



# Relatório de Impacto de Proteção de Dados

# SUMÁRIO

## Sumário

1. OBJETIVO.....	2
2. QUEM SÃO OS AGENTES DE TRATAMENTO E OS ENCARREGADOS DOS DADOS PESSOAIS? .....	2
3. QUAL BASE LEGAL PARA O TRATAMENTO DE DADOS DESTA SERVENTIA? .....	2
4. QUAL A NECESSIDADE DA ELABORAÇÃO DO PRESENTE RIPD? .....	3
5. COMO É REALIZADO O TRATAMENTO DE DADOS EM NOSSA SERVENTIA? .....	4
5.1 O QUE É TRATAMENTO DE DADOS? .....	4
5.2 QUAIS PRINCÍPIOS NORTEIAM O TRATAMENTO DE DADOS DE NOSSA SERVENTIA? .....	4
5.3 QUAL A NATUREZA E O ESCOPO DO TRATAMENTO DE DADOS PESSOAIS POR NOSSA SERVENTIA? .....	6
5.4 QUAL O CONTEXTO E A FINALIDADE DO TRATAMENTO DE DADOS PESSOAIS POR NOSSA SERVENTIA? .....	8
6. QUEM A NOSSA SERVENTIA CONSULTOU PARA REALIZAR O PRESENTE RIPD? .....	9
7. QUAIS MEDIDAS NOSSA SERVENTIA ADOTA PARA ASSEGURAR O CUMPRIMENTO DA NOSSA POLÍTICA DE PROTEÇÃO DE DADOS? .....	10
8. QUAIS OS RISCO NO TRATAMENTO DE DADOS PELO NOSSO CARTÓRIO? .....	10
9. QUAIS AS MEDIDAS NOSSA SERVENTIA ADOTA PARA TRATAR OS RISCOS? .....	14
10. O QUE FAZER NO CASO DA OCORRÊNCIA DE VAZAMENTO DE DADOS? .....	18
10.1 CLASSIFICAÇÃO DO VAZAMENTO.....	19
10.2 MEDIDAS INICIAIS.....	20
10.2.1 POSSÍVEIS CAUSAS.....	20
10.2.2 CONTENÇÃO.....	20
10.3 ANÁLISE, COMUNICADOS E AÇÕES.....	21
11. APROVAÇÃO DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS DA NOSSA SERVENTIA.....	23

## 1. OBJETIVO.

O presente **Relatório de Impacto à Proteção de Dados Pessoais** integra o nosso Programa de Adequação a Lei Geral de Proteção de Dados Pessoais.

Este documento objetiva abordar os processos de tratamentos de dados pessoais utilizados por nossa serventia, bem como as medidas e meios para resguardar e mitigar os riscos em nossa atividade diária.

Nossa Serventia possui compromisso e integridade no tratamento de dados dos usuários de nossos serviços e de nossos colaboradores. Porquanto, elaboramos o presente relatório em conformidade com o Provimento CNJ de nº 134/2022 e a Lei nº 13.709/2018, a fim de aprimorar nosso Programa de Proteção de Dados Pessoais.

---

## 2. QUEM SÃO OS AGENTES DE TRATAMENTO E OS ENCARREGADOS DOS DADOS PESSOAIS?

- **Controlador:** Cartório do Registro Civil e Tabelionato do Distrito de Carapina do Juízo de Serra da Comarca da Capital/ES;
- **Operador:** Silvio dos Santos Neto;
- **Encarregado:** Caio Cesar Cordeiro Francisco
  - **E-mail:** [dpo@cartoriocarapina.com.br](mailto:dpo@cartoriocarapina.com.br)

---

## 3. QUAL BASE LEGAL PARA O TRATAMENTO DE DADOS DESTA SERVENTIA?

Os serviços prestados pelas serventias extrajudiciais são realizados em caráter privado por delegação do Poder Público (*vide* art. 236 CF/88) e possuem a incumbência legal de garantir a publicidade, autenticidade,

segurança e eficácia dos atos jurídicos (*vide* Lei 8.935/94 e Lei 6.015/73). Desta forma, para exercer as atividades estipuladas por lei é indispensável que nossa serventia realize o tratamento de dados dos titulares que utilizam nossos serviços, conforme estipulado nesse RIPD.

O referido tratamento de dados pessoais por nossa serventia também se fundamenta na Lei Geral de Proteção de Dados, eis que ao regulamentar essa matéria, 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 registras e na Lei Geral de Proteção de Dados.

---

#### **4. QUAL A NECESSIDADE DA ELABORAÇÃO DO PRESENTE RIPD?**

Em decorrência da Lei Geral de Proteção de Dados (13.709/2018) o Conselho Nacional de Justiça – CNJ editou o Provimento nº 134/2022 que estabeleceu medidas a serem adotadas pelas serventias extrajudiciais. Dentre as várias medidas estipuladas pelo referido provimento, o inciso III do art. 6º trouxe a exigência da elaboração de Relatório de Impacto à Proteção de Dados Pessoais – RIPD.

Além disso, o referido relatório tem a finalidade de demonstrar o

mapeamento e o Inventário de Dados Pessoais e Dados Pessoais Sensíveis desta Serventia Extrajudicial, o objeto de seu tratamento e o seu ciclo de vida, fazendo do RIPD parte integrante, indissociável e **complementar** à Política de Proteção de Dados deste cartório.

---

## 5. COMO É REALIZADO O TRATAMENTO DE DADOS EM NOSSA SERVENTIA?

### 5.1 O QUE É TRATAMENTO DE DADOS?

Para que haja uma adequada compreensão deste RIPD, 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).

Fica fácil, com isso, compreender, que todo cartório realiza vários (se não todos) destes atos de tratamento e, muitas vezes, em grande volume e quantidade.

### 5.2 QUAIS PRINCÍPIOS 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 ser solicitados e utilizados somente os dados estritamente necessários para 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 a todas as exigências do Provimento CNJ n. 134/2022 para prevenir e garantir segurança dos dados de nossos usuários.
- e) **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, em conformidade com o Provimento CNJ n. 134/2022, dando-lhe o direito de preencher formulário próprio para exercício do seu direito de Titular dos Dados

### 5.3 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:

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

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

- Abertura de Cartão de Firma
- Apostilamento de Haia
- Ata Notarial (Constatação de fatos)
- Ata Notarial de Usucapião
- Certificado E-Notariado
- Cessão de Direitos Hereditários
- Comunicado de Venda de Veículos
- Cópia Autenticada
- Divórcio / Dissolução de União Estável
- Emancipação
- Escritura de Compra e Venda
- Escritura de Compra e Venda ou Doação
- Escritura de Compra e Venda ou Doação – Imóvel Rural
- Escritura Declaratória
- Escritura Pública de Doação
- Escritura de União Estável
- Inventário / Partilha / Nomeação de Inventariante
- Procuração
- Reconhecimento de Firma
- Testamento
- Averbação de Alteração de Nome e Gênero
- Averbação de Alteração de Prenome
- Averbação de Divórcio / Separação
- Averbação de Inclusão de Sobrenomes
- Averbação de Retificação
- Casamento
- Carteira de Identidade
- Inclusão / Regularização de CPF
- Registro de Nascimento
- Reconhecimento de Paternidade
- Reconhecimento de Paternidade / Maternidade Socioafetivo
- Registro de Óbito

Ato contínuo, cabe enfatizar que dos dados elencados acima, apenas a foto do usuário e os de natureza biométrica (digital) são coletados de forma rotineira em nossa serventia para os fins de cadastros de nossos usuários com o intuito de aprimorar a sua própria segurança na obtenção e emissão de certidões, além da realização de atos cartorários de forma online, 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.

Outro ponto a ser elencado é que nossa serventia, sempre que possível, exime-se de coletar dados referentes ao sexo (masculino/feminino) do usuário de nossos serviços, eis ser uma informação dispensada pelo art. 2º do Provimento do CNJ nº 61/2017, que regulamenta a qualificação em requerimentos para a prática de atos e serviços cartorários.

Por fim, cabe destacar que as informações sobre armazenamento, compartilhamento, medidas de segurança e eliminação dos dados tratados por nossa serventia se encontram exemplificados em nossa Política de Proteção de Dados.

#### 5.4 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, nossa 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.

---

## 6. QUEM A NOSSA SERVENTIA CONSULTOU PARA REALIZAR O PRESENTE RIPD?

Temos a consciência do grau de importância do presente Relatório de Impacto, eis que através dele nossa serventia reforça o compromisso e integridade no tratamento de dados dos usuários de nossos serviços e de nossos colaboradores, bem como que nele constará os nossos processos de tratamentos de dados pessoais e as medidas e meios para resguardar e mitigar os riscos em nossa atividade diária.

Diante disto, na elaboração do presente RIPD, consultamos o escritório **MENDES ADVOCACIA**. Pois, eles possuem vasta experiência na implementação e adequação a LGPD em serventias extrajudiciais em todo o Brasil, com ênfase no Estado do Espírito Santo.

---

## 7. QUAIS MEDIDAS NOSSA SERVENTIA ADOTA PARA ASSEGURAR O CUMPRIMENTO DA NOSSA POLÍTICA DE PROTEÇÃO DE DADOS?

A Política de Proteção de Dados de nossa serventia é composta por diversas medidas técnicas e organizacionais, dentre as quais destacamos:

- Encarregado pela proteção de dados;
- Relatório de Impacto à Proteção de Dados Pessoais;
- Política de Privacidade e de Segurança e Regimento Interno;

Com o objetivo de assegurar o cumprimento das medidas técnicas e organizacionais implementadas, nossa serventia promove a publicidade do nosso Programa de Proteção de Dados para os usuários de nossos serviços, para nossos colaboradores e para terceiros que possuem interesse.

Ademais, realizamos treinamentos com nossos colaboradores, a fim de capacitá-los para tratarem os dados pessoais e pessoais sensíveis conforme estabelecemos em nosso Programa de Proteção de Dados que está em conformidade com a LGPD e o Provimento CNJ nº 134/2022.

Por fim, com a finalidade de promovermos maior transparência no tratamento de dados por nossa serventia, nomeamos como encarregado pela proteção de dados o(a) Sr(a). **Caio Cesar Cordeiro Francisco**, bem como disponibilizamos o e-mail [dpo@cartoriocarapina.com.br](mailto:dpo@cartoriocarapina.com.br) como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados – ANPD.

## 8. QUAIS OS RISCO NO TRATAMENTO DE DADOS PELO NOSSO CARTÓRIO?

A LGPD ao conceituar o **Relatório de Impacto à Proteção de Dados Pessoais** definiu que ele é o documento pelo qual o controlador irá descrever os processos de tratamento de dados pessoais e definir quais medidas são

tomadas para diminuir os riscos de incidentes.

Contudo, antes de elencar quais medidas serão tomadas é importante definir quais os riscos no tratamento de dados pessoais realizado por nossa serventia e qual o grau de impacto potencial sobre o titular dos referidos dados.

Para estipular o grau de impacto, nossa Serventia utilizou os seguintes parâmetro escalares que levam em consideração a **Probabilidade** de ocorrência do evento de risco e o possível **Impacto** que tal evento pode gerar. Desta forma, seguimos os presentes parâmetros escalares:

<b>CLASSIFICAÇÃO</b>	<b>VALOR</b>
<b>Baixo</b>	5
<b>Moderado</b>	10
<b>Alto</b>	15

Seguindo os parâmetros escalares estabelecidos pela tabela acima, conseguimos elaborar a **Matriz Probabilidade x Impacto**. A elaboração da referida matriz é fundamental para embasarmos as classificações do nível de risco.

Probabilidade (P)	15	75	150	225
	10	50	100	150
	5	25	50	75
		5	10	15
		Impacto (I)		

Para melhor exemplificar a matriz acima, é importante destacarmos que as cores que preenchem cada área representam o seguinte:

- **Verde** → Risco Baixo;
- **Amarelo** → Risco Moderado;
- **Vermelho** → Risco Alto.

Estabelecido os parâmetros escalares e a Matriz Probabilidade x Impacto que nossa serventia seguirá para classificar os riscos inerentes ao tratamento de dados pessoais por nossa serventia em decorrência de nossas atividades estabelecidas por lei, faz-se necessário elencar quais os risco relacionados ao tratamento de dados pessoais por nossa serventia.

Para tanto, elaboramos a tabela a seguir:

<b>Id</b>	<b>Riscos referente ao tratamento de dados pessoais</b>	<b>P</b>	<b>I</b>	<b>Nível de Risco (P x I)</b>
<b>R01</b>	Acesso não autorizado.	10	15	150
<b>R02</b>	Modificação não autorizada.	10	15	150
<b>R03</b>	Perda.	5	15	75
<b>R04</b>	Roubo.	5	15	75
<b>R05</b>	Remoção não autorizada.	5	15	75
<b>R06</b>	Coleta excessiva de dados.	10	10	100
<b>R07</b>	Informação Insuficiente sobre a finalidade do tratamento.	10	15	150
<b>R08</b>	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não seja previsto em legislação ou regulamentação pertinente).	10	15	150
<b>R09</b>	Falha em considerar os direitos do titular dos dados pessoais (Ex. Perda do direito de acesso).	5	15	75
	Compartilhar ou distribuir dados pessoais com terceiros sem amparo legal.			

<b>R10</b>		10	15	150
<b>R11</b>	Retenção prolongada de dados pessoais sem necessidade.	10	5	50
<b>R12</b>	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	15	75
<b>R13</b>	Falha/erro de processamento.	5	15	75
<b>R14</b>	Reidentificação de dados pseudonimizados.	5	15	75

## 9. QUAIS AS MEDIDAS NOSSA SERVENTIA ADOTA PARA TRATAR OS RISCOS?

Estabelecemos no tópico anterior quais os riscos no tratamento de dados realizado por nossa serventia e qual o grau de risco que ele representa. Tal parâmetro se faz necessário para identificarmos e definirmos quais medidas de segurança, técnicas e administrativas adotaremos para proteger os dados pessoais dos usuários de nossos serviços.

Ademais, cabe esclarecer que as medidas adotadas por nossa serventia possuem o objetivo de eliminar, reduzir ou amenizar os riscos estabelecidos no tópico anterior.

Diante disto, para melhor visualização, confeccionamos a tabela a seguir, a fim de demonstrar quais medidas a nossa serventia adota

para tratar os riscos oriundos de nossas atividades estabelecidas por lei.

Risco	Medida(s)	Efeito sobre o Risco	Risco Residual			Medida (s) Aprova da(s)
			P	I	Nível (P x I)	
<b>R01</b>	<ul style="list-style-type: none"> <li>• Controle de acesso;</li> <li>• Segurança em rede.</li> </ul>	Reduzir	5	10	50	Sim
<b>R02</b>	<ul style="list-style-type: none"> <li>• Termo de responsabilidade;</li> <li>• Treinamentos;</li> <li>• Rastreabilidade</li> </ul>	Reduzir	5	10	50	Sim
<b>R03</b>	<ul style="list-style-type: none"> <li>• Cópia digital dos arquivos físicos;</li> <li>• Backup dos arquivos digitais.</li> </ul>	Reduzir	5	5	25	Sim
<b>R04</b>	<ul style="list-style-type: none"> <li>• Controle de acesso;</li> <li>• Segurança em rede (criptografada);</li> <li>• Câmeras de segurança.</li> </ul>	Reduzir	5	10	50	Sim
	<ul style="list-style-type: none"> <li>• Termo de</li> </ul>					



<b>R05</b>	responsabilidade; <ul style="list-style-type: none"> <li>• Treinamentos;</li> <li>• Rastreabilidade.</li> </ul>	Reduzir	5	5	25	Sim
<b>R06</b>	<ul style="list-style-type: none"> <li>• Limitação da coleta;</li> <li>• Estabelecimento da finalidade do tratamento.</li> </ul>	Reduzir	5	5	25	Sim
<b>R07</b>	<ul style="list-style-type: none"> <li>• Política de Proteção de Dados;</li> <li>• Rotinas Internas;</li> <li>• Treinamentos;</li> <li>• Publicidade das medidas adotadas.</li> </ul>	Reduzir	5	5	25	Sim
<b>R08</b>	<ul style="list-style-type: none"> <li>• Previsão legal para o tratamento;</li> <li>• Art. 236, CF/88; Leis 8.935/94 e 6.015/73; Art. 7º, II e IX da LGPD.</li> </ul>	Reduzir	5	5	25	Sim
<b>R09</b>	<ul style="list-style-type: none"> <li>• Política de Proteção de Dados;</li> <li>• Rotinas Internas;</li> <li>• Treinamentos.</li> </ul>	Reduzir	5	5	25	Sim

<b>R10</b>	<ul style="list-style-type: none"> <li>• Política de Proteção de Dados;</li> <li>• Rotinas Internas;</li> <li>• Treinamentos;</li> <li>• Publicidade;</li> <li>• Atribuição legal.</li> </ul>	Reduzir	5	10	50	Sim
<b>R11</b>	<ul style="list-style-type: none"> <li>• Política de Proteção de Dados;</li> <li>• Rotinas Internas;</li> <li>• Treinamentos;</li> <li>• Atribuição legal.</li> </ul>	Reduzir	5	5	25	Sim
<b>R12</b>	<ul style="list-style-type: none"> <li>• Política de Proteção de Dados;</li> <li>• Rotinas Internas;</li> <li>• Treinamentos;</li> <li>• Atribuição legal.</li> </ul>	Reduzir	5	10	50	
<b>R13</b>	<ul style="list-style-type: none"> <li>• Atualizações periódicas dos sistemas.</li> </ul>	Reduzir	5	5	25	Sim
<b>R13</b>	<ul style="list-style-type: none"> <li>• Política de Proteção de Dados;</li> <li>• Rotinas Internas;</li> <li>• Treinamentos;</li> </ul>	Reduzir	5	10	50	Sim

	• Atribuição legal.					
--	---------------------	--	--	--	--	--

No mais, nossa serventia esclarece que as medidas adotadas acima, possuem o objetivo de proteger os dados pessoais sensíveis dos usuários de nossos serviços de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Nossa Serventia também contratou a prestação de serviços do Software Makrolock que proporciona o monitoramento das atividades dos funcionários e a segurança contra vazamentos ao criar mecanismos que evitam a cópias de dados dos dispositivos de nosso Cartório.

Por fim, mesmo diante de todas as medidas adotadas, caso ocorra algum incidente de segurança, nossa serventia se reunirá imediatamente com o setor jurídico e o encarregado pela proteção de dados (DPO) e adotaremos as medidas cabíveis para mitigar, anular ou reduzir os impactos do incidente, além de comunicar em até 48 horas úteis (a contar do conhecimento dos fatos) a Autoridade de Proteção de Dados (ANPD), ao Juiz Corregedor Permanente e a Corregedoria Geral da Justiça.

---

## 10. O QUE FAZER NO 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.

## 10.1 CLASSIFICAÇÃO DO VAZAMENTO

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

- Física;
- Digital;
- Em pequeno volume;
- Em Grande Volume;
- Dados de baixo impacto.

A forma de vazamento física consiste no acesso não autorizado por terceiros de atos cartorários ou registrais, 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 registrais, ou ainda os que não se tornaram atos ou documentos “públicos”, como minutas ou 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.

## 10.2 MEDIDAS INICIAIS

### 10.2.1 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):

- Vazamento doloso causado por colaborador ou ex colaborador;
- Vazamento culposo causado por colaborador
- Vazamento decorrente de acesso hacker
- Vazamento decorrente de perda de backup em instrumento físico (pen drives, Hd's)
- Vazamento por compartilhamento de dispositivos telemáticos (smartfones, computadores, notebooks institucionais ou pessoais com acesso aos sistemas e redes do cartório);
- 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.*

### 10.2.2 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:

- 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);
- 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;
- Se de qualquer outra forma, incluindo a promovida por operadores de dados: promover a imediata substituição de todas as senhas de acessos a todo e qualquer dispositivo telemático da serventia.

Em qualquer dos casos, o Encarregado de Proteção de Dados deverá se fazer presente e recomendar a medida adequada.

### 10.3 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:

- **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 uma ficha de firma. O usuário (titular dos dados) deve ser comunicado para que possa criar

uma nova firma e não ficar sujeito à fraudes por reconhecimentos promovidos por impostores.

Um outro exemplo é o caso do vazamento de uma ata notarial 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 dar publicidade e disseminação à informação.

- **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 2 dias.

O comunicado deverá conter:

- Data e hora da detecção;
- Circunstâncias em que ocorreu a violação de segurança de dados pessoais, por exemplo, perda, roubo, cópia, vazamento, dentre outros;
- Descrição dos dados pessoais e informações afetadas, como natureza e conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados;
- Resumo do incidente de segurança com dados pessoais, com indicação da localização física e meio de armazenamento;
- Possíveis consequências e efeitos negativos sobre os titulares dos dados afetados;
- Medidas de segurança, técnicas e administrativas preventivas

tomadas pelo controlador de acordo com a LGPD;

- Resumo das medidas implementadas até o momento para controlar os possíveis danos;
- 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.***

---

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

O presente RIPD 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:

- Responsável pela elaboração do RIPD;
- Encarregado de dados;
- Representante do Controlador;
- Representante do Operador.

No mais, nossa serventia possui a consciência que o mundo é dinâmico e, por consequência, existem variações de cenários tecnológicos, normativos, políticos e institucionais. Diante disto, a fim de



demonstrar nosso compromisso e responsabilidade, avaliamos continuamente os riscos no tratamento de dados pessoais através da revisão deste RIPD anualmente ou sempre que surgir qualquer mudança significativa.

<b>RESPONSÁVEL PELA ELABORAÇÃO DO RIPD</b>	<b>ENCARREGADO</b>
Cleylton Mendes Passos	Caio Cesar Cordeiro Francisco
<b>REPRESENTANTE DO CONTROLADOR</b>	<b>REPRESENTANTE DO OPERADOR</b>
Silvio dos Santos Neto	Silvio dos Santos Neto