1. APRESENTAÇÃO

A presente Política de Segurança da Informação ("PSI") estabelece os princípios, diretrizes, responsabilidades e controles mínimos de segurança da informação adotados pelo 1° Oficial de Registro de Imóveis, Títulos e Documentos e Civil de Pessoa Jurídica da Comarca de Jundiaí com o objetivo de garantir a confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade e continuidade dos serviços prestados.

Esta Política observa as determinações da Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018), da Lei nº 8.935/1994, da Lei nº 6.015/1973, bem como do Provimento CNJ nº 213/2026, que estabelece os padrões mínimos de tecnologia da informação e comunicação aplicáveis às serventias extrajudiciais.

2. OBJETIVO

A presente Política tem como finalidade:

I – Estabelecer normas e controles de segurança da informação aplicáveis aos ativos físicos, digitais e documentais da serventia;

II – Garantir a proteção do acervo registral e notarial físico e eletrônico;

III – Assegurar a continuidade operacional dos serviços extrajudiciais;

IV – Prevenir incidentes de segurança da informação e violações de dados pessoais;

V – Definir responsabilidades relacionadas ao uso adequado dos recursos tecnológicos;

VI – Garantir conformidade com o Provimento CNJ nº 213/2026, à LGPD e às demais normas aplicáveis.

3. APLICAÇÃO

3.1. Esta Política aplica-se:

a) ao Oficial Titular;

b) substitutos;

c) escreventes;

d) colaboradores;

e) estagiários/jovens aprendizes;

f) prestadores de serviço;

g) fornecedores;

h) terceiros que tenham acesso aos sistemas, redes, documentos, bases de dados ou informações da serventia.

3.2. Todos os usuários devem observar integralmente esta Política e demais normas internas relacionadas à segurança da informação.

3.3. O descumprimento desta Política poderá acarretar medidas administrativas, civis, penais e disciplinares.

4. BASE LEGAL E NORMAS RELACIONADAS

Esta Política fundamenta-se especialmente em:

4.1. Lei nº 13.709/2018 – LGPD;

4.2. Lei nº 13.853/2019;

4.3. Lei nº 8.935/1994;

4.4. Lei nº 6.015/1973;

4.5. Provimento CNJ nº 213/2026;

4.6. Normativos da Corregedoria Nacional de Justiça e da Corregedoria Geral da Justiça;

4.7. Política de Privacidade e Proteção de Dados da Serventia.

5. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

A serventia observará os seguintes princípios:

I – Confidencialidade;

II – Integridade;

III – Disponibilidade;

IV – Autenticidade;

V – Rastreabilidade;
VI – Continuidade dos serviços;
VII – Prevenção;
VIII – Responsabilização;
IX – Transparência;
X – Proporcionalidade regulatória.

---

6. GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO

6.1. A serventia deverá manter estrutura de governança de segurança da informação compatível com seu porte, risco operacional e exigências legais.
6.2. O Oficial responderá pela implementação e manutenção dos controles de segurança.
6.3. O encarregado de proteção de dados (DPO) atuará conjuntamente com a área de tecnologia da informação na supervisão das medidas de proteção de dados pessoais.
6.4. A serventia deverá manter políticas, procedimentos, inventários e registros técnicos atualizados.

---

7. CLASSIFICAÇÃO DA INFORMAÇÃO

7.1. As informações deverão ser classificadas conforme seu nível de sensibilidade e criticidade.
7.2. Poderão ser adotadas, entre outras, as seguintes classificações:
a) Pública;
b) Uso Interno;
c) Restrita;
d) Confidencial.
7.3. O acesso às informações observará o princípio do menor privilégio.

---

8. CONTROLE DE ACESSO

8.1. O acesso aos sistemas e informações será concedido apenas mediante autorização formal.
8.2. Todo usuário deverá possuir identificação individual e intransferível.
8.3. É obrigatória a utilização de senhas fortes e periódica alteração das credenciais.
8.4. Sempre que tecnicamente possível, deverá ser implementada autenticação multifator (MFA).
8.5. Os acessos deverão ser registrados e auditáveis.
8.6. Os acessos deverão ser imediatamente revogados em caso de desligamento ou alteração de função.

---

9. SEGURANÇA DOS SISTEMAS E INFRAESTRUTURA

9.1. Os sistemas utilizados deverão possuir suporte técnico, atualizações de segurança e mecanismos de proteção contra vulnerabilidades.
9.2. A serventia deverá manter:
a) antivírus corporativo;
b) firewall;
c) sistemas de monitoramento;
d) mecanismos de proteção contra ransonware;
e) segregação de acessos administrativos;
f) registro de logs;
g) proteção contra acessos não autorizados.
9.3. Equipamentos e softwares obsoletos deverão ser substituídos ou isolados.
9.4. As redes sem fio deverão possuir criptografia adequada e controle de acesso.

---

10. BACKUP E CONTINUIDADE DE NEGÓCIOS

10.1. A serventia deverá manter política formal de backup.
10.2. Os backups deverão:
a) ser automatizados;
b) possuir periodicidade definida;

c) ser armazenados de forma segura;
d) possuir cópia externa ou em nuvem;
e) permitir restauração íntegra e auditável.
10.3. Os procedimentos de restauração deverão ser testados periodicamente.
10.4. A serventia deverá manter Plano de Continuidade de Negócios (PCN) e Plano de Recuperação de Desastres (PRD).
10.5. Os planos deverão prever contingência operacional para indisponibilidade tecnológica, incidentes cibernéticos e desastres físicos.

11. PROTEÇÃO DE DADOS PESSOAIS

11.1. O tratamento de dados pessoais deverá observar a LGPD e a Política de Privacidade da serventia.
11.2. Dados pessoais e sensíveis deverão possuir proteção compatível com sua criticidade.
11.3. Os dados somente poderão ser acessados por usuários autorizados e para finalidade legítima.
11.4. Sempre que possível, deverão ser aplicadas técnicas de anonimização, pseudonimização e criptografia.
11.5. O compartilhamento de dados com terceiros deverá observar contrato ou instrumento jurídico compatível com a LGPD.

12. REGISTROS, LOGS E RASTREABILIDADE

12.1. Os sistemas utilizados deverão permitir rastreabilidade das operações realizadas.
12.2. Os logs deverão registrar, minimamente:
a) identificação do usuário;
b) data e hora;
c) operação realizada;
d) origem do acesso;
e) alterações efetuadas.
12.3. Os registros deverão ser protegidos contra alteração ou exclusão indevida.

13. GESTÃO DE INCIDENTES DE SEGURANÇA

13.1. Todo incidente de segurança deverá ser imediatamente comunicado à administração da serventia.
13.2. A serventia deverá manter Plano de Resposta a Incidentes.
13.3. O plano deverá prever:
a) identificação;
b) contenção;
c) mitigação;
d) recuperação;
e) comunicação;
f) registro de evidências;
g) medidas corretivas.
13.4. Violações de dados pessoais deverão ser comunicadas à ANPD e às autoridades competentes quando exigido pela legislação aplicável.

14. USO ACEITÁVEL DOS RECURSOS TECNOLÓGICOS

14.1. Os recursos tecnológicos da serventia destinam-se exclusivamente às atividades profissionais e institucionais.
14.2. É proibido:
a) compartilhar senhas;
b) instalar softwares não autorizados;
c) acessar conteúdo ilícito;
d) utilizar dispositivos pessoais sem autorização;
e) remover informações sem autorização formal;
f) burlar mecanismos de segurança.

15. SEGURANÇA FÍSICA

15.1. O acesso às áreas técnicas deverá ser controlado.

15.2. Equipamentos críticos deverão permanecer em ambientes protegidos.

15.3. Documentos físicos contendo informações sensíveis deverão ser armazenados adequadamente.

15.4. A serventia deverá adotar proteção contra incêndio, falhas elétricas e acessos indevidos.

---

16. TREINAMENTO E CONSCIENTIZAÇÃO

16.1. Todos os colaboradores deverão receber treinamento periódico em:

a) segurança da informação;

b) proteção de dados pessoais;

c) prevenção contra phishing e engenharia social;

d) boas práticas de segurança;

e) resposta a incidentes.

16.2. A serventia poderá realizar campanhas internas de conscientização.

---

17. AUDITORIA E CONFORMIDADE

17.1. A serventia poderá realizar auditorias internas e externas para verificação da conformidade desta Política.

17.2. Os controles de segurança deverão ser revisados periodicamente.

17.3. A serventia deverá manter evidências documentais e técnicas de conformidade.

---

18. TRANSFERÊNCIA DE ACERVO E SUCESSÃO

18.1. A serventia deverá garantir a transferência organizada e íntegra dos acervos físicos e digitais em caso de sucessão, interinidade ou intervenção.

18.2. A transferência deverá incluir:

a) bases de dados;

b) sistemas;

c) inventário tecnológico;

d) registros de acesso;

e) políticas internas;

f) documentação técnica.

---

19. RETENÇÃO E DESCARTE DE INFORMAÇÕES

19.1. Informações e documentos deverão observar os prazos legais de guarda.

19.2. O descarte deverá ocorrer de forma segura e rastreável.

19.3. Mídias eletrônicas deverão ser inutilizadas de modo a impedir recuperação indevida das informações.

---

20. DISPOSIÇÕES FINAIS

20.1. Esta Política entra em vigor na data de sua aprovação.

20.2. Esta Política deverá ser revisada periodicamente, especialmente em razão de alterações legislativas, regulatórias ou tecnológicas.

20.3. Casos omissos serão analisados pela administração da serventia em conjunto com o encarregado de proteção de dados e responsáveis técnicos.

---

21. APROVAÇÃO

A presente Política de Segurança da Informação foi aprovada pelo Oficial Titular do 1° Oficial de Registro de Imóveis, Títulos e Documentos e Civil de Pessoa Jurídica da Comarca de Jundiaí em conjunto com a Diretora Administrativa e a Encarregada de Proteção de Dados (DPO), passando a vigorar na data de sua publicação interna.

CONTROLE DE REVISÕES:

DATA: 22/05/2026
APROVAO POR: Renata Bettinelli
ELABORAÇÃO INICIAL: Rev.00