



POLÍTICA INTERNA DE SEGURANÇA DA INFORMAÇÃO

Documento	Política Interna de Segurança da Informação – PISI
Versões anteriores	1.0 2.0 3.0 4.0
Versão	5.0
Data de aprovação	Maio de 2026
Responsável	Lorenço Boing Sobrinho
Base normativa	Provimento n. 213/2026 – CNJ LGPD (Lei 13.709/2018)
Classificação	Documento Interno – Uso Institucional
Próxima revisão	Maio de 2027



SUMÁRIO

SUMÁRIO	2
1. APRESENTAÇÃO	4
2. IDENTIFICAÇÃO DA SERVENTIA	4
3. OBJETIVOS	4
3.1 Objetivo Geral	4
3.2 Objetivos Específicos	4
4. ÂMBITO DE APLICAÇÃO	5
5. BASE NORMATIVA E REFERÊNCIAS	5
6. PRINCÍPIOS E DIRETRIZES	5
6.1 Confidencialidade	5
6.2 Integridade	5
6.3 Disponibilidade	5
6.4 Autenticidade	6
6.5 Rastreabilidade	6
6.6 Conformidade Legal	6
7. CLASSIFICAÇÃO DA INFORMAÇÃO	6
8. CONTROLE DE ACESSO E AUTENTICAÇÃO	6
8.1 Princípios de Controle de Acesso	6
8.2 Gestão de Credenciais	7
8.3 Controle de Acessos Privilegiados	7
8.4 Revogação de Acessos	7
9. SEGURANÇA FÍSICA E DO AMBIENTE	7
9.1 Controle de Acesso Físico	7
9.2 Proteção de Equipamentos	7
9.3 Proteção Contra Ameaças Ambientais	7
10. SEGURANÇA DE SISTEMAS E REDES	7
10.1 Softwares e Licenciamento	7
10.2 Atualizações e Correções de Segurança	8
10.3 Criptografia – Obrigatória para Classe 3	8
10.4 Proteção Contra Malware e Ataques	8
10.5 Teste de Intrusão (Pentest) – Obrigatório para Classe 3	8
10.6 Gestão de Redes	8
11. BACKUP, RECUPERAÇÃO DE DADOS E CONTINUIDADE	8
11.1 Política de Backup – Requisitos para Classe 3	8
11.2 Testes de Restauração – Periodicidade Classe 3	9
11.3 Parâmetros Obrigatórios de Continuidade – Classe 3	9
11.4 Plano de Continuidade de Negócios (PCN) e Plano de Recuperação de Desastres (PRD)	9
12. GESTÃO DE INCIDENTES DE SEGURANÇA	10
12.1 Classificação de Incidentes	10
12.2 Protocolo de Resposta	10
12.3 Registro de Incidentes	10
13. PROTEÇÃO DE DADOS PESSOAIS (LGPD)	10
13.1 Princípios do Tratamento de Dados	10
13.2 Encarregado de Proteção de Dados (DPO)	11
13.3 Registro das Operações de Tratamento	11
13.4 Direitos dos Titulares	11
14. INVENTÁRIO E GESTÃO DE ATIVOS TECNOLÓGICOS	11
14.1 Categorias de Ativos	11
14.2 Controles de Inventário	11
15. CAPACITAÇÃO E CONSCIENTIZAÇÃO	11
16. GESTÃO DE TERCEIROS E FORNECEDORES	12
17. AUDITORIA, MONITORAMENTO E CONFORMIDADE	12
17.1 Trilhas de Auditoria – Nível Ampliado (Classe 3)	12
17.2 Monitoramento Contínuo	12
17.3 Declaração no Sistema Justiça Aberta	12
17.4 Dossiê Técnico	12
18. REVISÃO E ATUALIZAÇÃO DESTA POLÍTICA	13



Cartório do 1º Ofício de Alta Floresta
Registro de Imóveis
Registro de Títulos e Documentos



19. DISPOSIÇÕES FINAIS E VIGÊNCIA.....	13
ANEXO I – TERMO DE CIÊNCIA E COMPROMISSO	Erro! Indicador não definido.
ANEXO II – FORMULÁRIO DE REGISTRO DE INCIDENTES	Erro! Indicador não definido.
ANEXO III – CRONOGRAMA DE IMPLEMENTAÇÃO – CLASSE 3.....	Erro! Indicador não definido.
ANEXO IV – REGISTRO DE TESTE DE RESTAURAÇÃO DE BACKUP	Erro! Indicador não definido.



1. APRESENTAÇÃO

A presente Política Interna de Segurança da Informação (PISI) do Cartório de Registro de Imóveis do 1º Ofício de Alta Floresta foi elaborada em cumprimento ao Provimento n. 213, de 20 de fevereiro de 2026, expedido pela Corregedoria Nacional de Justiça do Conselho Nacional de Justiça (CNJ), que estabelece os padrões mínimos de tecnologia da informação e comunicação (TIC) para os serviços notariais e de registro de todo o Brasil.

Esta política representa o compromisso desta serventia com a segurança, a integridade, a disponibilidade, a autenticidade e a rastreabilidade de todos os atos registrais praticados, bem como com a proteção dos dados pessoais dos usuários, em conformidade com a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei n. 13.709/2018).

O Cartório de Registro de Imóveis do 1º Ofício de Alta Floresta reconhece seu papel como instituição de organização técnica e administrativa destinada a assegurar a publicidade, a autenticidade, a segurança e a eficácia dos atos jurídicos, impondo-se que os meios operacionais e tecnológicos empregados sejam compatíveis com tais finalidades institucionais.

2. IDENTIFICAÇÃO DA SERVENTIA

Denominação	Cartório de Registro de Imóveis do 1º Ofício de Alta Floresta
Natureza jurídica	Serviço extrajudicial delegado pelo Poder Público
Estado	Mato Grosso
Comarca	Alta Floresta
Subordinação	Tribunal de Justiça do Estado de Mato Grosso – TJMT
CNPJ	49.685.895/0001-34
Endereço	Av. Ariosto da Riva, 3029, Setor C, Alta Floresta – MT
Telefone	66 3521-2303
E-mail institucional	adm@1oficioaf.com.br
Oficial Registrador	Lorenço Boing Sobrinho
Classe da serventia	CLASSE 3 – arrecadação bruta semestral acima de R\$ 500.000,00 (art. 16 do Provimento n. 213/2026 – CNJ)

3. OBJETIVOS

3.1 Objetivo Geral

Estabelecer diretrizes, responsabilidades e procedimentos para a gestão da segurança da informação nesta serventia, assegurando a proteção dos dados, sistemas e infraestrutura tecnológica, em conformidade com o Provimento n. 213/2026 do CNJ e demais normas aplicáveis.

3.2 Objetivos Específicos

- Garantir a confidencialidade, a integridade, a disponibilidade, a autenticidade e a rastreabilidade das informações tratadas pela serventia;
- Instituir diretrizes formais de continuidade operacional e preservação de dados;
- Definir mecanismos de controle de acesso, autenticação e responsabilização individual dos colaboradores;
- Estabelecer procedimentos de backup, recuperação de dados e plano de continuidade de negócios;
- Assegurar a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD);
- Definir protocolos de resposta a incidentes de segurança da informação;
- Promover a cultura de segurança da informação entre todos os colaboradores da serventia.



4. ÂMBITO DE APLICAÇÃO

Esta Política aplica-se a:

- O Oficial Registrador titular da delegação;
- Escreventes autorizados e demais colaboradores da serventia;
- Interinos e interventores, quando no exercício das funções;
- Prepostos e terceiros que, a qualquer título, acessem os sistemas, dados ou infraestrutura tecnológica da serventia;
- Fornecedores de tecnologia, suporte técnico e prestadores de serviços que operem com dados ou sistemas desta serventia.

Todos os sujeitos acima elencados estão obrigados a conhecer, observar e cumprir integralmente as disposições desta Política, sendo que o descumprimento sujeitará o infrator às medidas disciplinares, contratuais e legais cabíveis.

5. BASE NORMATIVA E REFERÊNCIAS

Esta Política foi elaborada com fundamento nas seguintes normas e referenciais técnicos:

Norma / Referência	Descrição
Provimento n. 213/2026 – CNJ	Padrões mínimos de TIC para serviços notariais e de registro (revoga o Provimento n. 74/2018)
Lei n. 13.709/2018 – LGPD	Lei Geral de Proteção de Dados Pessoais
Lei n. 6.015/1973	Lei de Registros Públicos (arts. 23 a 26)
Lei n. 8.935/1994	Lei dos Serviços Notariais e de Registro (art. 46)
ABNT NBR ISO/IEC 27001	Sistemas de Gestão de Segurança da Informação
ABNT NBR ISO/IEC 27002	Código de Prática para Controles de Segurança da Informação
ABNT NBR ISO 22301	Gestão de Continuidade de Negócios
Res. CNJ n. 67/2009	Regimento Interno do CNJ
NIST Cybersecurity Framework	Referencial técnico complementar de cibersegurança

6. PRINCÍPIOS E DIRETRIZES

A gestão da segurança da informação nesta serventia orienta-se pelos seguintes princípios, alinhados ao art. 3º do Provimento n. 213/2026:

6.1 Confidencialidade

As informações de caráter sigiloso, em especial dados pessoais e dados sensíveis dos usuários, serão acessadas exclusivamente por pessoas autorizadas, no estrito limite de suas atribuições, conforme os princípios da necessidade e da finalidade previstos na LGPD.

6.2 Integridade

Os dados, registros e documentos eletrônicos serão mantidos em sua forma original e íntegra, sendo vedada qualquer alteração não autorizada ou não rastreável. Mecanismos técnicos de controle de integridade serão implementados e periodicamente verificados.

6.3 Disponibilidade

Os sistemas e serviços serão mantidos disponíveis e acessíveis aos usuários legítimos, observando os parâmetros de RTO (Recovery Time Objective) e RPO (Recovery Point Objective) definidos nos planos de continuidade, conforme a classe desta serventia.



6.4 Autenticidade

A identidade dos usuários, a origem dos documentos e a autoria dos atos registrares serão asseguradas por meio de mecanismos de autenticação robustos, incluindo autenticação multifator para acessos a sistemas e funcionalidades críticas, conforme o art. 5º do Provimento n. 213/2026.

6.5 Rastreabilidade

Toda ação relevante realizada nos sistemas desta serventia será registrada em trilhas de auditoria, assegurando a identificação do usuário responsável, data, hora e natureza da operação, de modo a permitir a responsabilização individual por ações ou omissões.

6.6 Conformidade Legal

Todas as atividades de tratamento de dados e uso de tecnologia observarão rigorosamente a legislação aplicável, em especial a LGPD e as normas expedidas pelo CNJ, pelo TJMT e pela Corregedoria competente.

7. CLASSIFICAÇÃO DA INFORMAÇÃO

As informações tratadas por esta serventia são classificadas conforme o grau de sensibilidade e os requisitos de proteção:

Classificação	Descrição	Exemplos
RESTRITA	Acesso limitado ao Oficial e aos escreventes autorizados e seus auxiliares. Dados pessoais sensíveis e informações protegidas por sigilo legal.	CPF, dados bancários, contratos com garantia hipotecária, certidões negativas, dados de partes
INTERNA	Circulação interna na serventia. Informações de uso operacional que não devem ser divulgadas externamente.	Procedimentos internos, logs de auditoria, senhas de sistemas, inventário de TI
PÚBLICA	Informações de acesso irrestrito, divulgadas em cumprimento ao princípio da publicidade registral.	Certidões de ônus e ações, matrículas públicas, editais, informações sobre funcionamento

Os dados críticos, conforme definição do art. 2º, inciso V, do Provimento n. 213/2026 – que abrange livros e atos eletrônicos, bases registrares, trilhas de auditoria, backups, integrações sistêmicas e dados sensíveis –, receberão tratamento diferenciado com proteção máxima.

8. CONTROLE DE ACESSO E AUTENTICAÇÃO

Em conformidade com o art. 5º do Provimento n. 213/2026, esta serventia adota as seguintes diretrizes de controle de acesso:

8.1 Princípios de Controle de Acesso

- Princípio do menor privilégio: cada usuário receberá apenas os acessos estritamente necessários ao desempenho de suas funções;
- Segregação de funções: atividades críticas serão distribuídas entre diferentes usuários para evitar concentração de poderes;
- Responsabilização individual: é vedado o uso de credenciais compartilhadas, genéricas ou que impeçam a identificação do usuário;
- Autenticação multifator (MFA): obrigatória para todos os acessos a sistemas, bases de dados ou funcionalidades críticas.



8.2 Gestão de Credenciais

- Cada colaborador receberá credenciais individuais e intransferíveis no início de suas atividades;
- O compartilhamento de senhas é estritamente proibido;
- As senhas deverão ter comprimento mínimo de 12 (doze) caracteres, combinando letras maiúsculas, minúsculas, números e caracteres especiais;
- A troca periódica de senhas ocorrerá a cada 90 (noventa) dias, no mínimo;
- Senhas padrão de fábrica devem ser imediatamente alteradas na instalação de qualquer sistema ou equipamento.

8.3 Controle de Acessos Privilegiados

- Perfis de administrador de sistemas serão concedidos apenas a pessoas tecnicamente habilitadas e estritamente necessárias;
- O acesso remoto ao ambiente tecnológico da serventia somente será permitido mediante canais criptografados (VPN ou equivalente);
- Contas técnicas automatizadas para integração entre sistemas deverão ter segregação de privilégios e registro auditável de todas as operações.

8.4 Revogação de Acessos

- Os acessos de colaboradores serão imediatamente revogados em caso de desligamento, afastamento ou mudança de função;
- Revisão semestral de todos os perfis de acesso será realizada para verificar pertinência e adequação.

9. SEGURANÇA FÍSICA E DO AMBIENTE

A proteção física das instalações e dos ativos de tecnologia é parte essencial desta Política:

9.1 Controle de Acesso Físico

- O acesso à área de processamento de dados e servidores será restrito ao Oficial Registrador e a técnicos expressamente autorizados;
- Visitantes e prestadores de serviços somente acessarão áreas sensíveis com autorização prévia e acompanhamento de colaborador autorizado;
- Uso de controles físicos como travas, fechaduras e câmeras de monitoramento nas áreas críticas.

9.2 Proteção de Equipamentos

- Todos os equipamentos serão protegidos contra interrupções de energia por meio de nobreaks (UPS) dimensionados adequadamente;
- O descarte de equipamentos e mídias de armazenamento observará procedimentos de sanitização de dados (formatação segura ou destruição física), vedado o descarte sem eliminação prévia dos dados;
- Equipamentos móveis (notebooks, tablets, smartphones) utilizados para acesso aos sistemas da serventia deverão ter disco criptografado e tela de bloqueio com senha.

9.3 Proteção Contra Ameaças Ambientais

- Adoção de medidas preventivas contra incêndio, inundação, calor excessivo e outras ameaças ambientais nas salas de equipamentos;
- Manutenção preventiva periódica de equipamentos de TI.

10. SEGURANÇA DE SISTEMAS E REDES

10.1 Softwares e Licenciamento

Em conformidade com o art. 4º, §§ 2º e 3º, do Provimento n. 213/2026:

- Todos os softwares utilizados deverão possuir licenciamento regular para uso comercial ou serem de código aberto compatíveis com as normas de segurança;
- É vedada a utilização de sistemas operacionais, aplicações críticas ou componentes tecnológicos com suporte oficial encerrado pelo fabricante (End of Life – EOL);
- A serventia manterá inventário atualizado de todos os softwares, incluindo versão, licença e data de expiração do suporte.



10.2 Atualizações e Correções de Segurança

- Atualizações de segurança (patches) deverão ser aplicadas em prazo máximo de 30 (trinta) dias a contar de sua disponibilização pelo fabricante;
- Vulnerabilidades críticas (conforme definição do art. 2º, inciso XXII, do Provimento n. 213/2026) exigirão medidas imediatas de contenção em até 72 (setenta e duas) horas quando houver exploração ativa ou risco iminente, e tratamento definitivo em até 30 dias.

10.3 Criptografia – Obrigatória para Classe 3

Em conformidade com o art. 9º e Anexo II, item 2, do Provimento n. 213/2026, esta serventia (Classe 3) deverá adotar:

- Criptografia de dados em trânsito: protocolo TLS 1.2 ou superior (preferencialmente TLS 1.3) para toda comunicação de sistemas e transmissão de dados críticos em redes externas ou internas não confiáveis; vedado o uso de SSL, TLS 1.0 e TLS 1.1;
- Criptografia de dados em repouso: padrão equivalente ou superior a AES-256 para todos os dados críticos armazenados em servidores, sistemas de gestão registral e mídias de armazenamento;
- Criptografia obrigatória de todos os backups armazenados externamente, com padrão AES-256 ou superior;
- Gestão formal de chaves criptográficas: controle de acesso às chaves, segregação de funções, registro auditável de operações e revisão periódica das políticas de rotação e custódia;
- Dispositivos móveis que acessem dados críticos da serventia deverão ter armazenamento criptografado.

10.4 Proteção Contra Malware e Ataques

- Todos os equipamentos deverão ter solução de antivírus/antimalware atualizada e ativa;
- Será implementado firewall stateful para controle de tráfego de rede, tanto de entrada quanto de saída;
- O acesso à internet deverá ser realizado por meio de conexão segregada e monitorada;
- É proibida a instalação de softwares não autorizados pelo responsável pelo TI da serventia;
- Proteção específica contra ransomware: backups imutáveis, segmentação de rede e monitoramento de comportamentos anômalos.

10.5 Teste de Intrusão (Pentest) – Obrigatório para Classe 3

Conforme o Guia de Implementação do Provimento n. 213/2026 (Etapa 5, Anexo IV), esta serventia Classe 3 deverá:

- Realizar teste de intrusão (pentest) periódico, conduzido por profissional qualificado ou empresa especializada, como parte da gestão de vulnerabilidades;
- Documentar os resultados do pentest, as vulnerabilidades identificadas, as ações corretivas adotadas e os prazos de mitigação;
- Incluir os resultados e as evidências de mitigação no Dossiê Técnico da serventia.

10.6 Gestão de Redes

- A rede Wi-Fi de uso dos colaboradores será segregada da rede de atendimento ao público e da rede de servidores (segmentação de rede obrigatória);
- Redes sem fio utilizarão criptografia WPA3 ou equivalente superior;
- Firewall stateful configurado com regras de entrada e saída documentadas;
- Todo tráfego de dados críticos em redes externas será criptografado (TLS 1.2+).

11. BACKUP, RECUPERAÇÃO DE DADOS E CONTINUIDADE

Em conformidade com o art. 3º do Provimento n. 213/2026, esta serventia adota as seguintes diretrizes de preservação de dados e continuidade operacional:

11.1 Política de Backup – Requisitos para Classe 3

Em conformidade com o Anexo I, item 5, e o Anexo II, itens 2.1 e 2.2 do Provimento n. 213/2026, os parâmetros abaixo são obrigatórios para esta serventia (Classe 3):

- Backup completo: realizado semanalmente, preferencialmente aos domingos, fora do horário de expediente, de forma automatizada;



Cartório do 1º Ofício de Alta Floresta
Registro de Imóveis
Registro de Títulos e Documentos



- Backup incremental (ou equivalente – replicação contínua, point-in-time recovery): realizado ao menos diariamente, ao término do expediente, de forma a assegurar o RPO de 4 horas;
- Armazenamento obrigatório em dois ambientes tecnicamente independentes: um local (servidor, NAS ou storage da serventia) e um remoto com redundância geográfica (nuvem, mídia offsite ou arquitetura híbrida), conforme art. 12, § 6º do Provimento n. 213/2026;
- Proteção dos backups contra ransomware: cópias imutáveis (immutable backups) ou equivalente, de forma a impedir a criptografia maliciosa das cópias de segurança;
- Criptografia obrigatória de todos os backups armazenados externamente, com padrão equivalente ou superior a AES-256, com chaves gerenciadas pelo Oficial Registrador ou por gestor formalmente designado;
- Retenção mínima de 5 (cinco) anos para dados operacionais e permanente para livros e atos registrai, em conformidade com a legislação registral.

11.2 Testes de Restauração – Periodicidade Classe 3

- Testes documentados de restauração de backup deverão ser realizados SEMESTRALMENTE (mínimo obrigatório para Classe 3, conforme Anexo II do Provimento n. 213/2026), verificando a integridade e a funcionalidade dos dados recuperados;
- Recomenda-se a realização de testes trimestrais para maior segurança operacional;
- Os resultados de cada teste devem ser registrados em formulário próprio (ver Anexo IV desta Política), arquivados no Dossiê Técnico e mantidos por no mínimo 5 anos;
- Simulação anual de desastre (disaster recovery drill) documentando o processo completo de recuperação, com medição efetiva do RTO alcançado;
- Em caso de falha na restauração, o responsável pelo TI deverá ser imediatamente notificado e o incidente registrado conforme o protocolo do Capítulo 12.

11.3 Parâmetros Obrigatórios de Continuidade – Classe 3

Conforme o Provimento n. 213/2026, Anexos I e II, os parâmetros para a Classe 3 são:

Parâmetro	Exigência Classe 3 (Obrigatório)
RPO – Ponto Máximo de Perda de Dados	Máximo de 4 (quatro) horas
RTO – Tempo Máximo de Recuperação	Máximo de 8 (oito) horas
Backup completo	Semanal – automatizado
Backup incremental / replicação	Diário ou contínuo (para atender RPO 4h)
Ambientes de armazenamento	Mínimo 2 (local + remoto com redundância geográfica)
Criptografia dos backups externos	Obrigatória – padrão AES-256 ou superior
Imutabilidade dos backups	Obrigatória – proteção contra ransomware
Teste semestral de restauração	Obrigatório – com registro no Dossiê Técnico
Simulação anual de desastre	Obrigatória – Etapa 5 do Anexo IV
Retenção de dados operacionais	Mínimo 5 anos
Retenção de livros e atos registrai	Permanente

11.4 Plano de Continuidade de Negócios (PCN) e Plano de Recuperação de Desastres (PRD)

Em conformidade com o art. 3º, § 1º, do Provimento n. 213/2026, esta serventia (Classe 3) deverá:

- Implementar as Etapas 1 e 2 (governança, conformidade legal, infraestrutura e continuidade) em até 90 dias a partir de 23 de fevereiro de 2026, ou seja, até 24 de maio de 2026 (art. 20, I, do Provimento n. 213/2026);



Cartório do 1º Ofício de Alta Floresta

Registro de Imóveis

Registro de Títulos e Documentos



- Concluir a implementação integral de todas as 5 etapas do Anexo IV em até 24 meses contados de 23 de fevereiro de 2026, ou seja, até 23 de fevereiro de 2028 (art. 23, I, do Provimento n. 213/2026);
- O PCN e o PRD contemplarão: identificação e avaliação de riscos, medidas de mitigação, providências de curto prazo (até 30 dias) e médio prazo (até 90 dias) para tratamento de incidentes e restauração da normalidade operacional;
- O PCN deverá incluir procedimentos documentados para cenários de falha de energia, falha de hardware crítico, ataque de ransomware, perda de acesso à internet e indisponibilidade do sistema registral;
- O PRD deverá definir os procedimentos de ativação, papéis e responsabilidades, sequência de restauração e critérios de retorno à normalidade.

12. GESTÃO DE INCIDENTES DE SEGURANÇA

Em conformidade com o art. 2º, inciso VII, e o art. 7º, § 3º, do Provimento n. 213/2026, esta serventia adota o seguinte protocolo de gestão de incidentes:

12.1 Classificação de Incidentes

Nível	Exemplos e Critérios
CRÍTICO	Acesso não autorizado a dados registrais, vazamento de dados pessoais, ransomware, indisponibilidade total do sistema por mais de 2 horas, comprometimento de integridade de registros
ALTO	Tentativas de acesso não autorizadas, falhas de backup por mais de 24h, suspeita de malware ativo, indisponibilidade parcial de sistemas críticos
MÉDIO	Falhas de hardware não críticas, lentidão sistêmica persistente, erros de autenticação recorrentes
BAIXO	Incidentes menores sem impacto operacional, falhas de equipamentos periféricos

12.2 Protocolo de Resposta

1. IDENTIFICAÇÃO: Qualquer colaborador que identificar ou suspeitar de incidente deve comunicar imediatamente ao Oficial Registrador;
2. CONTENÇÃO: Isolar o sistema ou equipamento afetado para evitar propagação;
3. AVALIAÇÃO: Determinar a extensão do incidente e classificar o nível de criticidade;
4. NOTIFICAÇÃO: Incidentes críticos devem ser comunicados à Corregedoria do TJMT imediatamente. Incidentes envolvendo dados pessoais com risco relevante aos titulares devem ser comunicados também à ANPD;
5. ERRADICAÇÃO: Remover a causa raiz do incidente;
6. RECUPERAÇÃO: Restaurar os sistemas e dados a partir de backup íntegro;
7. DOCUMENTAÇÃO: Registrar todo o ocorrido em Relatório de Incidente, incluindo causa, impacto, ações adotadas e lições aprendidas;
8. COMUNICAÇÃO AOS USUÁRIOS: Quando pertinente, informar os titulares dos dados afetados.

12.3 Registro de Incidentes

Todos os incidentes, independentemente do nível de criticidade, deverão ser registrados em livro de registro de incidentes (físico ou digital), contendo: data e hora, descrição do incidente, responsável pela notificação, ações adotadas, responsável pela resolução e prazo de resolução.

13. PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Em conformidade com o art. 7º do Provimento n. 213/2026 e com a Lei n. 13.709/2018 (LGPD), o Cartório de Registro de Imóveis do 1º Ofício de Alta Floresta, na qualidade de controlador e/ou operador de dados pessoais, adota as seguintes medidas:

13.1 Princípios do Tratamento de Dados



Cartório do 1º Ofício de Alta Floresta

Registro de Imóveis

Registro de Títulos e Documentos



- Finalidade: os dados pessoais são coletados exclusivamente para finalidades registras e legais específicas e legítimas;
- Necessidade: coleta limitada ao mínimo necessário para a finalidade declarada;
- Qualidade: manutenção de dados exatos, claros e atualizados;
- Segurança: adoção de medidas técnicas e administrativas para proteger os dados pessoais.

13.2 Encarregado de Proteção de Dados (DPO)

Conforme o art. 7º, § 2º, do Provimento n. 213/2026, esta serventia designa como encarregado pelo tratamento de dados pessoais:

Encarregado (DPO)	Carlos Alberto Delagnolli da Silva
E-mail de contato	dpo@1oficioaf.com.br
Telefone	66 3521-2303

13.3 Registro das Operações de Tratamento

Esta serventia manterá registro atualizado das operações de tratamento de dados pessoais realizadas, contendo: finalidade, base legal, categorias de dados, categorias de titulares, prazo de retenção e medidas de segurança adotadas.

13.4 Direitos dos Titulares

Esta serventia garantirá, nos termos da LGPD, o exercício dos seguintes direitos aos titulares de dados: confirmação de tratamento, acesso, correção, anonimização ou bloqueio, portabilidade (quando aplicável), eliminação (quando não houver obrigação legal de manutenção) e informação sobre o compartilhamento de dados.

14. INVENTÁRIO E GESTÃO DE ATIVOS TECNOLÓGICOS

Em conformidade com o art. 6º, inciso III, do Provimento n. 213/2026, que determina a transferência organizada de acervos incluindo inventário de ativos tecnológicos, esta serventia manterá o seguinte controle:

14.1 Categorias de Ativos

- Hardware: computadores, servidores, nobreaks, scanners, impressoras, switches, roteadores, câmeras;
- Software: sistemas de gestão registral, sistemas operacionais, antivírus, ferramentas de backup, navegadores;
- Dados e informações: bases registras, livros eletrônicos, documentos digitalizados, trilhas de auditoria;
- Serviços: conexão à internet, serviços em nuvem, sistemas de e-mail;
- Mídias físicas: HDs externos, pen drives, CDs/DVDs utilizados para backup.

14.2 Controles de Inventário

- O inventário de ativos tecnológicos será mantido atualizado em planilha ou sistema específico, com dados sobre: identificação, localização, responsável, data de aquisição, garantia, versão do software e data de expiração do suporte;
- Revisão anual do inventário de ativos;
- Registro de entrada e saída de equipamentos.

15. CAPACITAÇÃO E CONSCIENTIZAÇÃO

Reconhecendo que a segurança da informação é responsabilidade de todos, esta serventia promoverá:

- Treinamento de integração sobre segurança da informação para todos os novos colaboradores, antes do início das atividades;
- Reciclagem anual obrigatória em segurança da informação para todos os colaboradores;



- Comunicação periódica sobre ameaças atuais, boas práticas de segurança e atualizações desta Política;
- Simulações periódicas de incidentes para avaliar a prontidão da equipe;
- Ciência formal desta Política por todos os colaboradores, mediante assinatura de termo de conhecimento e compromisso.

Os temas mínimos dos treinamentos incluirão: engenharia social e phishing, uso seguro de senhas, proteção de dados pessoais (LGPD), procedimentos de backup, resposta a incidentes e uso adequado dos recursos tecnológicos.

16. GESTÃO DE TERCEIROS E FORNECEDORES

Em conformidade com o art. 8º do Provimento n. 213/2026, que estabelece requisitos para as soluções tecnológicas utilizadas, esta serventia adota as seguintes diretrizes para gestão de fornecedores:

- Todos os contratos com fornecedores de tecnologia deverão conter cláusulas expressas sobre: confidencialidade, segurança da informação, proteção de dados pessoais (LGPD), segregação lógica de dados, portabilidade e reversibilidade dos dados;
- Fornecedores deverão submeter-se às diretrizes de segurança desta Política durante toda a vigência contratual;
- Esta serventia avaliará, antes de qualquer contratação, a dependência estrutural em relação ao fornecedor e os riscos de lock-in tecnológico, conforme art. 8º, inciso III, do Provimento n. 213/2026;
- A serventia assegurará mecanismos de portabilidade e reversibilidade dos dados em todos os contratos de software, garantindo a extração integral do acervo em formato interoperável;
- Incidentes de segurança envolvendo fornecedores deverão ser comunicados imediatamente ao Oficial Registrador.

17. AUDITORIA, MONITORAMENTO E CONFORMIDADE

17.1 Trilhas de Auditoria – Nível Ampliado (Classe 3)

Conforme o Anexo II, item 3, do Provimento n. 213/2026, esta serventia Classe 3 deverá manter trilhas de auditoria em nível ampliado, que inclui:

- Nível essencial: registro de autenticação (login/logout), identificação do usuário, data, hora e operações principais nos sistemas registrais;
- Nível intermediário: alterações cadastrais, tentativas de acesso não autorizadas e modificações em perfis de usuário;
- Nível ampliado (obrigatório Classe 3): operações administrativas nos sistemas, acessos privilegiados, integrações com plataformas externas e eventos de segurança da informação;
- Os logs devem ser imutáveis (protegidos contra alteração) e retidos por no mínimo 5 (cinco) anos;
- Os registros de auditoria devem conter: identificação do usuário, data e hora, tipo de operação, dado acessado ou modificado, endereço IP e resultado da operação.

17.2 Monitoramento Contínuo

- Revisão mensal dos logs de acesso e auditoria pelo Oficial Registrador ou responsável designado;
- Monitoramento de tentativas de acesso não autorizadas e alertas automáticos para eventos suspeitos;
- Verificação regular da integridade dos backups.

17.3 Declaração no Sistema Justiça Aberta

Conforme exigência do Provimento n. 213/2026, esta serventia realizará as declarações e prestará as informações sobre conformidade tecnológica no Sistema Justiça Aberta do CNJ, nos prazos e formatos determinados pela Corregedoria competente.

17.4 Dossiê Técnico

Esta serventia manterá Dossiê Técnico atualizado, conforme o art. 2º, inciso VI, do Provimento n. 213/2026, contendo evidências documentais, técnicas e operacionais aptas a demonstrar o cumprimento de cada etapa e requisito desta Política, elaborado sob responsabilidade do Oficial Registrador e, quando aplicável, por profissional qualificado.



18. REVISÃO E ATUALIZAÇÃO DESTA POLÍTICA

Esta Política será revisada obrigatoriamente:

- Anualmente, de forma programada, na mesma época de sua aprovação;
- Após a ocorrência de incidente crítico de segurança;
- Após mudanças relevantes na infraestrutura tecnológica da serventia;
- Após a publicação de novas normas do CNJ, do TJMT ou da Corregedoria competente que impactem seu conteúdo;
- Após mudança na titularidade da delegação.

As revisões serão formalizadas por meio de nova versão numerada do documento, com registro das alterações realizadas, data e assinatura do Oficial Registrador.

Versão	Histórico de Revisões
5.0 – Maio/2026	Versão inicial. Elaborada em conformidade com o Provimento n. 213/2026 do CNJ.

19. DISPOSIÇÕES FINAIS E VIGÊNCIA

Esta Política entra em vigor na data de sua aprovação pelo Oficial Registrador titular desta serventia e tem vigência por prazo indeterminado, até que seja substituída por versão posterior.

O descumprimento das normas desta Política, por colaboradores, prestadores de serviço ou fornecedores, sujeitará o infrator às medidas disciplinares, contratuais e legais aplicáveis, sem prejuízo das sanções previstas na LGPD, nas normas do CNJ e na legislação registral vigente.

Esta serventia se compromete a implementar progressivamente todos os requisitos do Provimento n. 213/2026, observando o cronograma definido nos Anexos da referida norma e comunicando à Corregedoria competente o seu cumprimento por meio das declarações no Sistema Justiça Aberta.

Alta Floresta – MT, 12 de maio de 2026

Oficial Registrador

Encarregado de Dados - DPO