CÂMARA MUNICIPAL DE PATO BRANCO
ATO DA MESA DIRETORA Nº 2, DE 12 DE NOVEMBRO DE 2024.

ATO DA MESA DIRETORA Nº 2, DE 12 DE NOVEMBRO DE 2024.

Institui as políticas de privacidade e proteção de dados pessoaise segurança da informaçãona Câmara Municipal de Pato Branco, em atendimento à Lei Geral de Proteção de Dados Pessoais (Lei Federal nº 13.709/2018).

A Mesa Diretora da Câmara Municipal de Pato Branco, Estado do Paraná, com fundamento no inciso I do art. 30 da Resolução nº 1, de 8 de janeiro de 2014 (Regimento Interno da Câmara Municipal de Pato Branco), e com base na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 2018), resolve:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º Este Ato dispõe sobre a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), no âmbito da Câmara Municipal de Pato Branco.

§ 1º Para os fins deste Ato, adotam-se as terminologias previstas no art. 5º da Lei nº 13.709, de 2018.

§ 2º Fica instituída, no âmbito da Câmara Municipal de Pato Branco, a Política de Privacidade e Proteção de Dados Pessoais, nos termos do Anexo I, com o objetivo de assegurar o cumprimento da Lei Federal nº 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e garantir o adequado tratamento de dados pessoais em todas as suas atividades administrativas e legislativas.

§3º Fica instituída, no âmbito da Câmara Municipal de Pato Branco, a Política de Segurança da Informação, nos termos do Anexo II, com o objetivo de assegurar o cumprimento da Lei Federal nº 13.709, de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), com a finalidade de institui diretrizes, responsabilidades e competências visando a assegurar a confidencialidade, disponibilidade, integridade e autenticidade das informações e comunicações, bem como a conformidade, padronização e normatização das atividades de gestão de segurança da informação e comunicações.

Art. 2º As políticas e diretrizes previstas neste Ato aplicam-se a todos os agentes públicos e prestadores de serviços que, direta ou indiretamente, realizem tratamento de dados pessoais no âmbito da Câmara Municipal.

Art. 3ºEste Ato não se aplica ao tratamento de dados pessoais:

I - realizado por vereadores, lideranças, bancadas, blocos e frentes parlamentares, quando não se utilizar dos sistemas institucionais da Câmara Municipal de Pato Branco;

II - realizado para fins exclusivamente:

a) jornalísticos e artísticos; ou
b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 da Lei Federal nº 13.709, de 2018;

III - realizadas para fins exclusivos de:

a) segurança pública;
b) defesa nacional;
c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais.

Parágrafo único. O vereador será informado, no início de cada Legislatura, das atividades previstas no inciso I, nas quais exercerá as atribuições de controlador de dados pessoais, mediante Termo de Ciência e Responsabilidade, na forma do Anexo III deste Ato.

CAPÍTULO II
DAS DIRETRIZES E PRINCÍPIOS PARA PROTEÇÃO DE DADOS

Art. 4º A Câmara Municipal de Pato Branco compromete-se a observar os princípios da boa-fé, finalidade, adequação, necessidade, segurança, prevenção e transparência no tratamento dos dados pessoais, conforme o disposto no art. 6º da LGPD.

Art. 5º São diretrizes para o cumprimento da política de proteção de dados pessoais:
I - implementação de procedimentos de tratamento de dados pessoais, conforme as Políticas de Privacidade e de Segurança da Informação, abordando as operações de coleta, armazenamento, uso, compartilhamento e descarte, conforme documentos anexos e normativos aplicáveis;
II - capacitação de servidores: promover treinamentos periódicos sobre privacidade e proteção de dados pessoais;
III - nomeação de um Encarregado pelo Tratamento de Dados Pessoais (DPO), com a função de atuar como canal de comunicação com os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD);
IV - adoção de medidas de segurança: implementar procedimentos de proteção contra acesso não autorizado, vazamento de dados e incidentes de segurança, nos termos da Política de Segurança da Informação.

CAPÍTULO III
DAS RESPONSABILIDADES

Art. 6º O Presidente designará o encarregado pelo tratamento de dados pessoais no âmbito da Câmara Municipal de Pato Branco, para os fins do art. 41 da Lei Federal nº 13.709, de 2018.

§ 1º O encarregado deverá possuir conhecimentos multidisciplinares essenciais à sua atribuição, preferencialmente, os relativos aos temas de privacidade e proteção de dados pessoais, análise jurídica, gestão de riscos, governança de dados e acesso à informação no setor público.

§ 2º Será assegurado ao encarregado contínuo aperfeiçoamento dos temas de privacidade e proteção de dados pessoais, observada a disponibilidade orçamentária e financeira da Câmara Municipal de Pato Branco.

§ 3º A identidade e as informações de contato do encarregado serão divulgadas no sítio eletrônico do órgão, em seção específica sobre tratamento de dados pessoais.

Art. 7º Além das atribuições de que trata o § 2º do art. 41 da Lei Federal nº 13.709, de 2018, cabe ao encarregado:
I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências cabíveis;
II - receber comunicações da Autoridade Nacional de Proteção de Dados (ANPD) e adotar providências;
III - orientar os funcionários e os contratados do agente de tratamento a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
IV - prestar assistência e orientação ao agente de tratamento na elaboração, definição e implementação, conforme o caso, de:
a) registro e comunicação de incidente de segurança;
b) registro das operações de tratamento de dados pessoais;
c) relatório de impacto à proteção de dados pessoais;
d) mecanismos internos de supervisão e de mitigação de riscos relativos ao tratamento de dados pessoais;
e) medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito;
f) processos e políticas internas que assegurem o cumprimento da LGPD e dos regulamentos e orientações da ANPD, instrumentos contratuais que disciplinem questões relacionadas ao tratamento de dados pessoais;
g) transferências internacionais de dados;
h) regras de boas práticas e de governança e de programa de governança em privacidade, nos termos do art. 50 da Lei nº 13.709, de 2018;
i) produtos e serviços que adotem padrões de design compatíveis com os princípios previstos na LGPD, incluindo a privacidade por padrão e a limitação da coleta de dados pessoais ao mínimo necessário para a realização de suas finalidades; e
j) outras atividades e tomada de decisões estratégicas referentes ao tratamento de dados pessoais.

V - executar as demais atribuições determinadas pelo agente de tratamento ou estabelecidas em normas complementares.

Parágrafo único. Ao receber comunicações da ANPD, o encarregado deverá adotar as medidas necessárias para o atendimento da solicitação e para o fornecimento das informações pertinentes, adotando, entre outras, as seguintes providências:

I - encaminhar internamente a demanda para as unidades competentes;
II - fornecer a orientação e a assistência necessárias ao agente de tratamento; e
III - indicar expressamente o representante do agente de tratamento perante a ANPD para fins de atuação em processos administrativos, quando esta função não for exercida pelo próprio encarregado.

Art. 8º O encarregado terá acesso irrestrito à todas as operações de tratamento de dados pessoais no âmbito da Câmara Municipal de Pato Branco.

Art. 9º As chefias de unidades organizacionais deverão comunicar ao encarregado:

I - a existência de qualquer tratamento de dados pessoais na unidade administrativa;
II - possível conflito entre a proteção de dados pessoais, o princípio da transparência ou outro interesse público;
III - qualquer outra situação que precise de análise e encaminhamento.

Art. 10. O encarregado comunicará à Diretoria Geral e a Equipe de Gestão de Incidentes a ocorrência de incidente que possa acarretar risco ou dano relevante aos titulares.

Art. 11. Os requerimentos do titular de dados, formulados nos termos do art. 18 da Lei Federal nº 13.709, de 2018, serão direcionados ao encarregado e deverão observar os prazos legalmente previstos.

Art. 12. No atendimento aos requerimentos dos titulares de dados, o encarregado deverá observar a garantia da prevenção à fraude e à segurança do titular de dados.

§ 1º O requerimento somente será atendido mediante apresentação de comprovante de identidade do titular de dados pessoais.

§ 2º No caso de titular incapaz, deverá ser apresentado comprovante de identidade do incapaz e de um dos pais ou responsável legal.

§ 3º O fornecimento de informações relativas a dados pessoais de terceiros a procurador somente será realizado mediante a apresentação de procuração e comprovante de identidade do procurador e do titular de dados.

§ 4º Para fins de comprovação de identidade, referida nos §§ 1º a 3º, será aceita a apresentação de Carteira de Identidade Nacional (CIN), Carteira de Identidade (RG), Carteira Nacional de Habilitação (CNH), passaporte ou documento de identidade emitido por órgão de classe desde que legalmente reconhecidos como documento de identificação.

Art. 13. O Comitê de Privacidade e Proteção de Dados Pessoais (CPPD) expedirá normas ou medidas administrativas necessárias ao cumprimento da Lei nº 13709, de 2018 e deste Ato.

Art. 14. O Comitê de Privacidade e Proteção de Dados (CPPD) terá a seguinte composição:
I - o encarregado pelo tratamento de dados pessoais;
II - um representante da diretoria geral;
III- um representante do departamento administrativo;
IV- um representante do departamento contábil;
V- um representante do departamento de tecnologia da informação;
VI- um representante do departamento de comunicação;
VII- um representante do departamento legislativo;
VIII- um representante da procuradoria jurídica;
IX- um representante da ouvidoria.

Art. 15. Compete ao Comitê de Privacidade e Proteção de Dados (CPPD) a responsabilidade pela governança de privacidade e proteção de dados dentro da organização, provendo orientação e o patrocínio necessários às ações de privacidade, proteção de dados pessoais e segurança da informação na Câmara Municipal Pato Branco, de acordo com os objetivos estratégicos, com as leis e regulamentos pertinentes e:

I - assegurar a implementação e manutenção de programa de governança em privacidade, assegurar o cumprimento das normas relativas à proteção dos dados pessoais, de forma adequada aos objetivos da Lei nº 13709, de 2018;
II - promover a contínua integração entre os processos de gestão da privacidade e proteção de dados, de segurança da informação e de gestão de riscos;
III - identificar os processos de tratamento e proteção de dados pessoais existentes no âmbito da Câmara Municipal de Pato Branco;
IV - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre privacidade e proteção de dados pessoais;
V - participar da atualização da Política de Privacidade, Política de Segurança da Informação, Plano de Resposta à Incidentes e Remediação e das demais normas internas de privacidade, proteção de dados pessoais e segurança da informação, além de propor atualizações e alterações nestes dispositivos;
VI - incentivar e assegurar a conscientização, capacitação e sensibilização das pessoas que desempenham qualquer atividade de tratamento de dados pessoais dentro do órgão;
VII - expedir instruções complementares, no âmbito de suas competências, que detalharão suas particularidades e procedimentos relativos à privacidade e proteção de dados pessoais no âmbito da Câmara Municipal de Pato Branco;
VIII - elaborar e aprovar seu regimento interno, bem como respectivas modificações.

Art. 16. Compete à Diretoria Geral:
I - identificar e avaliar, com apoio do encarregado, os processos de tratamento e proteção de dados pessoais existentes no âmbito da Câmara Municipal de Pato Branco;
II - assegurar o cumprimento das normas relativas à proteção dos dados pessoais, de forma adequada aos objetivos da Lei nº 13.709, de 2018;
III - recomendar à Comissão Executiva as medidas indispensáveis à implementação e ao aperfeiçoamento das normas e procedimentos necessários ao correto cumprimento da Lei nº 13.709, de 2018;
IV - elaborar normas de procedimento necessárias ao cumprimento da Lei nº 13.709de 2018 e deste Ato;
V - encaminhar ao encarregado informações que venham a ser solicitadas pela Autoridade Nacional de Proteção de Dados;
VII - atender as solicitações encaminhadas pelo encarregado buscando cessar eventuais violações à Lei Federal nº 13.709, de 2018 ou apresentar justificativa fundamentada.

Art. 17. A Câmara Municipal de Pato Branco elaborará relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais

Art. 18. Os requerimentos referidos no art.11 deste Ato não se confundem com o pedido de acesso à informação realizado com base na Lei Federal nº nº 12.527, de 18 de novembro de 2011.

CAPÍTULO IV
Das Disposições Finais

Art. 19. Este Ato entra em vigor na data de sua publicação, devendo ser revisado a cada dois anos ou sempre que necessário, conforme regulamentação e orientações da ANPD.

Pato Branco, 12 de novembro de 2024.

(Assinado Digitalmente)

EDUARDO ALBANI DALA COSTA
Presidente

RODRIGO JOSÉ CORREIA
Vice-Presidente

MARIA CRISTINA DE OLIVEIRA RODRIGUES HAMERA
1ª Secretária

ROMULO FAGGION
2º Secretário

ANEXO I
DA POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS

POLÍTICA DE PRIVACIDADE **Câmara Municipal de Pato Branco**	Versão: **1.0**
Nível de confidencialidade: ( ) Público (X) Restrito ( ) Confidencial	Atualização: **12/11/24**

Propósito
Esta Política de Privacidade tem por objetivo estabelecer diretrizes, princípios e conceitos a serem seguidos por todas as pessoas e entidades que se relacionam com Câmara Municipal de Pato Branco que em algum momento realizam operações de tratamento de dados pessoais, visando o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) e outras normas vigentes.
Escopo
Instituir a Política de Privacidade (PP), no âmbito da Câmara Municipal de Pato Branco, com a finalidade de estabelecer princípios e diretrizes para a implementação de ações que garantam a proteção de dados pessoais e, no que couber, no relacionamento com outras entidades públicas ou privadas.
Esta Política regula a proteção de dados pessoais dos quais a Câmara Municipal de Pato Branco atua como agente de tratamento, bem como os meios utilizados para estes tratamentos, sejam digitais ou físicos, além de qualquer pessoa que realize operações de tratamento de dados pessoais em seu nome ou em suas dependências.
Termos e Definições
Agentes de tratamento: o controlador e o operador.
Consentimento: Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
Controlador: pessoa física ou jurídica responsável por iniciar e tomar decisões relacionadas ao tratamento de dados;
Controladoria Conjunta: quando dois ou mais responsáveis pelo tratamento determinam conjuntamente as finalidades e os meios desse tratamento;
Dados Pessoais: referem-se a qualquer informação que, direta ou indiretamente, identifique ou possa identificar uma pessoa natural, como por exemplo, nome, CPF, data de nascimento, endereço IP, dentre outros;
Dados Pessoais Sensíveis: referem-se a qualquer informação que revele, em relação a uma pessoa natural, 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;
Encarregado pelo Tratamento de Dados Pessoais: também conhecido como DPO, é o profissional responsável por atuar como canal de

comunicação entre você, nós e a Autoridade Nacional de Proteção de Dados (ANPD);
Incidente de Segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado a Dados Pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de Tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do Titular dos Dados Pessoais.
Leis de Proteção de Dados: referem-se às disposições legais que regulem o Tratamento de Dados Pessoais, em especial, porém sem se limitar, a Lei Geral de Proteção de Dados Pessoais (Lei Federal nº 13.709/2018, "LGPD");
Operador: pessoa física ou jurídica que processa e trata os dados pessoais sob as ordens do controlador;
Tratamento: significa qualquer operação efetuada com Dados Pessoais, por meios físicos ou digitais, automáticos ou não, tal como 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;
Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

HISTÓRICO DE VERSÕES			
Data	**Versão**	**Descrição**	**Autoria**
10/09/2024	1.0	Política de Privacidade	Luana Varaschim Perin

CAPÍTULO I
DAS DIRETRIZES GERAIS

Art. 1º A Câmara Municipal de Pato Branco se compromete a tratar dados pessoais de acordo a Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), para propósitos legítimos, específicos, explícitos, conforme informados ao titular, em observância às bases legais previstas nas hipóteses dos artigos 7º, 11 e 14 da referida lei.

Art. 2º A Câmara Municipal de Pato Branco deve adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.

Art. 3º A Câmara Municipal de Pato Branco deve manter registro das operações de tratamento de dados pessoais que realizar.

Art. 4º Deve ser elaborado o Relatório de Impacto de Proteção de Dados Pessoais (RIPD) em todo contexto em que as operações de tratamento de dados pessoais possam gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados, atualizando-o quando necessário.

Art. 5º Devem ser estabelecidas revisões periódicas de processos com o objetivo de aferir a diminuição ou aumento de riscos que envolvem o tratamento de dados pessoais.

Art. 6º Os dados pessoais que forem coletados e tratados no site e serviços mantidos pela Câmara Municipal de Pato Branco também devem ser administrados de acordo com as diretrizes desta política.

Art. 7º A Câmara Municipal de Pato Branco poderá utilizar arquivos (cookies) para registrar e gravar no computador do usuário as preferências e navegações realizadas nas respectivas páginas para fins estatísticos e de melhoria dos serviços ofertados, respeitando o consentimento do titular.

Art. 8º A Câmara Municipal de Pato Branco deverá manter atualizados as políticas/avisos de privacidade, que fornecerão informações sobre o tratamento de dados pessoais em cada ambiente físico ou virtual, bem como detalhar as medidas de proteção de dados adotadas para salvaguardar esses dados pessoais.

Art. 9º Será estabelecido o programa de treinamento e conscientização para que os colaboradores entendam suas responsabilidades e

procedimentos na proteção de dados pessoais.

Art. 10.Serão formuladas regras de segurança, de boas práticas e de governança que definam procedimentos e outras ações referentes a privacidade e proteção de dados pessoais.

CAPÍTULO II
TRATAMENTO DE DADOS PESSOAIS

Art. 11. O tratamento de dados pessoais deverá ser realizado para o atendimento de sua finalidade pública, conforme o interesse público, com o objetivo de executar competências legais e de cumprir as atribuições legais do serviço público.

Art. 12. O tratamento de dados pessoais será pautado, ainda, pela boa-fé e pela observância dos princípios previstos no art. 6º da LGPD, quais sejam:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII - segurança: utilização 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;
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Art. 13. A Câmara Municipal de Pato Branco adotará mecanismos para que o titular do dado pessoal usufrua dos direitos assegurados pela LGPD e normativos correlatos, através dos seguintes canais de atendimento:

I - por telefone, através do número (46) 3272-1506;
II - por meio eletrônico, através do e-mail lgpd@patobranco.pr.leg.br.

Art. 14. O tratamento de dados pessoais sensíveis deverá ser realizado somente nos termos da seção II do capítulo II da LGPD e devem ser estabelecidos procedimentos de segurança no tratamento destes dados conforme a LGPD e demais normativos.

Art. 15. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado nos termos da seção III do capítulo II da LGPD, bem como, poderá ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da Lei Geral de Proteção de Dados Pessoais (LGPD), desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei.

Art. 16. O uso compartilhado de dados deverá atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de

proteção de dados pessoais elencados, conforme art. 26 da LGPD bem como sua comunicação estará sujeita ao que consta no art. 27 da mesma lei.

Art. 17. No caso de transferência internacional de dados pessoais deverá ser observado o que consta no Capítulo V da LGPD.

CAPÍTULO III
CONSCIENTIZAÇÃO, CAPACITAÇÃO E SENSIBILIZAÇÃO

Art. 18. As pessoas que possuem acesso aos dados pessoais na Câmara Municipal de Pato Branco devem fazer parte de programas de conscientização, capacitação e sensibilização em matérias de privacidade e proteção de dados pessoais, as quais devem ser adequadas aos papéis e responsabilidades das pessoas.

CAPÍTULO IV
SEGURANÇA E BOAS PRÁTICAS

Art. 19. Qualquer ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos dados pessoais dos titulares deve seguir o Plano de Resposta à Incidentes do órgão e ser comunicada a Autoridade Nacional de Proteção de Dados (ANPD) dentro do prazo previsto pela LGPD.

Art. 20. Serão adotadas as medidas técnicas e organizacionais de privacidade e proteção de dados dispostas a seguir, com o objetivo diminuir ou mitigar a existência incidentes com os dados pessoais do titular:
I - acesso a dados pessoais limitado às pessoas que necessitam do tratamento dos mesmos para o exercício de suas funções;
II - as funções e responsabilidades dos colaboradores envolvidos nos tratamentos de dados pessoais são claramente estabelecidas e comunicadas;
são estabelecidos acordos de confidencialidade, termos de responsabilidade ou termos de sigilo com operadores de dados pessoais;
III - todos os dados pessoais são armazenados em ambiente seguro, de modo que terceiros não autorizados não possam acessá-los.

CAPÍTULO V
AUDITORIA E CONFORMIDADE

Art. 21. O cumprimento desta Política, bem como dos normativos que a complementam devem ser avaliados periodicamente por meio de verificações de conformidade, buscando a certificação do cumprimento dos requisitos de privacidade e proteção de dados pessoais e da garantia de cláusula de responsabilidade e sigilo constantes de termos de responsabilidade, contratos, convênios, acordos e instrumentos congêneres.

Art. 22. As atividades, produtos e serviços desenvolvidos na Câmara Municipal de Pato Branco devem estar em conformidade com requisitos de privacidade e proteção de dados pessoais constantes de leis, regulamentos, resoluções, normas, estatutos e contratos jurídicos vigentes.

Art. 23. Os resultados de cada ação de verificação de conformidade devem ser documentados em relatório de avaliação de conformidade.

CAPÍTULO VI
FUNÇÕES E RESPONSABILIDADES

Art. 24. Qualquer pessoa natural ou jurídica de direito público ou privado que tenha interação em qualquer fase do tratamento de dados pessoais deve garantir a privacidade e a proteção de dados pessoais, mesmo após o término do tratamento, observando as medidas técnicas e administrativas determinadas pela organização.

Art. 25. Compete ao Comitê de Privacidade e Proteção de Dados (CPPD) a responsabilidade pela governança de privacidade e da LGPD dentro da organização, provendo orientação e o patrocínio necessários às ações de privacidade, proteção de dados pessoais e segurança da informação na Câmara Municipal de Pato Branco, de

acordo com os objetivos estratégicos e com as leis e regulamentos pertinentes e:
I - assegurar a implementação e manutenção de programa de governança em privacidade;
II - promover a contínua integração entre os processos de gestão da privacidade, de segurança da informação e de gestão de riscos;
III - revisar e aprovar o tratamento de dados pessoais, seguindo o Procedimento para Aprovação de Tratamento de Dados Pessoais;
IV - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre privacidade e proteção de dados pessoais;
V - participar da elaboração da Política de Privacidade, Política de Segurança da Informação e das demais normas internas de privacidade, proteção de dados pessoais e segurança da informação, além de propor atualizações e alterações nestes dispositivos;
VI - incentivar e assegurar a conscientização, capacitação e sensibilização das pessoas que desempenham qualquer atividade de tratamento de dados pessoais dentro da Câmara Municipal de Pato Branco;
VII - elaborar e aprovar seu regulamento, bem como respectivas modificações.

Art. 26. O Comitê de Privacidade e Proteção de Dados (CPPD) terá a seguinte composição:
I - o encarregado pelo tratamento de dados pessoais;
II - um representante da diretoria geral;
III - um representante do departamento administrativo;
IV - um representante do departamento contábil;
V - um representante do departamento de tecnologia da informação;
VI - um representante do departamento de comunicação;
VII - um representante do departamento legislativo;
VIII - um representante da procuradoria jurídica;
IX - um representante da ouvidoria.

Art. 27. A presidência do Comitê de Privacidade e Proteção de Dados (CPPD) será exercida pelo representante da Diretoria Geral da Câmara Municipal de Pato Branco.

Art. 28. A responsabilidade pelas decisões relacionadas ao tratamento de dados pessoais é da Câmara Municipal de Pato Branco que no exercício das atribuições típicas de controlador determina as medidas necessárias para executar a Política de Privacidade dentro de sua estrutura organizacional.

Art. 29. São atribuições do controlador:
I - observar os fundamentos, princípios da privacidade e proteção de dados pessoais e os deveres impostos pela LGPD e por normativos correlatos no momento de decidir sobre um futuro tratamento ou realizá-lo;
II - considerar o preconizado pelos art. 7º, art. 11 e art. 23 e seguir o procedimento para aprovação de tratamento de dados pessoais antes de realizar o tratamento de dados pessoais;
III - cumprir o previsto pelos art. 46 e art. 50 da LGPD buscando à proteção de dados pessoais e sua governança;
IV - indicar um encarregado pelo tratamento de dados pessoais, divulgando a identidade e as informações de contato do encarregado de forma clara e objetiva, preferencialmente no sítio institucional;
V - elaborar e manter atualizado o inventário de dados pessoais a fim de manter registros das operações de tratamento de dados pessoais;
VI - reter dados pessoais somente pelo período necessário para o cumprimento da hipótese legal e finalidade utilizadas como justificativa para o tratamento de dados pessoais;
VII - criar e manter atualizados os avisos ou políticas de privacidade, que informarão sobre os tratamentos de dados pessoais realizados em cada ambiente físico ou virtual, e como os dados pessoais neles tratados são protegidos.

Parágrafo único. É vedado qualquer tratamento de dados pessoais para fins não relacionados com as atividades desenvolvidas pela organização ou por pessoa não autorizada formalmente por esta Câmara Municipal de Pato Branco.

Art. 30. São considerados operadores de dados pessoais as pessoas naturais ou jurídicas de direito público ou privado que realizam operações de tratamento de dados pessoais em nome do controlador.

Parágrafo único. Qualquer fornecedor de produtos ou serviços, que por algum motivo, realiza o tratamento de dados pessoais a eles confiados, são considerados operadores e devem seguir as diretrizes estabelecidas nesta política, em especial o capítulo VII.

Art. 31. São atribuições do operador:
I - observar os princípios estabelecidos no Art. 6º da LGPD, ao realizar tratamento de dados pessoais.
II - seguir as diretrizes estabelecidas pelo controlador;
III - antes de efetuar o tratamento, verificar se as diretrizes estabelecidas pelo controlador cumprem os requisitos legais presentes nos art. 7º, art. 11 e art. 23 da LGPD.

Parágrafo único. É proibida a decisão unilateral do operador quanto aos meios e finalidades utilizados para o tratamento de dados pessoais.

Art. 32. São atribuições do encarregado de proteção de dados:
I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências cabíveis;
II - receber comunicações da ANPD e adotar providências;
III - orientar os funcionários e os contratados do agente de tratamento a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
IV - prestar assistência e orientação ao agente de tratamento na elaboração, definição e implementação, conforme o caso, de:

a) registro e comunicação de incidente de segurança;
b) registro das operações de tratamento de dados pessoais;
c) relatório de impacto à proteção de dados pessoais;
d) mecanismos internos de supervisão e de mitigação de riscos relativos ao tratamento de dados pessoais;
e) medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito;
f) processos e políticas internas que assegurem o cumprimento da LGPD e dos regulamentos e orientações da ANPD, instrumentos contratuais que disciplinem questões relacionadas ao tratamento de dados pessoais;
g) transferências internacionais de dados;
h) regras de boas práticas e de governança e de programa de governança em privacidade, nos termos do art. 50 da Lei nº 13.709, de 14 de agosto de 2018;
i) produtos e serviços que adotem padrões de design compatíveis com os princípios previstos na LGPD, incluindo a privacidade por padrão e a limitação da coleta de dados pessoais ao mínimo necessário para a realização de suas finalidades; e
j) outras atividades e tomada de decisões estratégicas referentes ao tratamento de dados pessoais.

V - executar as demais atribuições determinadas pelo agente de tratamento ou estabelecidas em normas complementares.

Parágrafo único. Ao receber comunicações da ANPD, o encarregado deverá adotar as medidas necessárias para o atendimento da solicitação e para o fornecimento das informações pertinentes, adotando, entre outras, as seguintes providências:
I - encaminhar internamente a demanda para as unidades competentes;
II - fornecer a orientação e a assistência necessárias ao agente de tratamento; e
III - indicar expressamente o representante do agente de tratamento perante a ANPD para fins de atuação em processos administrativos, quando esta função não for exercida pelo próprio encarregado.

CAPÍTULO VII
GESTÃO DE TERCEIROS

Art. 33. Os contratos, convênios, acordos e instrumentos similares que de alguma forma envolvam o tratamento de dados pessoais devem incorporar cláusulas específicas em total conformidade com a presente Política de Privacidade e que contemplem:
I - definição dos agentes de tratamento;

II - determinação de que o operador não processe os dados pessoais para finalidades que divergem da finalidade principal informada pelo controlador;
III - requisitos mínimos de segurança da informação;
IV - restrição ao compartilhamento de dados não previamente autorizado;
V - dever de cooperação para atendimento aos direitos dos titulares e à ANPD;
VI - dever de comunicação e coordenação em incidentes.
VII - condições sob as quais o operador deve devolver ou descartar com segurança os dados pessoais após a conclusão do serviço, rescisão de qualquer contrato ou de outra forma mediante solicitação do controlador;
VIII - diretrizes especificas sobre o uso de subcontratados pelo operador para execução contratual que envolva tratamento de dados pessoais;
IX - autorização de auditorias pelo permite que o controlador verifique o cumprimento das obrigações pelo operador contratado.

Art. 34. São adotadas medidas rigorosas com o propósito de assegurar que os terceiros e operadores de dados pessoais contratados estão plenamente em conformidade com as cláusulas contratuais estabelecidas no momento da celebração do acordo entre as partes envolvidas.

CAPÍTULO VIII
DA CONSERVAÇÃO E ELIMINAÇÃO

Art. 35. Os dados pessoais serão eliminados após o término de seu tratamento nos prazos previstos na Tabela de Temporalidade e segundo as instruções contidas na Política de Segurança da Informação, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:
I - cumprimento de obrigação legal ou regulatória pelo controlador;
II - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

Parágrafo único. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:
I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
II - fim do período de tratamento;
III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, resguardado o interesse público devidamente justificado e autorizado pelo Comitê de Privacidade e Proteção de Dados (CPPD); ou
IV - determinação da Autoridade Nacional de Proteção de Dados Pessoais.

CAPÍTULO IX
PENALIDADES

Art. 36. Ações que violem esta Política de Privacidade poderão acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 37. Casos de descumprimento desta Política de Privacidade deverão ser registrados e comunicados ao(à) Presidente da Câmara Municipal de Pato Branco para ciência e tomada das providências cabíveis.

CAPÍTULO X
DISPOSIÇÕES FINAIS

Art. 38. Os integrantes do Comitê de Privacidade e Proteção de Dados (CPPD) poderão expedir instruções complementares, no âmbito de suas competências, que detalharão suas particularidades e procedimentos relativos à Proteção de Dados Pessoais alinhados às diretrizes emanadas pelo CPPD e aos respectivos Planos Estratégicos Institucionais da Câmara Municipal de Pato Branco.

Art. 39. Dúvidas sobre a Política de Privacidade e seus documentos devem ser submetidas ao Comitê de Privacidade e Proteção de Dados (CPPD).

Art. 40. Esta política deverá ser revisada bianualmente a partir do início de sua vigência.

Art. 41. Os casos omissos serão resolvidos pelo Comitê de Privacidade e Proteção de Dados (CPPD).

Art. 42. Esta Política de Privacidade entra em vigor na data de sua publicação.

ANEXO II
DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO **Câmara Municipal de Pato Branco**	Versão: **1.0**
Nível de confidencialidade: ( ) Público (X) Restrito ( ) Confidencial	Atualização: 12/11/24

SUMÁRIO

HISTÓRICO DE VERSÕES			
Data	**Versão**	**Descrição**	**Autoria**
11/09/2024	1.0	Política de Segurança da Informação	Luana Varaschim Perin

1. DOS OBJETIVOS

1.1 A Política de Segurança da Informação (POSIN) institui diretrizes, responsabilidades e competências visando a assegurar a confidencialidade, disponibilidade, integridade e autenticidade das informações e comunicações, bem como a conformidade, padronização e normatização das atividades de gestão de segurança da informação e comunicações no âmbito da Câmara Municipal de Pato Branco.

2. DA ABRANGÊNCIA

2.1 Ficam submetidos a esta Política de Segurança da Informação todos os servidores, colaboradores, estagiários, prestadores de serviços e demais agentes públicos ou privados que tenha qualquer tipo de acesso aos dados ou informações oriundas da Câmara Municipal de

Pato Branco, sob pena de responsabilidade, conforme previsto na legislação brasileira.

3. DOS TERMOS E DEFINIÇÕES

Agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública e equipara-se a agente público quem trabalha para empresa prestadora de serviços contratada ou conveniada para a execução de atividade, de qualquer natureza, desenvolvida na Câmara Municipal de Pato Branco;

Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

Áreas restritas: são locais dentro da Câmara Municipal de Pato Branco onde o acesso é controlado e limitado a pessoas autorizadas, devido à natureza sensível ou crítica das atividades ou informações ali presentes. Essas áreas incluem: sala de servidores, arquivos, salas de segurança, áreas com equipamentos críticos, centros de processamento de dados, etc.

Ativo: qualquer bem, tangível ou intangível, que tenha valor para a organização;

Ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

Backup: é a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados;

Confidencialidade: é a garantia de que a informação é acessível somente a pessoas com acesso autorizado;

Integridade: é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;

Disponibilidade: garante que as informações e recursos estejam disponíveis quando necessários.

Firewall: É um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede;

Incidente de segurança da informação: evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de informação, de computação ou das redes de computadores;

Mídias Removíveis: Dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Disquete, Pen Drive, cartão de memória entre outros;

Modem 3G: É um dispositivo sem fio, com saída USB para conexão em outro dispositivo tais como Tablets (com suporte 3G), notebooks, netbooks, desktops, etc. objetivando conexão com a internet. O modem 3G recebe e decodifica o sinal digital de alta velocidade transmitido pelas operadoras de celulares para aparelhos portáteis (celulares, smartphones e notebooks) compatíveis com a tecnologia 3G;

Software: É a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores. Toda interação dos usuários de computadores é realizada através de softwares;

TI: Tecnologia da Informação.

4. NÍVEIS DE CONFIDENCIALIDADE DE INFORMAÇÕES E DOCUMENTOS

4.1 As informações e documentos existentes são classificadas de acordo com os seguintes níveis de confidencialidade:

Público: É uma informação ou documento da Câmara Municipal de Pato Branco com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter legal, informativo, educativo ou promocional. É destinada ao público externo ou cidadãos ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma.

Restrito: É uma informação ou documento da Câmara Municipal de Pato Branco que o órgão não tem obrigação legal de divulgar, onde o acesso por parte de indivíduos externos à organização deve ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem da organização, porém, não com a mesma magnitude de uma informação confidencial. Pode ser acessada sem restrições por todos os agentes públicos da Câmara Municipal de Pato Branco.

Confidencial: É uma informação crítica que está acessível apenas a servidores ou agentes públicos previamente definidos, sempre associados aos interesses estratégicos da Câmara Municipal de Pato Branco. É sempre restrita a um grupo específico de pessoas. Dados Pessoais, ou seja, toda informação relacionada a pessoa natural identificada ou identificável, neste contexto aplicável também à dados pessoais sensíveis, isto é, toda informação 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, são informações confidenciais.

5. ATRIBUIÇÕES E RESPONSABILIDADES NA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Cabe a todos os agentes públicos:
Cumprir fielmente esta Política;
Buscar orientação do gestor imediato em caso de dúvidas relacionadas à segurança da informação;
Proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados;
Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo órgão;
Comunicar imediatamente o órgão quando do descumprimento ou violação desta política, através da Ouvidoria.

Cabe às Diretorias, Gerências e Coordenações:
Cumprir, disponibilizar os recursos e orçamento necessários e fazer cumprir esta Política;
Assegurar que suas equipes possuam acesso e conhecimento desta Política de Segurança da Informação;
Comunicar imediatamente eventuais casos de violação de segurança da informação à Ouvidoria.

Cabe ao Comitê de Privacidade e Proteção de Dados:
Propor ajustes, melhorias, aprimoramentos e modificações desta Política;
Convocar, coordenar, lavrar atas e prover apoio às reuniões que discutam a respeito desta Política;
Prover todas as informações de gestão de segurança da informação solicitadas por Gestores;
Observar o Plano de Resposta à Incidentes e Remediação e servir como equipe para execução do mesmo.

6. PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

6.1 As normas e procedimentos que complementam esta Política de Segurança da Informação abordam a segurança física e lógica, conforme os aspectos a seguir:
Segurança do Ambiente Físico;
Segurança do Ambiente Lógico:
Acesso à Rede;
Estação de Trabalho;
Uso da Internet;
Controles de Acesso;
Credenciais de Acesso e Senhas;
Backups (Cópias de Segurança)
Programas
Equipamentos Particulares e Dispositivos Móveis;
Dos Usos de Computação em Nuvem;
E-mail Corporativo;
Mídias Removíveis e Portas USB.
6.2 O órgão deverá assegurar que todas as transferências internacionais de dados pessoais sejam realizadas em conformidade com Procedimento para Transferência Internacional de Dados.

7. DA SEGURANÇA DO AMBIENTE FÍSICO

7.1. Disposições Gerais

A segurança física se baseia no acesso físico das pessoas aos ambientes que possuam equipamentos de tecnologia da informação e/ou tratem ou armazenem informações e tem como escopo garantir a proteção da informação contra violações e acessos não autorizados, permitindo a circulação apenas de pessoas treinadas, capacitadas e autorizadas.

7.2 Controle de Acesso Físico

Toda e qualquer pessoa que necessitar ingressar na Câmara Municipal de Pato Branco, além do Plenário e das áreas destinadas ao atendimento ao público, deverá ser devidamente identificada nas áreas de recepção. O acesso deve ser concedido apenas para finalidades específicas e autorizadas.
Todo e qualquer acesso de terceiros às dependências internas da Câmara Municipal de Pato Branco deverá ser acompanhado durante toda sua permanência por um servidor do órgão.
É vedada a entrada de qualquer pessoa não autorizada nas dependências internas da Câmara Municipal de Pato Branco.
O acesso às dependências da Câmara Municipal de Pato Branco com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar fora do ambiente da Plenária e saguão só pode ser feito a partir de autorização expressa da Diretoria Geral ou Presidência e mediante supervisão, exceto para eventos e treinamentos organizados pelo próprio órgão.
O acesso às áreas restritas é franqueado apenas aos agentes públicos autorizados da Câmara Municipal de Pato Branco, devendo ser protegido a evitar acesso não autorizado.
Deve ser mantido registro detalhado de todos os acessos físicos às áreas restritas, incluindo data, hora e identidade do indivíduo que acessou as instalações.

7.3 Ameaças Ambientais
Compete ao Departamento de Administração assegurar o funcionamento adequado do suprimento de energia elétrica, telecomunicações e ar-condicionado, protegidos contra incêndios e alagamentos.
Os locais que armazenem informações restritas devem estar equipados com sistemas de detecção e combate a incêndios adequados, incluindo alarmes, extintores de incêndio e, quando necessário, sistemas de supressão de incêndios que não danifiquem equipamentos eletrônicos.
As salas de servidores e outros locais críticos devem ter sistemas de controle ambiental para manter níveis adequados de temperatura e umidade, prevenindo danos aos equipamentos e dados.
Áreas de armazenamento de dados e equipamentos essenciais devem ser protegidas contra inundações, com medidas como instalação de barreiras físicas e sistemas de drenagem adequados.
Todos os sistemas de proteção ambiental devem ser sujeitos a manutenção preventiva regular, garantindo que estejam sempre operacionais e eficientes.

7.4 Gestão de Ativos Físicos
Deverá ser mantido e atualizado regularmente inventário completo de todos os ativos físicos que armazenam ou processam informações restritas.
Equipamentos que armazenem informações restritas devem ser descartados de maneira segura, utilizando métodos de destruição que garantam que os dados não possam ser recuperados.
Os documentos impressos e anotações que precisem estar em um papel devem permanecer nas mesas em caráter temporário devendo ser recolhidos em compartimentos fechados disponíveis em seu departamento ou qualquer dependência da organização que forneça segurança e proteção a esses materiais.
Toda informação que permanecer nas mesas poderá e deverá ser destruída pelo agente público responsável ou por qualquer outro agente público que assim o quiser fazê-lo exercitando as boas práticas de proteção de informações da organização.
Os documentos órfãos notoriamente importantes (que possuem assinaturas, por exemplo) deverão ser depositados em um armário ou gaveta designada pelo Departamento de Administração para que possam ser revisados posteriormente antes de sua destruição segura.

8. DA SEGURANÇA DO AMBIENTE LÓGICO
8.1 Disposições Gerais
Todo acesso às informações e aos ambientes lógicos deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas. As autorizações devem ser revistas, confirmadas e registradas continuadamente. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado. Os dados, as informações e os sistemas de informação da entidade devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, confidencialidade e disponibilidade desses bens.

8.2 Estações de Trabalho

Constituem estações de trabalho os computadores e notebooks registrados como patrimônio do órgão e utilizados pelos servidores no desempenho de suas atividades funcionais. As seguintes medidas de segurança que devem ser adotadas quanto à utilização das estações de trabalho:

Tudo que for executado na estação de trabalho é de responsabilidade do agente público a quem pertence;

Fica proibida a instalação, modificação ou desinstalação de hardwares e softwares sem a autorização do Setor de Tecnologia da Informação. Qualquer software que, por necessidade do serviço, necessitar ser instalado deverá ser comunicado ao Setor de Tecnologia da Informação, para que o mesmo possa ser homologado e disponibilizado para a área requerente;

Somente devem ser utilizados softwares devidamente licenciados;

Ao se ausentar da estação de trabalho, o agente público deve efetuar o bloqueio ou "logoff" da mesma, evitando assim o acesso indevido de outra pessoa à estação de trabalho através do seu usuário (login);

O acesso à estação de trabalho deverá ser encerrado no final do expediente, desligando-se o equipamento;

As estações de trabalho devem sofrer bloqueio automático depois de 10 minutos de inatividade;

As configurações de segurança de estações de trabalho não devem ser alteradas, desativadas ou ignoradas pelo agente público;

Informações restritas, confidenciais ou cuja divulgação possa causar ao órgão só devem ser manipuladas em equipamentos com controles adequados;

A liberação do dispositivo móvel (notebook, tablets ou celulares) será permitida após os solicitantes assinarem o acordo de conhecimento das suas responsabilidades;

Em caso de furto/roubo ou perda do dispositivo móvel, o servidor deverá comunicar imediatamente à Diretoria Geral, bem como deverá ser tal fato registrado em boletim de ocorrência junto às autoridades policiais;

As estações de trabalho devem ser utilizadas somente para o exercício funcional;

A proteção antivírus das estações de trabalho devem ser atualizadas regularmente;

A varredura por vírus é dever do agente público e deverá ser constantemente executada nas estações e nos servidores.

8.3 Equipamentos Particulares e Dispositivos Móveis

Ficam estabelecidas as seguintes regras para o uso de equipamentos particulares e de dispositivos moveis:

A liberação para utilização de notebooks e para acesso à internet do órgão se dará mediante solicitação justificada e assinatura do termo de compromisso, vide anexo I;

É proibida a inclusão de smartphones na rede corporativa, a inclusão desses equipamentos se dará conforme disposto nesta Política.

Os dispositivos de usuário final utilizados pelo órgão deverão ter criptografia implementada para proteger os dados armazenados contra acessos não autorizados. A criptografia deverá seguir as melhores práticas do mercado e estar em conformidade com as normativas de segurança vigentes.

Os dispositivos móveis adquiridos pelo órgão deverão ser configurados para ocorrer o bloqueio automático após 2 minutos de inatividade.

8.4 Mídias Removíveis e Portas USB

O uso de mídias removíveis não órgão não é estimulado, devendo ser tratado como exceção à regra.

É vedada a transferência de informações das estações de trabalho para dispositivos de armazenamento externo, como pendrives e discos rígidos externos, sem a autorização da Diretoria Geral.

Os usuários de mídias removíveis são diretamente responsáveis pelos riscos e impactos que o uso de tais dispositivos possa vir a causar nos ativos de informação, pois este tipo de mídia pode conter vírus e softwares maliciosos que podem danificar e corromper dados, além de serem passíveis de extravio.

É vedado aos agentes públicos utilizarem as mídias removíveis como meio preferencial de armazenamento de informações corporativas.

8.5 Acesso à Rede

Os agentes públicos terão acesso única e exclusivamente àqueles recursos da rede corporativa que lhe forem indispensáveis à realização de suas atividades.
Os serviços e sistemas autenticados serão disponibilizados para os usuários registrados e identificados pelo seu login e senha.
Cada unidade de lotação terá uma unidade de armazenamento em rede para os usuários lotados na respectiva área de atuação, com acesso de leitura e gravação.
O órgão disponibilizará o acesso à rede de internet sem fio (Wi-Fi) a seus visitantes e agentes públicos, o ingresso a rede se dará mediante cadastro quando solicitado o acesso. A rede de internet sem fio (Wi-Fi) será segregada, garantido assim o isolamento da rede interna do órgão.
Material sexualmente explícito não pode ser acessado, exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede corporativa.
Não é permitida a gravação de arquivos particulares (músicas, filmes, fotos, etc..) nos drivers de rede.

8.6 Uso da Internet
A concessão de acesso à internet em ambiente laboral na Câmara Municipal de Pato Branco será disponibilizada como ferramenta de trabalho destinada ao atendimento das finalidades institucionais do órgão.
O uso da internet no órgão poderá ser monitorado e os acessos serão registrados em dispositivo ou sistema computacional que assegure a possibilidade de rastreio e apuração de responsabilidades em caso de incidentes cibernéticos, incidentes de segurança e outras violações à esta Política.
Para apuração das quebras de segurança de que trata o *caput*, os ativos de informação fornecidos pelo órgão poderão ser analisados, a qualquer tempo, pelo Departamento de Tecnologia da Informação.
O uso de Internet deve ocorrer apenas através da arquitetura segura definida pelo Setor de Tecnologia da Informação, devendo ser acessada por meio da rede local da organização com a infraestrutura adequada e proteção do firewall.
Deverão ser utilizadas conexões cifradas (TLS/HTTPS) ou aplicativos com criptografia ponta-a-pronta para serviços de comunicação.
Fica proibido ao agente público alterar as configurações do navegador da sua estação de trabalho no que diz respeito aos parâmetros de segurança. Havendo necessidade, o Setor de Tecnologia da Informação deve ser acionado para informar o procedimento a ser seguido.
O acesso às páginas e websites é de responsabilidade de cada usuário ficando vedado o acesso a sites com conteúdos impróprios e de relacionamentos.
O agente público deve se certificar da procedência do site e a utilização de conexões seguras (criptografadas) ao realizar transações via internet.
O agente público deve verificar se o certificado do site ao qual se deseja acessar é íntegro e corresponde realmente aquele site, observando ainda, se o mesmo está dentro do prazo de validade.
O agente público deve certificar que o endereço apresentado no navegador corresponde ao sítio que realmente quer acessar, antes de realizar qualquer ação ou transação.
O agente público deve digitar no navegador o endereço desejado e não utilizar links como recurso para acessar um outro endereço destino.
O acesso à internet poderá ser monitorado pelo Setor de Tecnologia da Informação.
É vedada a transferência ou cópia de arquivos de vídeo, som, ou quaisquer outros tipos de arquivos que não sejam relacionados aos interesses do órgão.

8.7 Controle de Acesso
Os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas por usuários autorizados, concedendo-se permissão apenas aos recursos necessários e indispensáveis ao desempenho de suas funções, definidas pela chefia imediata aplicando-se o princípio do menor privilégio (*need to know*). O responsável pela autorização deve ser claramente definido e ter registrado a aprovação concedida.
Todo usuário deverá possuir identificação pessoal e intransferível, qualificando-o, inequivocamente, como responsável por qualquer atividade desenvolvida sob essa identificação.

8.8 Credenciais de Acesso e Senhas

Todo agente público deve ter uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação.

É dever do agente público manter sigilo e trocar periodicamente a senha pessoal de acesso aos sistemas do órgão, bem como não divulgar a terceiros suas credenciais, além de não utilizar a identificação de acesso e senha de terceiros.

É dever do agente público utilizar senha de qualidade, com pelo menos oito caracteres contendo números, letras (maiúsculas e minúsculas) e caracteres especiais (símbolos). Não deverão ser utilizadas informações pessoais fáceis de serem obtidas como o nome, o número de telefone ou data de nascimento como senha.

A senha inicial, quando gerada pelo sistema, deve ser trocada pelo agente público no primeiro acesso.

As credenciais de acesso não podem ser deixadas em notas postadas sobre ou sob as estações de trabalho, nem escritas em locais acessíveis a terceiros.

É obrigatório o uso de autenticação multifator (2FA ou MFA; Two factor Authentication ou MultiFactor Authentication) para todos os serviços onde a opção estiver disponível.

8.9 E-mail Corporativo

O serviço de correio eletrônico (e-mail corporativo) é permitido somente para as atividades profissionais de seus usuários, não sendo permitido enviar ou arquivar mensagens que não estejam relacionadas ao atendimento das finalidades institucionais do órgão ou que:

Contenham assuntos que provoquem assédio, perturbação a outras pessoas ou que prejudiquem a imagem do Iprev/DF;

Contenham temas difamatórios, discriminatórios, calunioso, degradante, ofensivo, violento, ameaçador, material obsceno, material pornográfico, ilegal ou antiético;

Contenham fotos, imagens, sons ou vídeos que não tenham relação com as finalidades institucionais do órgão;

Compartilhem arquivos com códigos executáveis (.exe, .cmd, .pif, .js, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que possa apresentar risco a segurança da informação do órgão.

É vedada a instalação ou utilização de outras soluções de e-mail que não as oficialmente disponibilizadas pelo Setor de Tecnologia da Informação.

8.10 Aplicativos de Mensageria

É vedado o envio de documentos com informações restritas e/ou confidenciais através de aplicativos de mensageria não autorizados ou sem criptografia adequada (como WhatsApp, por exemplo). Em vez disso, deve-se utilizar canais de comunicação seguros, aprovados pelo Setor de Tecnologia da Informação, que garantam a proteção dos dados em trânsito e estejam em conformidade tanto com a Política de Privacidade quando esta Política.

8.11 Backups (Cópias de Segurança)

Os procedimentos de backup deverão ser fixados por norma interna de segurança da informação do órgão.

O serviço de backup deverá ser automatizado por sistemas informacionais próprios, considerando, inclusive, a execução agendada fora do horário de expediente.

A solução de backup deverá ser testada regularmente e mantida sempre atualizada, considerando suas diversas características, tais como atualizações de correção, novas versões, ciclo de vida, garantia, melhorias, entre outros.

O órgão deve possuir pelo menos 3 cópias dos dados, armazená-las em pelo menos 2 tipos de mídia diferentes e manter pelo menos 1 das cópias em um local fora das dependências da Câmara Municipal de Pato Branco.

8.12 Gestão de Ativos Digitais

Não poderão ser executados softwares que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilidade de serviços.

Não poderão ser executados programas, instalados equipamentos, armazenados arquivos ou promovidas ações que possam facilitar o acesso de usuários não autorizados à rede corporativa do órgão.

Deverá ser realizada a desinstalação ou desativação periódica de serviços desnecessários nos ativos e softwares do órgão, garantindo que apenas os serviços essenciais para o funcionamento das atividades permaneçam ativos. Esta prática deve ser revisada regularmente para assegurar a otimização da segurança dos sistemas.
O órgão deverá garantir a implementação de mecanismos de coleta de logs do provedor de serviços, incluindo a captura de eventos de autenticação e autorização. Esses logs deverão ser armazenados de forma segura e analisados regularmente para detecção de atividades suspeitas ou não autorizadas.
O órgão deverá implementar um processo semanal para a identificação e tratamento de ativos não autorizados, garantindo a remoção ou regularização desses ativos conforme as políticas internas estabelecidas. Este processo incluirá a atualização contínua do inventário de ativos e a validação de suas autorizações. Qualquer exceção deverá ser formalmente documentada e aprovada pela equipe responsável pela segurança da informação.

8.13 Dos Uso de Computação em Nuvem
A implementação ou contratação de computação em nuvem deverá estar em conformidade com as diretrizes desta Política e com a legislação sobre contratação vigente no órgão.
O uso de recursos de computação em nuvem para suprir demandas de transferência e armazenamento de documentos, processamento de dados, aplicações, sistemas e demais tecnologias da informação será regido por norma interna de segurança da informação que deverá ser instituída pela unidade responsável pelos ativos de tecnologia e atenderá às determinações desta Política.
Fica vedado o uso de recurso de computação em nuvem não disponibilizado pelo órgão para o armazenamento de ativo de informação institucional.
O uso da computação em nuvem deverá promover:
melhorias no ambiente computacional do órgão;
facilidade e agilidade na implementação;
diminuição de vulnerabilidades pela atualização constante de aplicações defasadas;
possibilidade de integração à outras soluções;
melhoria da gestão da segurança da informação; e
redução de custos.

9. DA CONSERVAÇÃO E ELIMINAÇÃO
Os prazos de guarda da documentação contendo Informações Restritas e Confidenciais devem seguir estritamente a Tabela de Temporalidade do órgão.
Após o término do prazo de guarda estabelecido na Tabela de Temporalidade, as Informações Restritas e Confidenciais devem ser descartadas de forma segura e irreversível, garantindo que não possam ser recuperadas ou identificadas.
O descarte de Informações Restritas e Confidenciais contidas em documentos físicos deve ser realizado por meio de trituração ou incineração, de forma que os dados não possam ser reconstruídos.
Para documentos eletrônicos, deve-se utilizar técnicas de exclusão segura que garantam a impossibilidade de recuperação dos dados, tais como a sobrescrita de dados ou a destruição física dos dispositivos de armazenamento.
Todos os processos de descarte de Informações Restritas e Confidenciais devem ser devidamente documentados, incluindo a data, o método de descarte e o responsável pela execução.
É responsabilidade de todos os agentes públicos garantirem que o descarte de Informações Restritas e Confidenciais seja realizado de acordo com esta Política e com a Tabela de Temporalidade.
Qualquer incidente ou não conformidade relacionada ao descarte de Informações Confidenciais envolvendo Dados Pessoais deve ser reportado imediatamente ao Encarregado pelo Tratamento de Dados Pessoais para a devida investigação e correção.

10. DA GESTÃO DE INCIDENTES
10.1 O órgão deverá estabelecer e manter um Plano de Respostas a Incidentes que inclua a designação de uma equipe de gestão de incidentes, composta por agentes públicos designados. O plano deverá abranger funções e responsabilidades, requisitos de conformidade e estratégias de comunicação. Além disso, deverá ser implementado um processo contínuo para atualizar as informações de contato relevantes para a comunicação durante incidentes de segurança, bem como a

realização de exercícios regulares de resposta a incidentes para testar a eficácia dos canais de comunicação e dos recursos técnicos. Após a resolução de cada incidente, deverá ser realizada uma análise pós-incidente para identificar lições aprendidas e definir ações de acompanhamento necessárias.

11. DAS CONDUTAS VEDADAS

Além das demais condutas não permitidas insertas nesta Política, é proibido:

Introduzir códigos maliciosos nas redes e sistemas do órgão;

Revelar códigos de identificação, autenticação e autorização de uso pessoal (conta, senhas, chaves privadas etc.) ou permitir o uso por terceiros de recursos autorizados por intermédio desses códigos;

Divulgar ou comercializar produtos, itens ou serviços a partir de qualquer recurso dos sistemas do órgão;

Tentar interferir sem autorização em um serviço, sobrecarregá-lo ou, ainda, desativá-lo, inclusive aderir ou cooperar com ataques de negação de serviços internos ou externos;

Alterar registro de evento dos sistemas, informações ou dados;

Modificar qualquer dado, configuração, protocolos de comunicação, sem a expressa autorização da Diretoria Geral ou Presidência;

Obter acesso não autorizado, ou acessar indevidamente dados, sistemas ou redes, incluindo qualquer tentativa de investigar, examinar ou testar vulnerabilidades nos sistemas do órgão;

Monitorar ou interceptar o tráfego de dados nos sistemas sem as devidas autorizações;

Violar medida de segurança ou de autenticação, sem as devidas autorizações;

Fornecer informações a terceiros sobre usuários ou serviços disponibilizados nos sistemas do órgão, exceto os de natureza pública ou mediante autorização de autoridade competente;

Compartilhar ou viabilizar o compartilhamento, sem autorização da Presidência ou Diretoria Geral, de informações classificadas como restritas ou confidenciais, bem como dados pessoais;

Enviar informações do órgão para endereços particulares de e-mail;

Utilizar uma impressora coletiva para gerar informações confidenciais e não recolher o documento impresso imediatamente;

Discutir ou comentar assuntos confidenciais em locais públicos;

Discutir ou comentar assuntos confidencias com pessoas não autorizadas;

Utilizar as informações do órgão para obter ganhos pessoais;

Armazenamento ou uso de jogos em computador ou sistema informacional do órgão.

12. DAS PENALIDADES

A violação das regras estabelecidas nesta Política ou suas normas internas de segurança, por qualquer pessoa física ou jurídica, acarretará as penalidades civis, penais e administrativas previstas na legislação, conforme o caso.

Para os agentes públicos, pode acarretar na aplicação de advertência, suspensão, desligamento formal ou rescisão contratual sem prejuízo das penalidades civis, penais e administrativas previstas na legislação, conforme o caso.

13. VIGÊNCIA E VALIDADE

Esta Política, suas normas internas de segurança e suas atualizações deverão ser divulgadas amplamente aos agentes públicos do órgão.

Esta Política, bem como todas as normas dela decorrentes, deverão ser revisadas e atualizadas sempre que se fizer necessário, não excedendo o período máximo de dois anos.

Os integrantes do Comitê de Privacidade e Proteção de Dados (CPPD) poderão expedir instruções complementares, no âmbito de suas competências, que detalharão suas particularidades e procedimentos relativos à Segurança da Informação alinhados às diretrizes emanadas pelo CPPD e aos respectivos Planos Estratégicos Institucionais da Câmara Municipal de Pato Branco.

Casos omissos serão resolvidos pelo Comitê de Privacidade e Proteção de Dados (CPPD), ao qual também serão submetidas eventuais dúvidas sobre esta Política e seus documentos.

Esta Política entra em vigor na data de sua publicação.

ANEXO III

TERMO DE CIÊNCIA E RESPONSABILIDADE

Eu, nome, nacionalidade, estado civil, profissão, inscrito no CPF nº XXX.XXX.XXX-XX, declaro ciência de que, durante o exercício do mandato parlamentar de vereador na _____ª Legislatura da Câmara Municipal de Pato Branco, quando realizar atividades de tratamento de dados pessoais relacionadas ao desempenho do mandato por vereadores, lideranças, bancadas, blocos e frentes parlamentares, em que não forem utilizados sistemas institucionais da Câmara Municipal de Pato Branco, exercerei as atribuições de controlador de dados pessoais, nos termos da Lei Federal nº 13.709/2018 (LGPD).

Pato Branco, _____ de _____ de 20___.

_____
Nome

Vereador

Publicado por:
Eliana Scariot Amorim
Código Identificador:D35D2F99

Matéria publicada no Diário Oficial dos Municípios do Paraná no dia 13/11/2024. Edição 3153
A verificação de autenticidade da matéria pode ser feita informando o código identificador no site:
https://www.diariomunicipal.com.br/amp/