POLÍTICAS DE ADEQUAÇÃO E CONDUTA COM O TRATAMENTO, SEGURANÇA, INTEGRIDADE E DISPONIBILIDADE DE DADOS E TECNOLOGIA DA INFORMAÇÃO

(versão 2.0)

Regulamenta a atuação da equipe do Ofício de Registro de Imóveis, Títulos e Documentos e Civil das Pessoas Naturais e Jurídicas de Iranduba/AM diante das diretrizes constantes da Lei Geral de Proteção de Dados, do Provimento 74/CNJ e Provimento 134/CNJ;

O Registrador Titular do Regulamenta a atuação da equipe do Ofício de Registro de Imóveis, Títulos e Documentos e Civil das Pessoas Naturais e Jurídicas de Iranduba/AM, em conformidade com os deveres que lhe são atribuídos pela legislação, e

CONSIDERANDO a edição da Lei 13.709, de 14 de agosto de 2018, que 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 de privacidade e o livre desenvolvimento da personalidade da pessoa natural;

CONSIDERANDO que o art. 23, em seu parágrafo 4º, informa que é aplicável aos serviços notariais e de registro o tratamento concedido às pessoas jurídicas de direito público referidas na Lei de Acesso à Informação, devendo ser realizado de acordo com o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências e atribuições legais;

CONSIDERANDO a regulamentação exarada pela Corregedoria-Geral de Justiça do Estado do Amazonas no Provimento nº 385, de 09 de dezembro de 2020, e pela Corregedoria Nacional de Justiça no Provimento nº 134, de 24 de agosto de 2022;

CONSIDERANDO a disciplina de segurança, integridade e disponibilidade de dados para a continuidade dos serviços notariais e de registro apresentada pelo Provimento nº 74, de 31 de julho de 2018, do Conselho Nacional de Justiça;

CONSIDERANDO a quantidade de dados e riscos inerentes à atividade notarial e de registro;

CONSIDERANDO o programa de *compliance* adotado por esta Serventia com a causa;

CONSIDERANDO os treinamentos já realizados por oficial e colaboradores, e as discussões e opiniões decorrentes desse processo;

RESOLVE

DAS DISPOSIÇÕES GERAIS

Art. 1º. Instituir as políticas permanentes de tratamento, segurança, integridade e disponibilidade de dados nesta Serventia, na forma que segue.

Art. 2º. Para os fins dessa normativa, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável, inclusive:

a) nome, apelido ou qualquer designação que identifique uma pessoa;

b) número de documentos de identificação;

c) CPF;

d) estado civil;

e) ascendência ou descendência e sua origem biológica ou de outra natureza, bem como eventual ausência da indicação dessas informações ;

f) data de nascimento, casamento ou óbito;

g) endereço, e-mail, telefone, ou qualquer forma de localização da pessoa;

h) local de nascimento, naturalidade, casamento ou óbito;

i) restrições de qualquer natureza existentes e relativas à pessoa;

j) dívidas, patrimônio e poder econômico.

II - 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, ou qualquer informação que pode levar, direta ou indiretamente, a qualquer forma de discriminação, incluindo:

a) cor da pele;

b) dados relativos à identificação de indígenas como tais, como RANI, etnia, aldeia, entre outros;

c) indicação dos associados de determinada pessoa jurídica de cunho político, religioso, filosófico ou sindical;

d) preferências políticas, religiosas ou filosóficas, incluindo o fato de ser pessoa politicamente exposta;

e) fotografias;

f) impressão digital ou qualquer outra forma de identificação biométrica;

g) tipo sanguíneo

h) o fato de a pessoa ser transgênero, transexual, homossexual ou qualquer outra informação relativa à sua sexualidade;

i) doenças, CIDs e causas de morte;

III - dado anonimizado: dado relativo a titular que, em virtude do processo de anonimização, se dissocie daquele, não podendo ser identificado, como pesquisas de satisfação e controles de senha;

IV - banco de dados: conjunto de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico, que podem estar armazenados em meios físicos ou eletrônicos, desde computadores, celulares, informações de sistema, arquivo, entre outros;

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento, incluindo usuários, colaboradores e o próprio oficial;

VI - controlador: pessoa a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa que realiza o tratamento de dados pessoais em nome do controlador;

VII - encarregado: pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

IX - agentes de tratamento: o controlador e o operador;

X – tratamento de dados: 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;

XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada, diferenciando da mera **"ciência"**, em que apenas foi comunicado sobre o tratamento;

XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;

XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado, como eliminação do arquivo físico e das informações digitais;

XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados, como o envio a centrais, órgãos e entidades mediante determinação normativa ou legal;

XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar

riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e

XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

§1º O **controlador** do tratamento de dados desta Serventia é o **Oficial Registrador**.

§2º O **encarregado** do tratamento de dados será nomeado pelo controlador e será divulgado a todos operadores e usuários, por meio de avisos internos e no sítio eletrônico mantido pela serventia, podendo ser suprimida a função se a ANPD vier a declarar a desnecessidade de sua existência no âmbito desta serventia.

§3º São **operadores** no tratamento de dados **as** pessoas que, mediante contrato verbal ou escrito, lidem com os dados que transitam pela Serventia, equiparando-se, no que couber, os próprios colaboradores da serventia.

Art. 3º. A atuação de todos os agentes envolvidos no tratamento de dados desta serventia deve se dar com vistas a proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, tendo como fundamentos:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Parágrafo único: As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

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. Não se pode utilizar o dado para fins diversos dos pretendidos e informados inicialmente.

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento. A forma pela qual é adquirido o dado deve ser compatível com o que se pretende fazer com o dado.

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. Averiguar em cada procedimento a necessidade de obtenção de determinadas informações.

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. A consulta não se confunde com a emissão de certidões. O livre acesso é de que informações estão de posse da Serventia, quanto tempo permanecem no cartório e de que forma é realizado o tratamento/manuseio delas.

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. Para manter a integridade, devem ser mantidas formas de restauração e salvaguarda das informações, incluindo backups, treinamentos, auditorias.

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. 4º. O tratamento de dados pessoais (art. 2º, I) somente poderá ser realizado:

I - mediante o fornecimento de consentimento por escrito ou outra forma inequívoca pelo titular dos dados;

II - sem fornecimento de consentimento do titular, nas seguintes hipóteses:

a) para o cumprimento de obrigação legal ou regulatória pelo controlador, como a prática dos atos inerentes ao exercício do ofício registral ou da legislação trabalhista, nos termos dos arts. 2º e 3º do Provimento 385/2020, da CGJ-AM;

b) pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;

c) para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais, como o envio de informações para o IBGE, FUNAI e INCRA;

d) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

e) para o exercício regular de direitos em processo judicial ou administrativo pela serventia;

f) para a proteção da vida ou da incolumidade física do titular do dado ou de terceiro;

g) para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

h) quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

i) para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Art. 5º. O tratamento de dados pessoais sensíveis (art. 2º, II), somente poderá ocorrer:

I - quando o titular ou seu responsável legal consentir, **de forma específica e destacada**, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador, como a prática dos atos inerentes ao exercício do ofício registral ou da legislação trabalhista, nos termos dos arts. 2º e 3º do Provimento 385/2020, da CGJ-AM;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis, como o envio de informações para o IBGE e FUNAI;

d) exercício regular de direitos, inclusive em contrato e em processo judicial e administrativo pela serventia;

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados e

exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Art. 6º. Compete ao encarregado de proteção de dados:

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações da autoridade nacional e adotar providências;

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

Parágrafo único: Será mantido canal de atendimento para informações, reclamações e sugestões ligadas ao tratamento de dados pessoais, podendo ser realizado presencialmente na serventia, por meio do sítio eletrônico ou e-mail específico, divulgado no mural da serventia e sítio eletrônico..

DO CONTROLE DE FLUXO DE DADOS

Art. 7º. Os dados serão **obtidos** primordialmente pelas seguintes formas:

I. Extração das informações contidas em documentos apresentados para a prática de atos registrais, como títulos, requerimentos e declarações;

II. Preenchimento de formulários, físicos ou eletrônicos, bem como informações prestadas voluntariamente pelas partes em mensagens instantâneas ou correios eletrônicos;

III. Aposição de impressão digital por meio de "digiselo", nos atos que o declarante das informações não for alfabetizado e a lei permitir a captura de sua impressão biométrica;

IV. Consulta às Centrais de Serviços Eletrônicos, nos termos das normativas respectivas;

V. Redução a termo, de declarações prestadas pelas partes, em procedimentos que exijam a entrevista ou a indagação de dados, para o convencimento do oficial ou preposto para a prática de atos registrais;

VI. Excepcionalmente, por informações verbais das partes, nos atos que exijam declarações, quando não for possível ou exigível a sua aposição em formulários escritos, de forma a preservar a confidencialidade diante dos demais presentes no ambiente.

Art. 8º. O **tratamento interno** de dados dar-se-á observando os seguintes preceitos:

I. Os dados serão utilizados tão somente para o cumprimento de suas finalidades, como a prática dos atos registrais solicitados ou comunicações obrigatórias;

II. Somente o operador incumbido da prática do ato ou do seu compartilhamento deve se ater aos dados relativos a ele, vedado repassar aos demais operadores senão para dar continuidade ao tratamento;

III. Quando o tratamento depender de autorização do seu titular, a autorização permanecerá arquivada em ficheiro próprio;

IV. Após a prática do ato, os documentos relativos serão arquivados fisicamente, e, quando for o caso, também eletronicamente;

V. Ao responsável pela digitalização do acervo é proibida a análise dos dados digitalizados, tão somente a visualização da sua nitidez e a indexação em pastas próprias;

VI. O acesso aos arquivos físicos ou eletrônicos da serventia é restrito a quem estiver praticando atos registrais a ele relativos, ou em fase de seu tratamento, sendo vedada a consulta para qualquer outro fim;

VII. As informações aos titulares serão prestadas de forma exata, clara, relevante, a atualizadas, abrangendo a forma e duração do tratamento e a integralidade dos dados pessoais, quando não for imposto sigilo pela lei;

VIII. As informações poderão ser prestadas de forma escrita ou verbal, conforme for solicitado, constando a advertência de que foi entregue ao seu titular, na forma da Lei 13.709/18, e que não produz os efeitos de certidão, não possuindo fé pública para prevalência de direito perante terceiros.

IX. (Revogado).

Parágrafo primeiro. (Revogado).

Parágrafo segundo. (Revogado).

Art. 8º-A. A emissão de certidões seguirá o previsto neste artigo.

§1º. As certidões do registro civil de pessoas naturais observarão o seguinte:

I. Independente de requerimento ou identificação, é possível a emissão de certidões em breve relato (modelo padronizado em campos próprios pelo Prov. 63/CNJ), a qualquer pessoa.

II. Não constarão no campo averbações/anotações qualquer outra informação adicional dos registros que não sejam compatíveis com o mencionado campo, não se aplicando referida proibição às informações relativas a indígenas.

III. A emissão de certidão de inteiro teor, datilografada ou reprográfica (por imagem), **sempre** depende de requerimento com firma reconhecida, com assinatura digital ou assinatura no balcão da serventia, com **identificação do requerente, finalidade da certidão, grau de parentesco com o registrado (caso exista) e se este é ou não falecido.**

IV. A certidão que não for expedida em breve relato e contiver **dados sensíveis somente** serão expedidas ao **próprio interessado** ou seus **representantes** ou a quem detiver **autorização judicial**, e sendo **falecido** o titular do dado sensível, aos **parentes em linha reta que comprovarem tal condição**.

V. Recebem o mesmo tratamento de **dados sensíveis**, os **dados restritos**, como os relativos a adoção, reconhecimento de filiação e os de alteração de sexo e nome de transgêneros, bem como os **dados sigilosos**, como a alteração de nome judicialmente ordenada para proteção de testemunhas que colaboraram em processo criminal e podem sofrer coação.

VI. A referência no registro de ser "legítima" a filiação não impede a sua livre emissão, inclusive a terceiros.

VII. A referência no registro de seu titular ter sido "**legitimado**" posteriormente, ou ser "**ilegítimo**", recebe o tratamento de dado restrito.

VIII. A certidão de habilitação de casamento somente pode ser entregue aos próprios nubentes ou aos seus representantes, ou a quem obtiver autorização judicial.

IX. As buscas para localização de assentos independem de requerimento ou justificação, respeitados os emolumentos devidos.

X. As certidões de óbito, em qualquer modalidade, podem ser emitidas livremente, independente do seu conteúdo, do seu requerente ou a sua finalidade.

XI. O edital de proclamas deve conter apenas o nome, estado civil, filiação, cidade e circunscrição do domicílio dos noivos.

§2º. As certidões relativas ao registro de imóveis observarão o seguinte:

I. Todos os pedidos de certidão deverão ter a identificação do requerente, não sendo possível a emissão para anônimos.

II. Pedidos de certidões, buscas e informações **em bloco, ou vintenária, ou por nome ou por endereço**, dependem de identificação **e indicação da finalidade**.

§3º. A emissão de certidão do registro civil das pessoas jurídicas que de qualquer forma informe os membros da entidade que por seu objeto ou ideologia indique dado sensível, deve vir precedida de requerimento e finalidade.

§4º. As notificações extrajudiciais que contenham dados pessoais, sensíveis ou não, devem ser realizadas pelo próprio oficial.

§5º: A retificação ou restauração de dado pessoal deverá observar o procedimento próprio e respectivo previsto na legislação

Art. 9º. Os atos registrais e documentos correlatos permanecerão **arquivados e/ou armazenados** nesta Serventia, em meio físico e/ou digital, em conformidade com a tabela de temporalidade prevista no Provimento 50 do Conselho Nacional de Justiça.

§1º Quando passível de eliminação, os documentos físicos devem ser fragmentados e incinerados de forma segura, de modo que não seja possível sua recuperação, e, no caso de arquivos digitais, a eliminação deve ser permanente.

§2º Semanalmente, serão eliminados os arquivos digitalizados que não devam permanecer arquivados.

§3º Os e-mails ou mensagens instantâneas contendo dados pessoais serão eliminados tão logo não possuam qualquer utilização para a comprovação da prática ou resposta das demandas.

§4º Os currículos recebidos serão eliminados tão logo não sejam selecionados nem haja a possibilidade de seleção futura.

Art. 10. O **compartilhamento** de dados somente se dará em cumprimento de determinação legal, normativa ou ordem judicial, e deve ser realizado pelo operador responsável, observando o tratamento previsto nos artigos anteriores.

Art. **11.** Os **registros** dos tratamentos de dados serão realizados nos respectivos sistemas informatizados.

DIREITOS DOS TITULARES DE DADOS

Art. 12. São direitos dos titulares dos dados:

I – a ciência das hipóteses em que, no exercício das competências desta Serventia, seja realizado o tratamento de dados pessoais;

II – o fornecimento de informações claras e atualizadas sobre a previsão legal, a finalidade, o tempo de conservação, os procedimentos e as práticas utilizadas para a execução dessas atividades;

III – ter acesso às políticas de tratamento de dados desta serventia, inclusive por meio eletrônico;

IV – requerer, a qualquer tempo, informações acerca dos dados esta serventia possui a seu respeito e a que autoridades ou centrais são compartilhados;

V – requerer, a qualquer tempo, a exclusão dos dados que esta serventia possui e não estejam em tratamento nas hipóteses legais, ou que não estejam dentre as hipóteses que devam permanecer em seu banco de dados;

VI – ser respeitado com discrição e sem qualquer discriminação por conta dos dados que qualquer membro desta serventia tenha conhecimento no exercício de suas atribuições;

VII – ser notificado de eventuais ocorrências com seus dados;

VIII – somente ter seus dados em tratamento sem sua autorização quando as normativas assim permitirem;

IX – ter fácil acesso e meios de comunicação adequados com o encarregado de dados (DPO), com resposta de suas demandas em prazo razoável.

§1º. Constituem hipóteses previstas em atos normativos que haverá compartilhamento de dados pessoais e sensíveis, entre outras, o envio de informações:

I. Ao IBGE, relativamente aos nascimentos, casamentos e óbitos, trimestralmente, nos termos do art. 49, da Lei 6.015/73;

II. À CRC, relativamente aos atos e alterações praticados no Registro Civil das Pessoas Naturais, nos termos do Provimento 46 do Conselho Nacional de Justiça;

III. Ao SIRC, relativamente aos atos e alterações praticados no Registro Civil das Pessoas Naturais, nos termos do Decreto 9.929/19;

IV. À Receita Federal do Brasil; à Secretaria de Segurança Pública; ao INSS; à Junta Militar do Município; à Secretaria de Saúde do Município; ao Juiz da Zona Eleitoral; à Polícia Federal, Embaixadas e repartições consulares; e à secretaria de estado de administração, relativamente aos registros de óbitos ocorridos no mês anterior, na forma do art. 80, parágrafo único, da Lei 6.015/73, e art. 308 do Provimento 278/CGJ-AM;

V. Ao Judiciário e ao Poder Executivo Federal, relativamente aos registros eletrônicos em geral, na forma do art. 41 da Lei 11.977/09;

VI. Ao Ministério Público e à Coordenadoria da Infância e da Juventude, relativamente aos registros de nascimento em que a mãe possuía menos de 14 anos e 9 meses na data do parto, na forma dos Provimentos 380 e 383 da CGJ-AM;

VII. Ao Juiz Corregedor Permanente, nos casos de registro de nascimento sem paternidade estabelecida, na forma da Lei 8.560/92;

VIII. Às autoridades judiciárias e administrativas, quando solicitado, na forma do art. 30, III, da Lei 8.935/94;

IX. À Receita Federal, as declarações sobre operações imobiliárias (DOI), na forma da IN RFB 1112/2010;

X. Ao SISCOAF, no que diz respeito às operações financeiras informadas no Provimento 88 do Conselho Nacional de Justiça;

XI. Ao INCRA, as alterações nas matrículas de imóveis rurais, na forma do art. 22, §7º, da Lei 4.947/66 e regulamentações posteriores;

XII. Ao INCRA, à CGJ-AM, ao Ministério da Agricultura e ao Gabinete de Segurança Nacional, relativamente às aquisições de imóveis rurais por estrangeiro, na forma do Provimento 207/2013; da CGJ-AM;

XIII. Ao SINTER, relativamente ao fluo de dados cadastrais, fiscais e geoespaciais, na forma do Decreto 8.764/2016;

XIV. À CNIB e demais órgãos judiciários, relativamente à titularidade de bens objeto de ordem de indisponibilidade, na forma do Provimento 39 do Conselho Nacional de Justiça.

§2º. Será observado, nos termos da legislação, as causas de sigilo impostas a determinados atos registrais e as limitações delas decorrentes.

§3º. Sempre que possível pelas normativas será realizada a anonimização de dados pessoais antes do compartilhamento.

§4º. O direito de informação gratuito aos titulares de dados constantes nesta Serventia não substitui as certidões, tampouco desobriga o pagamento dos emolumentos devidos para sua emissão, quando não for causa de gratuidade.

§5º. Não cabe a esta serventia certificar a forma de tratamento ou prazo de armazenamento de dados pelos órgãos que os receberem em virtude do compartilhamento mencionado.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DE RESPOSTA A INCIDENTES DE SEGURANÇA

Art. 13. Para salvaguarda da segurança da informação e de dados, objetivando a confidencialidade, disponibilidade, autenticidade, integridade e mecanismos preventivos de controle físico e lógico, é vedado aos operadores de dados, aos quais os colaboradores se equiparam, sob pena de aplicação das medidas sancionatórias legais:

I. o compartilhamento de qualquer dado pessoal obtido em virtude do desempenho de atribuições dos operadores na Serventia a qualquer agente externo, salvo nas hipóteses legais, incluindo-se na proibição o compartilhamento com família, amigos, conhecidos ou em redes sociais, ou até mesmo entre operadores, em ambientes externos e/ou com finalidade desnecessária ao tratamento.

II. o uso de equipamentos (hardware) de armazenamento de dados nas dependências da serventia, como pendrive, hd externo, unidade de cd ou dvd, ainda que a pedido de usuários, exceto os destinados exclusivamente ao backup de dados da serventia;

III. a instalação de qualquer aplicação nos computadores da serventia, sem autorização do controlador;

IV. o download de arquivos que não sejam necessários à prática dos atos;

V. a utilização da internet ou acesso a endereços eletrônicos diversos àqueles inerentes à prática de atos;

VI. a utilização de wi-fi da serventia, para qualquer fim pessoal, bem como o compartilhamento da sua forma de acesso a usuários do serviço;

VII. compartilhar senhas pessoais de acesso aos demais operadores;

VIII. desativar os sistemas de proteção dos computadores;

IX. eliminar documentos ou arquivos físicos e eletrônicos nas hipóteses em que seja obrigatória a sua manutenção no acervo da serventia;

X. eliminar documentos ou arquivos físicos, quando possível, sem a sua destruição de forma a não poder se recuperar os respectivos dados;

XI. o acesso ou envio de e-mails particulares, utilizando a rede da serventia;

XII. abrir ou responder e-mails, mensagens ou arquivos que sejam de procedência evidentemente duvidosa, solicitando ao controlador, se for o caso, orientações em caso de dúvida sobre a possibilidade de existência de malwares ocultos;

XIII. anotar ou gravar qualquer dado pessoal ou sensível em locais diversos dos exigidos para a prática dos atos;

XIV. a impressão desnecessária de documentos contendo dados;

XV. o vazamento ou uso indevido de rascunhos contendo dados pessoais;

XVI. tirar fotografias no interior da serventia, que, de qualquer forma, possam expor dados;

XVII. manter documentos com dados pessoais em cima das mesas quando não estiverem sendo utilizados para a prática de atos no momento;

XVIII. reutilizar dados cadastrais dos titulares já constantes nos bancos de dados para a prática de novos atos sem a sua autorização;

XIX. deixar documentos contendo dados em espaços que outros operadores não autorizados ou outros usuários do serviço possam ter acesso;

XX. falar, conversar ou de qualquer forma pronunciar em voz alta dados pessoais e sensíveis, ainda que em tratativas com os próprios titulares no ambiente de atendimento, de forma que outros operadores ou usuários possam ouvir;

XXI. fornecer as imagens do sistema de segurança (câmeras) sem autorização;

XXII. alterar qualquer senha ou configuração padrão dos equipamentos da serventia sem prévia autorização do controlador;

XXIII. salvar modelos ou minutas com dados pessoais;

XXIV. utilizar os celulares da serventia em desacordo com a sua finalidade.

Parágrafo único: Para evitar e fiscalizar o disposto neste artigo, poderá o controlador se valer de:

a) treinamentos periódicos;

b) auditorias internas;

c) controle de acessos a sites, computadores, e-mails, aplicações ou demais itens de software dos computadores corporativos.

Art. 14. Será exigido, tanto dos operadores quanto dos prestadores de serviços técnicos, a assinatura de termo orientando sobre os deveres, requisitos e responsabilidades decorrentes da Lei Geral de Proteção de Dados, principalmente no que diz respeito ao consentimento, sigilo e confidencialidade de uso de dados, ficando arquivada a ciência de qualquer nova orientação prestada..

Parágrafo único. A responsabilidade dos prepostos e terceirizados subsiste mesmo após o término do tratamento dos dados ou da relação contratual com o controlador.

Art. 15. Serão realizados backups de segurança dos dados e arquivos na nuvem e em disco rígido, na forma do Provimento 88 do Conselho Nacional de Justiça.

Art. 16. São ocorrências nocivas ao regular funcionamento dos serviços, entre outras:

a) queda de energia;

b) queda de conexão com a internet;

c) infecção das máquinas por malware;

d) comprometimento de equipamentos, de forma parcial ou total;

e) rompimento do banco de dados;

f) vazamento de dados por mau uso de operadores;

g) sequestro dos bancos de dados;

h) incêndio e enchentes;

i) crimes contra o patrimônio físico da serventia.

§1º As ocorrências classificam-se em recorrentes, possíveis e pouco prováveis.

§2º As ocorrências designadas nas letras "a" e "b" são recorrentes.

§3º As ocorrências designadas nas letras "c", "d", "e" e "f" são possíveis.

§4º As ocorrências designadas nas letras "g", "h" e "I" são pouco prováveis.

Art. 16. Em caso de queda de energia, deve-se desligar todos os equipamentos que não estão em uso urgente, a fim de que o nobreak sustente os equipamentos essenciais por mais tempo.

Parágrafo único: Em caso de duração superior a 30 minutos, deve-se contatar a empresa de energia para averiguar o retorno dos serviços.

Art. 17. Em caso de queda de conexão com a internet, deve-se tentar reiniciar os equipamentos de roteamento, a fim de averiguar a possibilidade de retorno.

§1º Em caso de duração de queda superior a 15 minutos, deve-se contatar a empresa de fornecimento de internet a fim de averiguar o ocorrido.

§2º Sempre que possível, a serventia contará com duas conexões distintas de internet.

Art. 18. Em caso de infecção dos equipamentos por malware, deve-se retirá-lo da rede assim que percebido o ocorrido.

§1º Se o caso puder ser solucionado internamente, a máquina retornará ao seu uso habitual.

§2º Caso contrário, deverá a máquina ser levada para manutenção.

§3º É vedado aos operadores sem qualificação técnica tentar solucionar o problema.

Art. 19. O comprometimento de equipamentos deve ter sua tentativa de conserto realizada internamente, e, não sendo possível, enviar para a assistência.

§1º Em caso de impossibilidade de retorno ao trabalho do equipamento, ele será substituído.

§2º Não devem ser armazenados dados e arquivos diretamente nas máquinas, apenas em rede.

§3º É vedado aos operadores sem qualificação técnica tentar solucionar o problema.

Art. 20. Em caso de vazamento de dados por mau uso dos operadores ou sequestro dos bancos de dados, a situação deverá ser analisada de acordo com a extensão do vazamento e dos eventuais danos causados, sem prejuízo da apuração da responsabilidade daqueles que deram causa ao incidente.

§1º o incidente pode ser identificado por:

a) notificação do titular dos dados pessoais ao encarregado de proteção de dados;

b) notificação da ANPD;

c) auditoria interna;

d) contato de hackers;

e) fiscalização do encarregado;

f) monitoramento de conteúdo;

g) auditoria de segurança de banco de dados;

h) denúncias internas e externas

i) quaisquer outras formas que demonstrem fidedignidade da informação.

§2º deverá ser analisada a possibilidade de recuperação do banco de dados pelos backups realizados.

Art. 21. Em caso de incêndio e enchentes, o servidor e o acervo físico de manutenção permanente devem ser prioridade de "salvamento", quando não houver risco à saúde e integridade daqueles que estão no local.

§1º A serventia manterá seguro patrimonial prevendo estas ocorrências e outras decorrentes da ação da natureza.

§2º Em caso de incêndio, todos devem ser evacuados pelas saídas de emergência, caso esteja presente alguém no local.

§3º Será promovido curso de capacitação para uso de extintores e medidas de emergência de salvamento, bem como de primeiros socorros.

§4º Os bombeiros devem ser acionados em qualquer caso de incidentes dessa natureza.

Art. 22. Em caso de crimes contra o patrimônio físico da serventia, a prioridade será a salvaguarda de todos os presentes no local, vedada qualquer forma de resistência por qualquer operador.

Art. 23. Em hipóteses de incidentes que comprometam a segurança com dados pessoais deverá haver:

I. a comunicação do ocorrido pelos operadores ao controlador, para que adote as medidas cabíveis;

II. a comunicação do ocorrido pelo controlador ao Juiz Corregedor Permanente e à Corregedoria Geral da Justiça, no prazo máximo de 24 horas, com esclarecimento do incidente e das medidas adotadas para apuração das suas causas e a mitigação de novos riscos e dos impactos causados aos titulares dos dados;

III. a comunicação do ocorrido pelo controlador à Agência Nacional de Proteção de Dados e, sempre que possível, aos titulares dos dados, do ocorrido, em prazo razoável, conforme definido pela autoridade nacional, em notificação que deverá mencionar, no mínimo:

a) a descrição da natureza dos dados pessoais afetados;

b) as informações sobre os titulares envolvidos;

c) a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

d) os riscos relacionados ao incidente;

e) os motivos da demora, no caso de a comunicação não ter sido imediata; e

f) as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Parágrafo único: a serventia manterá seguro de responsabilidade civil.

DOS DADOS DOS COLABORADORES

Art. 24. Os dados dos colaboradores da serventia estão igualmente protegidos pela Lei Geral de Proteção de Dados.

Art. 25. Os dados dos colaboradores somente podem ser usados pelo empregador nas hipóteses legais, como para manutenção dos contratos de trabalho, registro de ponto, pagamento de salários e benefícios, e alimentação das informações obrigatórias aos órgãos de fiscalização das relações empregatícias.

§1º. O colaborador encarregado de realizar a digitalização e guarda dos documentos relativos aos contratos de trabalho, incluindo os holerites, deverá firmar termo especial de sigilo das informações que possuir em decorrência dessa atribuição.

§2º. Os atestados médicos serão mantidos em sigilo, principalmente quanto ao que concerne a eventual CID neles inserido.

§3º. Aos colaboradores é vedado compartilhar informações de outros colegas de trabalho, inclusive sobre eventual ausência, falta ou saída do trabalho.

§4º. Para cumprir com as obrigações trabalhistas, o empregador manterá contrato com contabilidade especializada.

Art. 26. Aos colaboradores também fica assegurada a aplicação dos princípios, direitos e premissas previstos neste documento, no que couber, com as seguintes ressalvas:

I – não lhes será exigido o compartilhamento de informações pessoais senão aquelas essenciais à contratação e alimentação do e-social e sistemas correlatos;

II – aos colaboradores é assegurado o direito de não expor questões de foro íntimo, como de saúde, religião ou convicções políticas;

III – é dever do colaborador acometido de doença contagiosa informar imediatamente ao oficial;

IV – não há sigilo entre oficial e colaboradores no que diz respeito aos e-mails e aplicativos de mensagens corporativos.

Art. 27. Nenhum colaborador será constrangido a participar de qualquer ato que exponha seus dados pessoais, como fotografias da equipe, por exemplo.

Parágrafo único. O colaborador pode, voluntariamente, participar dos atos previstos no caput.

Art. 28. Os endereços de e-mail institucionais apenas conterão o nome do colaborador quando por ele autorizado.

DOS DADOS DO OFICIAL DA SERVENTIA

Art. 29. Os dados do oficial da serventia também estão sujeitos à proteção prevista na Lei Geral de Proteção de Dados, não podendo ser compartilhados pelos colaboradores, exceto quando expressamente autorizado, como aqueles estritamente necessários ao pagamento de emolumentos, por exemplo.

DISPOSIÇÕES FINAIS

Art. 30. Qualquer alteração à presente será objeto de comunicação e debate em reunião agendada para este fim.

Art. 31. O descumprimento da presente política por qualquer operador será objeto de análise pelo controlador com a tomada das medidas cabíveis para sua solução e reparação.

Art. 32. O presente documento entra em vigor na presente data.

Iranduba, 10/01/2023

ALAN FELIPE PROVIN

Oficial Registrador/Controlador