Ipueira deverá elaborar e manter Plano de Gerenciamento de Riscos voltado à identificação, análise, avaliação e tratamento de ameaças e vulnerabilidades que possam causar danos à Administração Pública Municipal, especialmente aqueles relacionados à segurança da informação, à privacidade e à proteção de dados pessoais.

Parágrafo único. O plano deverá estabelecer critérios objetivos para classificação e priorização dos riscos, definindo quais são aceitáveis e quais demandam controles técnicos, administrativos ou organizacionais específicos, considerando os impactos institucionais e os potenciais prejuízos aos direitos e liberdades dos titulares de dados pessoais.

SEÇÃO VIII - Da Gestão de Continuidade

Art. 24. O Município adotará procedimentos formais e emergenciais destinados a assegurar a continuidade das atividades administrativas e dos serviços públicos essenciais, mediante a instituição de Sistema de Gestão de Continuidade de Negócios, para enfrentamento de incidentes de segurança da informação, falhas tecnológicas, desastres naturais ou quaisquer eventos que possam interromper processos organizacionais ou comprometer a proteção de dados pessoais.

Art. 25. O Sistema de Gestão de Continuidade de Negócios será responsável pela implementação de rotinas periódicas de cópias de segurança (backups) dos ativos de informação e dos dados pessoais, com vistas à prevenção de perdas, danos ou indisponibilidades decorrentes de incidentes ou desastres.

SEÇÃO IX - Da Auditoria e Conformidade

Art. 26. Todos os ativos de informação, sistemas, processos e atividades que envolvam o tratamento de dados pessoais no âmbito da Administração Pública Municipal poderão ser submetidos a auditorias por equipe designada pela Unidade Responsável pela Tecnologia da Informação, pelo Encarregado de Dados ou por comitê específico, de acordo com os termos definidos em norma específica.

SEÇÃO X - Dos Controles de Acessos

Art. 27. A política de controle de acessos terá por finalidade restringir e gerenciar o acesso às informações, aos dados pessoais e aos recursos de processamento e armazenamento de dados, observadas as disposições deste Decreto e em norma específica, abrangendo, no mínimo:

I – Controles de acesso físico e lógico às informações sigilosas e aos dados pessoais;

II – Definição de perfis, papéis e responsabilidades para usuários com acesso privilegiado a sistemas e dados pessoais;

III – Requisitos para autorização formal de acesso a informações fiscais, financeiras, administrativas ou a dados pessoais sensíveis;

IV – Procedimentos para concessão, revisão, suspensão e revogação de privilégios de usuários, observando os princípios da necessidade, finalidade e minimização do acesso;

V – Controles para gerenciamento de credenciais de autenticação, incluindo prazos de validade, padrões mínimos de complexidade, senhas temporárias e hipóteses de bloqueio;

VI – Requisitos de acesso às redes e aos serviços de tecnologia da informação, com segmentação, registro de logs e monitoramento;

VII – Definição de regras de controle de entrada física em prédios, salas, arquivos e áreas críticas da Administração Municipal, conforme o nível de criticidade dos ativos e a presença de dados pessoais.

Art. 28. O acesso físico ou lógico aos ativos de informação, sistemas, aplicações e áreas protegidas será permitido exclusivamente a pessoas previamente autorizadas, de acordo com a finalidade institucional e a base legal do tratamento de dados.

Art. 29. Os servidores, empregados públicos, terceirizados, estagiários e demais colaboradores que tenham acesso a dados pessoais ou informações sigilosas deverão firmar termo de confidencialidade e responsabilidade.

Art. 30. As pessoas que, em razão do exercício de cargo, função ou emprego com a Administração Municipal, tenham acesso a dados pessoais ou informações protegidas por sigilo legal ficam sujeitas às penalidades prescritas neste Decreto em caso de uso indevido, divulgação não autorizada ou descumprimento do dever de sigilo.

Art. 31. O compartilhamento de dados pessoais pelo Município com outros órgãos ou entidades públicas ou privadas estarão sujeitos aos termos de acordos de cooperação ou instrumentos congêneres assinados, para fins de controle de acesso e responsabilidades sobre o tratamento desses dados, em conformidade com a LGPD.

Art. 32. Todos os servidores devem ser orientados a manter a confidencialidade das informações de autenticação que lhes pertencem.

§ 1º A senha de autenticação deve possuir um padrão mínimo de qualidade de acordo com as regras dispostas em norma

específica, devendo ser alterada toda vez que a sua confidencialidade for comprometida.
§ 2º Os usuários ficam responsáveis pelos danos causados pela divulgação não autorizada das informações de autenticação que lhes pertencem.
§ 3º As informações de autenticação não devem ser anotadas, a menos que seja feito por procedimento seguro e aprovado.
Art. 33. O acesso relacionado aos sistemas corporativos será provido via perfis de trabalho ou autorizado quando possível pelo seu responsável, observando-se o princípio do privilégio mínimo.
Art. 34. O cadastro de usuário interno para utilização dos recursos de TI será realizado pela Unidade Responsável pela Tecnologia da Informação (URTI) mediante requisição do chefe da unidade organizacional.
Art. 35. Encerrado o vínculo funcional ou contratual do usuário com a Administração Municipal, suas credenciais serão imediatamente revogadas, com remoção dos direitos de acesso e adoção de medidas para eliminação, bloqueio ou anonimização dos dados pessoais, conforme a finalidade e as exigências legais.
Art. 36. Serão definidos perímetros de segurança física a partir dos quais devem haver níveis de proteção específicos contra acesso indevido, de acordo com a criticidade dos recursos e dados pessoais que a eles pertencem.
Parágrafo único. Procedimentos para proteção contra acesso físico não autorizado serão estabelecidos de acordo com os perímetros de segurança física definidos, com foco na proteção de dados pessoais.
Art. 37. As áreas destinadas à entrega, recebimento, armazenamento ou transporte de documentos e materiais que contenham dados pessoais deverão ser controladas, monitoradas e, sempre que possível, segregadas das demais áreas restritas.

SEÇÃO XI - Do Tratamento dos Dados Pessoais

Art. 38. A Administração Pública Municipal deverá especificar, de forma clara e objetiva, a finalidade e os métodos utilizados no tratamento de dados pessoais, assegurando transparência e livre acesso às informações.
Art. 39. Somente serão tratados dados pessoais estritamente necessários ao atendimento da finalidade pública e ao desempenho das competências legais e administrativas do Município, observando-se os princípios da necessidade, adequação e minimização.
§ 1º Nas hipóteses em que a Administração Pública Municipal exercer atividades não diretamente vinculadas às suas competências típicas, o tratamento de dados pessoais deverá observar as bases legais previstas na Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).
§ 2º O consentimento do titular só será necessário quando desempenhadas funções atípicas e nas específicas situações em que a Lei Geral de Proteção de Dados Pessoais exigir, sempre de forma livre, informada e inequívoca.
Art. 40. A Administração deverá assegurar a integridade, exatidão e atualização dos dados pessoais tratados, garantindo ao titular o exercício dos direitos de acesso, correção, anonimização, eliminação, portabilidade e demais direitos previstos na legislação aplicável.
Art. 41. A proteção de dados pessoais deverá abranger todos os meios de tratamento, físicos ou digitais, inclusive documentos impressos, arquivos, sistemas, bancos de dados e quaisquer outros suportes informacionais.
Art. 42. É vedado o tratamento de dados pessoais para fins discriminatórios, ilícitos, abusivos ou que atentem contra a dignidade, os direitos e as liberdades fundamentais dos titulares.
Art. 43. Os sistemas, portais e serviços eletrônicos que realizem coleta de dados pessoais deverão disponibilizar termos de uso e políticas de privacidade contendo, de forma destacada, as finalidades do tratamento e os direitos dos titulares.
Art. 44. O compartilhamento de dados pessoais com outros órgãos ou entidades públicas, bem como com entidades privadas, somente poderá ocorrer mediante fundamento legal e formalização por instrumentos jurídicos que estabeleçam responsabilidades, medidas de segurança e garantias de proteção dos dados.
Art. 45. Os sistemas e ambientes tecnológicos utilizados pela Administração deverão adotar medidas técnicas e

administrativas de segurança, tais como criptografia, controle de acesso, gerenciamento de sessões, registros de eventos (logs) e trilhas de auditoria, a fim de prevenir incidentes e permitir a rastreabilidade de operações.

Art. 46. Constatado incidente de segurança que possa acarretar risco ou dano relevante aos titulares de dados pessoais, o Encarregado pelo Tratamento de Dados Pessoais deverá ser imediatamente comunicado para avaliar a extensão do evento e adotar as providências cabíveis, inclusive, quando necessário, a notificação à Autoridade Nacional de Proteção de Dados – ANPD e aos titulares afetados, nos prazos e termos legais.

SEÇÃO XII - Do Correio Eletrônico Institucional

Art. 47. O uso do serviço de correio eletrônico institucional do Município deverá ocorrer exclusivamente para a execução de atividades funcionais, comunicação oficial e desempenho das atribuições administrativas dos órgãos e entidades da Administração Pública Municipal.

Art. 48. Os agentes públicos, servidores efetivos, comissionados, contratados, estagiários e demais colaboradores poderão solicitar à Unidade Responsável pela Tecnologia da Informação o fornecimento de endereço eletrônico institucional para fins de comunicação oficial e exercício de suas funções.

Art. 49. As comunicações realizadas em nome da Administração Pública Municipal deverão, sempre que possível, utilizar exclusivamente endereços eletrônicos institucionais, vedado o uso de contas pessoais para atos administrativos ou troca de informações oficiais.

Art. 50. As mensagens transmitidas entre os servidores deverão, prioritariamente, ter como destinatários endereços institucionais, com o objetivo de garantir rastreabilidade, autenticidade, integridade, segurança da informação e preservação do interesse público.

Art. 51. As regras complementares relativas ao uso seguro do correio eletrônico institucional, incluindo limites de armazenamento, procedimentos de cópia de segurança, padrões de segurança, responsabilidades dos usuários, monitoramento, direitos, deveres e penalidades, serão disciplinadas em norma específica, observadas as disposições legais referentes à proteção de dados pessoais e à segurança da informação.

SEÇÃO XIII - Do Acesso à Internet

Art. 52. Terão acesso à Internet os agentes públicos, servidores, contratados, estagiários e demais colaboradores da Administração Pública Municipal, ficando restritos aos endereços permitidos pelas regras dispostas em norma complementar, com o objetivo de proteger a rede corporativa, os sistemas e os dados institucionais e pessoais tratados pelo Município.

Art. 53. Cabe à Unidade Responsável pela Tecnologia da Informação (URTI) implantar os controles de acesso e mecanismos de auditoria que garantam o monitoramento do acesso à internet pela rede corporativa municipal, sempre em conformidade com a legislação e políticas internas de privacidade.

Art. 54. Os usuários são responsáveis pelos conteúdos dos endereços acessados por eles, bem como por qualquer download que possa comprometer a segurança da rede ou a proteção de dados pessoais.

SEÇÃO XIV - Da Publicação de Informação

Art. 55. A Secretaria de Administração e demais unidades administrativas competentes do Município possuem atribuição para realizar publicações institucionais, divulgação de notícias, informes oficiais e transmissões ao vivo de eventos, sempre em conformidade com a **Lei de Acesso à Informação** e com a **Lei Geral de Proteção de Dados Pessoais**.

Parágrafo único. O Prefeito Municipal poderá autorizar outras unidades administrativas a realizar publicações institucionais e transmissões de eventos oficiais, observadas as diretrizes de segurança da informação, proteção de dados pessoais, privacidade e interesse público.

Art. 56. A utilização de perfis institucionais mantidos em redes sociais ou quaisquer meios digitais de comunicação oficial, com a finalidade de divulgar, compartilhar ou transmitir informações do Município, deverá observar a Política de Proteção de Dados Pessoais e Privacidade, os objetivos estratégicos da Administração Pública Municipal, as políticas de uso das plataformas digitais e os direitos dos titulares de dados.

SEÇÃO XV - Da Segurança em Recursos Humanos

Art. 57. As obrigações contratuais estabelecidas aos novos servidores, estagiários e terceirizados, ou aos que decorrerem

de renovação de contrato, devem estar em consonância com esta Política de Proteção de Dados Pessoais e Privacidade, incluindo cláusulas específicas sobre confidencialidade e tratamento de dados pessoais.

Art. 58. Os servidores, empregados públicos, estagiários, terceirizados e demais colaboradores do Município observarão, no exercício de suas funções, os padrões éticos e legais de conduta inerentes ao serviço público, norteando-se pelos princípios da legalidade, transparência, prudência, integridade profissional e pessoal, dignidade, probidade e lisura na relação entre atividades públicas e privadas, assegurando a preservação da segurança da informação e a proteção de dados pessoais tratados no exercício da função pública.

§ 1º Os agentes públicos e colaboradores deverão conduzir suas atividades de modo a prevenir incidentes de segurança da informação, vazamentos, acessos indevidos ou qualquer violação de dados pessoais, bem como a garantir a continuidade dos serviços públicos.

§ 2º Em caso de desligamento, exoneração, término de estágio ou cessação de vínculo, por iniciativa própria ou da Administração, os direitos de acesso serão removidos e as senhas compartilhadas deverão ser alteradas, com a devida eliminação ou anonimização dos dados pessoais sob sua responsabilidade, conforme a finalidade e prazos legais.

§ 3º Em caso de demissão, as ações de segurança e proteção de dados deverão ser feitas em paralelo ao ato de formalização do desligamento.

CAPÍTULO III – DA GOVERNAÇA

Art. 59. Fica instituído, no âmbito da Administração Pública Municipal, o Comitê de Proteção de Dados Pessoais e Privacidade (CPDPP), de caráter permanente, com a finalidade de formular, acompanhar e conduzir as diretrizes estabelecidas nesta Política, analisar periodicamente sua efetividade, propor normas, procedimentos e mecanismos institucionais de melhoria contínua, bem como assessorar o Encarregado de Dados Pessoais (DPO) e as unidades administrativas responsáveis pela segurança da informação.

§ 1º É de competência do CPDPP a revisão, no máximo a cada 2 (dois) anos ou sempre que se fizer necessário, em função de alterações na legislação pertinente, novas tecnologias ou novos requisitos corporativos, de modo a atender aos novos desafios e oportunidades na proteção de dados.

§ 2º Fica sob a responsabilidade do CPDPP a criação de termos específicos, em norma complementar, que definirão a forma adequada da realização de cópias de segurança dos ativos de informação e dados pessoais pertencentes ao órgão, com especial atenção à proteção e criptografia.

§ 3º A composição, as competências específicas e o regulamento interno do CPDPP serão definidos por ato do Chefe do Poder Executivo Municipal.

Art. 60.O Município designará formalmente um Encarregado de Dados Pessoais (DPO), nos termos da legislação vigente, que atuará como canal de comunicação entre a Administração Pública Municipal, os titulares de dados pessoais e a Autoridade Nacional de Proteção de Dados, competindo-lhe orientar, receber reclamações e comunicações, prestar esclarecimentos, adotar providências e supervisionar o cumprimento desta Política e das normas de proteção de dados pessoais.

CAPÍTULO IV - DAS PENALIDADES

Art. 61. As ações ou omissões que violem esta Política, suas diretrizes, normas ou procedimentos, ou que infrinjam os controles de proteção de dados pessoais, privacidade e segurança da informação deverão ser comunicadas à autoridade administrativa competente ou à unidade responsável pela apuração disciplinar, para fins de instauração do procedimento administrativo cabível.

Parágrafo único. Caberá à autoridade competente aplicar aos responsáveis as penalidades previstas na legislação municipal aplicável ao regime jurídico dos servidores públicos, sem prejuízo de outras sanções administrativas e civis cabíveis, conforme a LGPD.

CAPÍTULO V - DAS DISPOSIÇÕES FINAIS

Art. 62. Os casos omissos serão decididos pela autoridade máxima do Poder Executivo Municipal, mediante consulta ao Comitê de Proteção de Dados Pessoais e Privacidade e ao Encarregado de Dados Pessoais (DPO), quando couber, observadas as normas de proteção de dados, segurança da informação e a legislação vigente.

Art. 63. Este decreto entra em vigor na data de sua publicação.

Gabinete do Prefeito do Município de Ipueira/RN, em 02 de Março de 2026.

ADEMIR JOSÉ DE MEDEIROS
Prefeito Municipal

Publicado por:
Leonardo Cleriston Nóbrega Félix
Código Identificador:EB16943A

Matéria publicada no Diário Oficial dos Municípios do Estado do Rio Grande do Norte no dia 03/03/2026. Edição 3741
A verificação de autenticidade da matéria pode ser feita informando o código identificador no site:
https://www.diariomunicipal.com.br/femurn/