



**Cartório Gurupi**  
**1º Tabelionato de Notas**

# **Relatório de Impacto e Política Interna de Privacidade e Proteção de Dados**

**Gurupi - TO**

**2025**

## **INTRODUÇÃO**

O Cartório 1º Tabelionato de Notas de Gurupi - TO assegura que está em conformidade com a Lei Geral de Proteção de Dados (LGPD), Lei Federal nº 13.709/2018. Esta serventia, por meio do titular e de seus prepostos, prioriza a preservação da privacidade das informações relativas aos seus usuários, em constante desenvolvimento e aprimoramento de sua Política de Privacidade, demonstrando seu compromisso com a proteção aos dados pessoais, nos termos da Lei Geral de Proteção de Dados. Sem prejuízo aos direitos garantidos pela legislação vigente, reservamo-nos no direito de alterar esta Política de Privacidade de modo a refletir os avanços tecnológicos, as mudanças na legislação ou normas infralegais, assim como a evolução da sociedade como um todo.

## **OBJETIVO**

Este documento tem como objetivo demonstrar nosso compromisso com a Lei, e descrever de que forma a privacidade dos usuários é protegida pela serventia, uma vez que, para a prática dos atos notariais, haverá sempre a coleta, o tratamento e o armazenamento de documentos, dados e informações pessoais remetidos por meio do site <https://cartoriogurupi.com.br/>, de plataformas de transmissão segura ou quando tais dados, documentos ou informações — físicos ou eletrônicos — oriundos de atendimentos presenciais venham a compor as bases de dados da serventia.

## **BASE LEGAL**

**Artigo 236 da CF/1988**

**Lei 8.935/1994**

**Provimento CNJ de no 134/2022**

**Lei no 13.709/2018**

A LGPD abordou em seu art. 7, inciso II e IX que o tratamento de dados pessoais está autorizado para os fins de cumprimento de obrigação legal e para atender aos interesses legítimos do controlador ou de terceiros.

Ademais, no que tange aos dados pessoais sensíveis a Lei Geral de Proteção de Dados (13.709/2018) também fundamenta e autoriza o tratamento destes dados pelas serventias extrajudiciais, eis que o art. 11, inciso II, alínea “a” dispensou o consentimento do titular dos dados nas hipóteses de cumprimento de obrigação legal ou regulatória.

Por conseguinte, o tratamento de dados pessoais por nossa serventia encontra sua base legal na Constituição Federal de 1988, nas legislações referentes as atividades notariais e na Lei Geral de Proteção de Dados.

## **DO CONSENTIMENTO PARA USO DOS DADOS**

Sempre que o usuário solicitar a prática de um ato notarial, esta serventia, por intermédio de seus prepostos, coletará os dados necessários visando o cumprimento das disposições legais, normativas ou meramente baseadas no consentimento do usuário. Os dados coletados têm a função precípua de: (i) qualificação das partes nos atos notariais; (ii) dados bancários para devolução de valores de depósito prévio não utilizados; (iii) acompanhamento online dos serviços; (iv) emissão e envio de selo digital por meio do Sistema GISE do TJTO; (v) emissão de declaração de operações imobiliárias à Receita Federal; (vi) emissão de declaração de operações suspeitas previstas na Lei 9.613/1998 ao COAF; (vii) envio de dados para a Central de Serviços Compartilhados CENSEC; (viii) envio de dados e informações relacionadas à Lei 11.441/2007 ao Instituto Brasileiro de Geografia e Estatística e (ix) atendimento de ordens Judiciais.

A coleta dos dados e informações destinados à prática dos atos notariais é baseada na legislação aplicada ou normas regulamentares, mas sempre visando ao cumprimento dos princípios que regem a atividade. Esses dados e informações serão coletados, armazenados e tratados, notadamente quando relacionados à personalidade, como por exemplo, o nome, o CPF, o número do documento de identificação apresentado, a data de nascimento, a data de casamento e os dados relacionados ao assento, a existência ou não de união estável, a filiação, a nacionalidade, o estado civil, o endereço e a profissão, inclusive dos falecidos quando o ato se referir a eles.

Ainda a depender do ato solicitado, o usuário deverá consentir a respeito da coleta de número de telefone, de plataformas eletrônicas de comunicação ou de endereço de e-mail caso queira receber notificações ou mensagens relacionados ao ato notarial.

Esta serventia não fornece os seus dados pessoais para terceiros, salvo nas comunicações decorrentes de obrigações legais ou normativas, mandados judiciais ou em observância ao Princípio da Publicidade nos termos determinados pelas diretrizes da comissão de Proteção de Dados do CNJ. Ao usuário é livre a concessão ou revogação do seu consentimento, a qualquer momento, bastando fazer comunicação através do e-mail: [lgpdcartoriodegurupi@gmail.com](mailto:lgpdcartoriodegurupi@gmail.com).

## **AGENTES DE TRATAMENTO E OS ENCARREGADOS DE DADOS PESSOAIS**

Em conformidade com a Lei Geral de Proteção de Dados nº 13709/2018, o 1º Tabelionato de Notas de Gurupi - TO dispõe, ainda, de um colaborador encarregado pelo tratamento de dados dentro da Serventia, o qual pode ser contatado diretamente ou de forma eletrônica, via e-mail: [cartorionotaslorrany@gmail.com](mailto:cartorionotaslorrany@gmail.com) ou, ainda, pelo canal disponível no site <https://cartoriogurupi.com.br/>.

Como antes explicitado, o tratamento de dados pessoais no cartório é feito pelos prepostos da serventia de forma a cumprir os deveres legais no exercício da atividade notarial.

## **COMO É REALIZADO O TRATAMENTO DE DADOS EM NOSSA SERVENTIA:**

### **O que é tratamento de dados?**

Para que haja uma adequada compreensão deste RIPD (Relatório de Impacto à Proteção de Dados Pessoais), é importante que se compreenda o que é o tratamento de dados.

Por tratamento, considera-se qualquer manipulação realizada com alguma informação considerada pessoal ou sensível, como por exemplo: coletar, produzir, recepcionar, classificar, utilizar, acessar, reproduzir, transmitir, distribuir, processar,

arquivar, armazenar, eliminar, avaliar ou controlar as informações, modificar, comunicar, transferir, difundir ou extrair (Art. 5º, X, LGPD).

### **Quais os princípios que norteiam o tratamento de dados de nossa serventia?**

Esclarecido que as serventias extrajudiciais realizam tratamento de dados pessoais e dados pessoais sensíveis para cumprir com suas obrigações legais, cabe enfatizar que diante deste cenário seguimos uma série de princípios que norteiam essa atividade em nosso Cartório e que subsidiam este relatório.

Os referidos princípios estão contidos em nossa Política de Proteção de Dados, eles funcionam como norteadores de nossa serventia no tratamento dos dados pessoais dos usuários de nossos serviços, são eles:

**a) Princípio da Finalidade:** Por esse princípio, exigido também pelo Provimento CNJ n. 134/2022, a entrega de informações solicitadas por terceiros deverá atender a propósitos e fins legítimos elencados na Lei 13.709/2018 (LGPD) e devidamente informados e preenchidos em requerimento próprio.

**b) Princípio da Adequação:** Compatibilidade do tratamento com as finalidades informadas ao titular em nossa Política de Dados, de acordo com o contexto do tratamento.

**c) Princípio da Minimização de Tratamento:** Tanto na Coleta quanto na entrega de informações/dados para o próprio titular dos dados ou para terceiros, deverão estritamente ser solicitados necessários para e utilizados somente a prática de cada ato cartorário. Devem-se compatibilizar os provimentos que rege cada ato junto ao **Provimento CNJ n. 134/2022.**

**d) Princípio da Segurança e Prevenção:** Nossa Serventia adota todas as exigências do Provimento CNJ n. 134/2022 para prevenir e garantir a segurança dos dados dos nossos usuários.

**Qual a natureza e o escopo do tratamento de dados pessoais por nossa serventia?**

Para o exercício com excelência da atividade cartorária é fundamental o tratamento de dados (pessoais e sensíveis). A título de exemplo de Dados Pessoais nossa Serventia trata diversos dados pessoais, como:

**1. Cadastrais / Identificação:** Nome Completo, CPF, RG, Estado Civil, Endereço, Telefone, E- mail, Data de Nascimento, dentre outros dados que são necessárias à identificação dos usuários de nossos serviços e exigidos pelos respectivos Provimentos de Corregedorias Estaduais e Nacionais, bem como legislações pertinentes.

**2. Dados Sensíveis:** em alguns casos existe a necessidade do tratamento de dados considerados sensíveis pela Lei no 13.709/2018 (LGPD) que podem ser:

1. Origem racial ou étnica,
2. Convicção religiosa,
3. Opinião política,
4. Filiação a sindicato ou a organização de caráter religioso,
5. Filosófico ou político, dado referente à saúde ou à vida sexual,
6. Dado genético ou biométrico,
7. Quando vinculado a uma pessoa natural;

**3. Esses dados podem constar dos mais diversos atos cartorários de nossa serventia, tais como:**

Registro de Nascimento  
Registro de Óbito  
Registro de Casamento  
Registro de Natimorto  
União Estável  
Adoção  
Reconhecimento de Paternidade e Maternidade  
Alteração de Prenome e Gênero  
Retificações Administrativas  
Emancipação  
Certidões de Breve Relato

Certidões em Inteiro Teor

Anotações

Averbações

Comunicações

Os dados elencados acima são coletados no intuito da correta identificação das pessoas que participam dos atos, de modo presencial e on-line, garantindo-se a fidedignidade da correta identificação do titular ou solicitante de serviços.

Ademais, em casos excepcionais, não previstos neste relatório, os colaboradores e tabelião(ã) deverão se nortear pelos princípios contidos em nossa Política de Privacidade, especialmente aos que tangem à Minimização de Coleta, Finalidade e Adequação.

### **Qual o contexto e a finalidade do tratamento de dados pessoais por nossa serventia?**

Como mencionado nos tópicos anteriores, as serventias extrajudiciais tratam dados pessoais e pessoais sensíveis. O tratamento destes dados decorre da obrigação legal dos cartórios em garantir a publicidade, autenticidade, segurança e eficácia dos atos praticados pelos usuários de nossos serviços.

Nessa mesma ótica, destaca-se o fato de nossa serventia seguir, dentre os vários princípios trazidos pela LGPD, os princípios da finalidade, da adequação e da necessidade. Ou seja, realizamos o tratamento de dados com propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades e com contexto que deu origem ao tratamento do dado.

Ademais, nossa serventia se limita ao tratamento dos dados dos usuários de nossos serviços no mínimo necessário para a realização de nossas atribuições legais, sempre observando a finalidade, abrangência, pertinência e proporcionalidade do tratamento.

Por fim, cabe esclarecer que em conformidade com o **art. 27 da Lei no 8.935/1994**, essa serventia sempre realiza o tratamento de dados única e exclusivamente objetivando o interesse público, nos abstermos de praticar, pessoalmente, qualquer ato que esteja diretamente e/ou indiretamente ligado aos nossos interesses.

## **MAPEAMENTO DE PROCESSOS E DADOS PESSOAIS**

Este documento detalha os principais processos de tratamento de dados pessoais e os tipos de dados envolvidos nas rotinas do 1º Tabelionato de Notas de Gurupi - TO. A compreensão desses fluxos é fundamental para a correta aplicação da Lei Geral de Proteção de Dados (LGPD) e para a elaboração de um plano de ação eficaz.

As atividades notariais são intrinsecamente ligadas ao tratamento de dados pessoais, uma vez que formalizam atos e negócios jurídicos, conferem publicidade e garantem a segurança jurídica, o que frequentemente exige a coleta, o armazenamento e o compartilhamento de informações que identificam ou podem identificar pessoas naturais.

O 1º Tabelionato de Notas é responsável por formalizar a vontade das partes em atos como escrituras públicas, procurações, testamentos e atas notariais, além de realizar autenticações e reconhecimentos de firma.

### **Processos Relevantes:**

#### **1 - Lavratura de Escrituras Públicas (Compra e Venda, Doação, Inventário, Divórcio, União Estável, etc.)**

Este é um dos processos centrais. Envolve a coleta de dados dos comparecentes (outorgantes, outorgados, herdeiros, cônjuges, etc.) e, por vezes, de terceiros mencionados no ato. Os dados são coletados para qualificação das partes, verificação da capacidade civil, descrição do objeto do negócio e cumprimento de obrigações legais. Os dados são registrados no livro de notas e compartilhados com centrais eletrônicas (CENSEC, DOI - Declaração sobre Operações Imobiliárias para a Receita Federal).

#### **Dados Pessoais Tratados:**

Nome completo, nacionalidade, estado civil, profissão, número de CPF, número de RG (ou outro documento de identidade) e órgão emissor, endereço residencial e comercial, e-mail, telefone, regime de bens, data de casamento, pacto antenupcial, filiação (em alguns casos), dados biométricos (para identificação, se aplicável), informações financeiras e patrimoniais relacionadas ao ato.

## **2 - Lavratura de Procurações**

Coleta de dados do outorgante e do outorgado para formalizar a representação. Os dados são registrados em livro próprio.

### **Dados Pessoais Tratados:**

Nome completo, nacionalidade, estado civil, profissão, CPF, RG, endereço.

## **3 - Lavratura de Testamentos**

Ato personalíssimo que envolve a coleta de dados do testador e, potencialmente, de herdeiros e legatários. O conteúdo do testamento é sigiloso até o falecimento do testador. A existência do testamento é comunicada à RCTO (Registro Central de Testamentos Online).

### **Dados Pessoais Tratados:**

Nome completo, CPF, RG, endereço do testador; nomes e qualificações (parciais ou completas) de herdeiros/legatários; informações patrimoniais.

## **4 - Lavratura de Atas Notariais**

Constatação de fatos a pedido de uma parte. Pode envolver a descrição de conteúdos de websites, mensagens, ou a presença de pessoas em determinados locais.

### **Dados Pessoais Tratados:**

Dados do solicitante (nome, CPF, RG, endereço); dados de terceiros que possam estar envolvidos nos fatos constatados (nomes, imagens, conversas – dependendo do objeto da ata).

## **5 - Reconhecimento de Firmas (Autenticidade e Semelhança)**

Coleta de dados para abertura do cartão de assinatura (ficha de firma) e comparação da assinatura no documento.

### **Dados Pessoais Tratados:**

Nome completo, CPF, RG, assinatura, dados biométricos (impressão digital, foto – para o cartão de firma).

## **6 - Autenticação de Cópias**

Verificação da conformidade da cópia com o documento original. Não envolve, geralmente, a retenção de dados do solicitante, mas o documento copiado pode conter dados pessoais.

## **7 - Emissão de Certidões e Traslados**

Fornecimento de cópias fiéis dos atos lavrados nos livros do tabelionato.

### **Dados Pessoais Tratados:**

Todos os dados constantes no ato original.

## **PROCEDIMENTO EM CASO DA OCORRÊNCIA DE VAZAMENTO DE DADOS**

O primeiro passo para saber o que fazer no caso de um vazamento de dados é compreender o que é um vazamento de dados.

Por vazamento de dados entende-se pelo acesso à informações por terceiros que não teriam autorização para tê-lo.

### **Classificação do vazamento**

Trazendo para dentro da Serventia, esse vazamento pode ocorrer de forma:

- 1.Física;
- 2.Digital;
- 3.Em pequeno volume;
- 4.Em grande volume;
- 5.Dados de baixo impacto;

A forma de vazamento física consiste no acesso não autorizado por terceiros de atos cartorários, ou ainda os que não se tornaram atos ou documentos “públicos”, como minutas ou documentos que não irão compô-los no formato em papel ou qualquer similar em que possuam representação material no mundo físico.

A forma de vazamento digital consiste no acesso não autorizado por terceiros de atos cartorários, ou ainda os que não se tornaram atos ou documentos “públicos”, como minutas documentos que não irão compô-los no formato em formato de “bytes” que possam ser acessados via dispositivos telemáticos digitais como smartphones, computadores, notebooks, tablets etc.

Quanto ao volume, a análise se dá se o vazamento visou uma ou algumas pessoas determinadas ou se ele se deu de forma aleatória atingindo todo ou considerável parte do banco de dados do cartório.

Em relação ao potencial do dano, a classificação verifica-se pela natureza do dado vazado: se tem natureza puramente cadastral ou se nele também há informações sensíveis (questões relativas à sexo, dados de saúde, origem étnica, raça, preferência política).

Feito esta análise, passamos as medidas de respostas e condutas a serem adotadas.

## **Medidas Iniciais**

### **Possíveis Causas**

A primeira medida inicial a ser adotada no caso de um incidente de vazamento é promover uma varredura sobre a potencial causa, que dentro dos cartórios poderão ser (não somente):

1. Vazamento doloso causado por colaborador ou ex colaborador;
2. Vazamento culposos causado por colaborador;
3. Vazamento decorrente de acesso hacker;
4. Vazamento decorrente de perda de backup em instrumento físico (pen drives, Hd's)
5. Vazamento por compartilhamento de dispositivos telemáticos (smartphones, computadores, notebooks institucionais ou pessoais com acesso aos sistemas e redes do cartório);
6. Vazamento ocasionado por Operadores dos Dados do Cartórios (Sistemas, Redes, Nuvens, Contabilidade, Prestadores de Serviços em Geral).

**Os exemplos acima não são taxativos, podendo as causas ser outras, variadas e conjuntas.**

### **Contenção**

Identificado o potencial de causa, devem ser adotadas medidas imediatas para mitigação dos eventuais danos.

Essas medidas dependerão de análise caso a caso, entretanto, via de regra devem ser:

1. Se causada por colaborador: retirar-lhe o acesso à sistemas, banco de dados ou até mesmo as dependências físicas como arquivos ou demais locais de armazenamento de dados até que seja apurada sua conduta (dolosa ou culposa);
2. Se causada por operador de dados: convocar reunião de urgência exigindo relatório do que foi vazado (item a item) e quais medidas de mitigação e segurança estão ou serão adotadas;

### **Análise, comunicados e ações**

Promovida a classificação do vazamento e realizadas as medidas de sua contenção, deverá a Serventia, junto com seu **Encarregado de Proteção de Dados** quais deverão ser os próximos passos junto ao titular dos dados e autoridades de fiscalização, seguindo as seguintes recomendações:

1. Potencial de Risco ao Usuário: Se o dado vazado puder colocar em risco o patrimônio, a honra, a imagem ou privacidade do usuário, deve a Serventia promover o seu imediato comunicado para que este também possa tomar as suas próprias medidas para evitar danos ou minimizá-los.

Por exemplo, no caso de um vazamento de imagem de assento digitalizado. O usuário (titular dos dados) deve ser comunicado para que possa tomar ciência e não ficar sujeito à fraudes por reconhecimentos promovidos por impostores.

Um outro exemplo é o caso do vazamento de requerimento com conteúdo sensível. A depender do caso, é possível ao titular tomar medidas judiciais para evitar a divulgação, pesquisas em sites e demais medidas de restrição contra potenciais terceiros que tentarem das publicidade e disseminação à informação.

2. Volume: Se o vazamento se der em grande volume (vazamento total ou parcial de banco de dados), ainda que de baixo potencial lesivo ao titular, deve o responsável pela Serventia, além das medidas acima e constantes nesse relatório, promover comunicados à ANPD (Autoridade Nacional de Proteção de Dados) e à Corregedoria dando-lhes ciência do fato e das medidas que estão sendo adotadas, dentro do prazo máximo de 48 horas.

O comunicado deverá conter:

1. Data e hora da detecção;
2. Circunstâncias em que ocorreu a violação de segurança de dados pessoais, por exemplo, perda, roubo, cópia, vazamento, dentre outros;

3. Descrição dos dados pessoais e informações afetadas, como natureza e conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados;
4. Resumo do incidente de segurança com dados pessoais, com indicação da localização física e meio de armazenamento;
5. Possíveis consequências e efeitos negativos sobre os titulares dos dados afetados;
6. Medidas de segurança, técnicas e administrativas preventivas tomadas pelo controlador de acordo com a LGPD;
7. Resumo das medidas implementadas até o momento para controlar os possíveis danos;
8. Outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos.

**Agir com transparência, além de uma exigência do Provimento, faz com que eventuais penalidades devam ser reduzidas ou não aplicadas. Se o conhecimento do vazamento ocorrer por outros meios, que não o da própria Serventia, ficará demonstrada a omissão por parte do responsável pela Serventia.**

## **A APROVAÇÃO DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS DA NOSSA SERVENTIA.**

O presente RIPD (Relatório de Impacto à Proteção de Dados Pessoais) buscou descrever os processos de tratamento de dados pessoais que podem gerar riscos e quais as medidas que nossa serventia adota para eliminar, reduzir ou amenizar tais riscos.

Diante disto, a fim de trazer maior segurança e efetividade ao presente RIPD, nossa serventia formaliza a aprovação deste documento através das assinaturas das seguintes pessoas:

1. Tabelião;
2. Encarregado de dados.

No mais, diante da dinamicidade das relações sociais e formas de comunicação, além da inovação tecnológica, este relatório passa a ser avaliado continuamente sobre os riscos no tratamento de dados pessoais através da revisão deste RIPD (Relatório de Impacto à Proteção de Dados Pessoais) anualmente ou sempre que surgir qualquer mudança significativa.

**1º Tabelionato de Notas de Gurupi - TO, 02/01/2025**

**Data da última atualização: 10/10/2025**

---

**Mateus Pedro Oliveira Martins Rocha - Tabelião**

---

**Lorrany Marina Diniz Fuentes - Encarregado**