



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



PLANO DE CONTINUIDADE DE NEGÓCIOS
PCN + PLANO DE RECUPERAÇÃO DE DESASTRES (PRD) – DOCUMENTO INTEGRADO

Documento	Plano de Continuidade de Negócios (PCN) e Plano de Recuperação de Desastres (PRD) – Documento Integrado
Versões anteriores	1.0 2.0 3.0 4.0
Versão	5.0
Data de aprovação	Maio de 2026
Classe da Serventia	CLASSE 3 – Arrecadação bruta semestral acima de R\$ 500.000,00
RTO (Classe 3)	Máximo 8 (oito) horas
RPO (Classe 3)	Máximo 4 (quatro) horas
Responsável / Aprovador	Lorenço Boing Sobrinho
Base normativa	Provimento n. 213/2026 – CNJ ABNT NBR ISO 22301 LGPD
Classificação	CONFIDENCIAL – Uso Interno
Próxima revisão	Maio de 2027 (revisão anual) ou após incidente crítico



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



SUMÁRIO

SUMÁRIO	2
1. APRESENTAÇÃO E PROPÓSITO	3
2. IDENTIFICAÇÃO DA SERVENTIA	3
3. BASE NORMATIVA E REFERÊNCIAS	3
4. ESTRUTURA DE GOVERNANÇA E RESPONSABILIDADES	4
4.1 Papéis e Responsabilidades	4
4.2 Contatos de Emergência	4
5. ANÁLISE DE IMPACTO NO NEGÓCIO (BIA)	5
5.1 Processos Críticos e Objetivos de Recuperação	5
6. IDENTIFICAÇÃO, AVALIAÇÃO DE RISCOS E MEDIDAS DE MITIGAÇÃO	6
6.1 Metodologia	6
6.2 Matriz de Riscos – Ameaças Tecnológicas	6
7. ESTRATÉGIAS DE CONTINUIDADE OPERACIONAL (PCN)	8
7.1 Níveis de Contingência	8
7.2 Procedimento de Atendimento Manual em Contingência	8
7.2.1 Protocolo Manual de Títulos	8
7.2.2 Expedição de Certidões em Contingência	9
7.2.3 Comunicação com Usuários	9
7.3 Continuidade da Conectividade	9
7.4 Continuidade da Energia	9
7.5 Continuidade em Caso de Ausência do Oficial Registrador	9
8. INFRAESTRUTURA DE TI E BACKUP (CLASSE 3)	9
8.1 Inventário dos Ativos Críticos	9
8.2 Política de Backup – Parâmetros Obrigatórios Classe 3	10
9. PLANO DE RECUPERAÇÃO DE DESASTRES (PRD)	11
9.1 Critérios de Ativação do PRD	11
9.2 Procedimento Geral de Resposta – Fases	11
FASE 1 – DETECÇÃO E NOTIFICAÇÃO IMEDIATA (0 a 30 minutos)	11
FASE 2 – CONTENÇÃO (30 minutos a 2 horas)	11
FASE 3 – AVALIAÇÃO E COMUNICAÇÃO (2 a 4 horas)	12
FASE 4 – ERRADICAÇÃO E RECUPERAÇÃO (4 a 8 horas – RTO máximo)	12
FASE 5 – RETORNO CONTROLADO À OPERAÇÃO NORMAL	12
FASE 6 – PÓS-INCIDENTE: ANÁLISE DE CAUSA RAIZ E LIÇÕES APRENDIDAS	12
10. PROCEDIMENTOS ESPECÍFICOS POR CENÁRIO	12
10.1 Ataque de Ransomware	12
Procedimento específico:	12
10.2 Falha Total do Servidor Principal	13
10.3 Queda de Conectividade com a Internet	13
10.4 Falha de Energia	13
10.5 Desastre Físico (Incêndio / Inundação)	13
11. PROVIDÊNCIAS DE CURTO E MÉDIO PRAZO (ART. 3º, §2º, PROV. 213/2026)	13
11.1 Providências de Curto Prazo – Até 30 dias do Incidente	14
11.2 Providências de Médio Prazo – Até 90 dias do Incidente	14
12. SIMULAÇÃO DE DESASTRE E TESTES DE CONTINUIDADE	15
12.1 Testes de Restauração de Backup – Semestrais (Obrigatório Classe 3)	15
12.2 Simulação Anual de Desastre (Disaster Recovery Drill)	15
12.3 Calendário de Testes e Revisões	15
13. TREINAMENTO E CONSCIENTIZAÇÃO	16
14. REVISÃO E ATUALIZAÇÃO DO PCN/PRD	16
15. APROVAÇÃO E VIGÊNCIA	16
ANEXO I – LISTA DE VERIFICAÇÃO DO PCN/PRD (CHECKLIST DE ATIVAÇÃO)	16
ANEXO II – TERMO DE CIÊNCIA E COMPROMISSO	Erro! Indicador não definido.
ANEXO III – FORMULÁRIO DE REGISTRO DE INCIDENTE	17
ANEXO IV – FORMULÁRIO DE TESTE DE RESTAURAÇÃO DE BACKUP	18
ANEXO V – SEQUÊNCIA DE RESTAURAÇÃO (MANUAL TÉCNICO RESUMIDO)	20
V.1 Pré-Requisitos	20
V.2 Sequência de Restauração	20
V.3 Critérios de Validação antes do Retorno	20



Cartório do 1º Ofício de Alta Floresta

Registro de Imóveis

Registro de Títulos e Documentos



1. APRESENTAÇÃO E PROPÓSITO

O presente documento integra o Plano de Continuidade de Negócios (PCN) e o Plano de Recuperação de Desastres (PRD) do Cartório de Registro de Imóveis do 1º Ofício de Alta Floresta, elaborados em conformidade com o art. 3º, §§ 1º e 2º, e o Anexo IV do Provimento n. 213, de 20 de fevereiro de 2026, da Corregedoria Nacional de Justiça do Conselho Nacional de Justiça (CNJ).

O PCN responde à pergunta: como esta serventia continua prestando o serviço público registral se algo der errado? O PRD responde: como recuperamos sistemas e dados após um incidente grave? Integrados em um único instrumento, esses planos asseguram a continuidade ininterrupta do serviço público extrajudicial, a preservação permanente do acervo registral e a proteção dos dados pessoais de todos os usuários.

Esta serventia é classificada como CLASSE 3 (arrecadação bruta semestral acima de R\$ 500.000,00), o que impõe os requisitos mais elevados do Provimento n. 213/2026: RTO máximo de 8 horas, RPO máximo de 4 horas, criptografia AES-256, backups imutáveis com redundância geográfica, trilhas de auditoria em nível ampliado e testes semestrais documentados de restauração.

2. IDENTIFICAÇÃO DA SERVENTIA

Denominação	Cartório de Registro de Imóveis do 1º Ofício de Alta Floresta
Comarca / Estado	Alta Floresta / Mato Grosso
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
Oficial Registrador	Lorenço Boing Sobrinho
Classe (Prov. 213/2026)	CLASSE 3 – arrecadação bruta semestral acima de R\$ 500.000,00
RTO obrigatório	Máximo 8 horas (Anexo I, Prov. 213/2026)
RPO obrigatório	Máximo 4 horas (Anexo I, Prov. 213/2026)
Encarregado de TI	Flauberth Wesley Dias Meireles
Encarregado LGPD (DPO)	Carlos Alberto Delagnolli da Silva dpo@1oficioaf.com.br
Conectividade mínima	50 Mbps (Classe 3 – Anexo I, Prov. 213/2026)

3. BASE NORMATIVA E REFERÊNCIAS

Norma / Referência	Dispositivo Aplicável	Obrigações para Esta Serventia
Provimento n. 213/2026 – CNJ	Arts. 3º §§1-2, 6º IV, 11; Anexos I, II, IV	PCN e PRD formalizados com RTO 8h e RPO 4h; 5 etapas de implementação; simulação anual de desastre; pentest
Lei n. 13.709/2018 – LGPD	Arts. 7º, 11, 37, 48	Proteção de dados pessoais; notificação de incidentes à ANPD; registro de operações de tratamento
Lei n. 6.015/1973	Arts. 22, 23	Preservação permanente dos livros de registro; impossibilidade de eliminação do acervo registral
Lei n. 8.935/1994	Art. 46	Responsabilidade do delegatário pela continuidade e segurança do serviço
Lei Federal n. 15.352/2026	—	Comunicação de incidentes com impacto em dados pessoais à ANPD



Cartório do 1º Ofício de Alta Floresta

Registro de Imóveis

Registro de Títulos e Documentos



ABNT NBR ISO 22301	—	Referencial técnico para Sistema de Gestão de Continuidade de Negócios
ABNT NBR ISO/IEC 27001	—	Sistema de Gestão de Segurança da Informação
NIST SP 800-34	—	Guia de planejamento de continuidade para sistemas de informação
Resolução CD/ANPD n. 15/2024	—	Notificação de incidentes de segurança com dados pessoais à ANPD

4. ESTRUTURA DE GOVERNANÇA E RESPONSABILIDADES

4.1 Papéis e Responsabilidades

Papel / Função	Responsável	Atribuições no PCN/PRD
Autoridade de Continuidade (Gestor do PCN)	Lorenço Boing Sobrinho	Aprovar e revisar o PCN/PRD; declarar situação de contingência; comunicar Corregedoria e ANPD; tomar decisões estratégicas durante incidentes; assinar o Dossiê Técnico
Coordenador de TI / Resposta a Incidentes	Flauberth Wesley Dias Meireles / Mundel Tecnologia	Acionar e coordenar a resposta técnica; executar procedimentos de backup, restauração e recuperação; manter inventário de ativos; conduzir testes de restauração semestrais
Encarregado de Dados (DPO)	Carlos Alberto Delagnolli da Silva	Avaliar impacto em dados pessoais; notificar ANPD quando necessário; comunicar titulares afetados; manter ROPA atualizado
Equipe Operacional	João Pedro Rodrigues Bizi / Reginaldo Liberal / Gustavo Henrique Gasques Antunes / Carlos Alberto Delagnolli da Silva / Flauberth Wesley Dias Meireles	Registrar incidentes; adotar procedimentos manuais de contingência; preservar atendimento ao público durante contingência; comunicar anomalias ao Coordenador de TI
Suporte Técnico Externo (Fornecedor)	Mundel Tecnologia	Prestar suporte técnico especializado conforme SLA contratado; notificar a serventia sobre incidentes em seus sistemas; garantir reversibilidade dos dados
Contador / Assessoria Jurídica	C&R Assessoria Contábil	Apoiar em questões trabalhistas, fiscais e jurídicas decorrentes de incidentes

4.2 Contatos de Emergência

Entidade / Pessoa	Contato	Quando Acionar
Oficial Registrador – Lorenço Boing Sobrinho	66 3521-2303 adm@1oficioaf.com.br	Qualquer incidente – autoridade máxima
Responsável de TI – Flauberth Wesley Dias Meireles	66 3521-2303	Qualquer falha tecnológica



Cartório do 1º Ofício de Alta Floresta

Registro de Imóveis

Registro de Títulos e Documentos



Fornecedor do Sistema Registral – Online Engenharia de Sistemas	samila.falcao@onlinesistemas.net	Falha no sistema registral
Fornecedor de Backup / Nuvem – Mundel Tecnologia	contato@mundel.com.br 65 2121-6934	Falha no backup ou acesso remoto
Corregedoria do TJMT	corregedoria.dfe@tjmt.jus.br 65 3617-3116 / 3117 / 3118	Incidentes críticos – prazo máximo 72h (art. 11 Prov. 213/2026)
ANPD – Canal de Comunicação de Incidente de Segurança	https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis	Incidentes com risco a dados pessoais (Res. CD/ANPD n. 15/2024)
Operadora de Internet – Wavemax Internet	0800 567 5848	Queda de conectividade
Operadora de Internet – Amigo Internet	0800 645 4200	Ativação do link de contingência
Seguradora – Tokio Marine Seguradora	Telefone: 0800 31 86546 Número da apólice: 180000000001497668	Sinistros – incêndio, furto, danos
Bombeiros / SAMU	193 / 192	Emergências físicas
Polícia Civil / Militar	197 / 190	Furto, invasão, ameaças físicas

5. ANÁLISE DE IMPACTO NO NEGÓCIO (BIA)

A Análise de Impacto no Negócio (Business Impact Analysis – BIA) identifica os processos críticos da serventia, avalia as consequências de sua interrupção e define os objetivos de recuperação que fundamentam os parâmetros de RTO e RPO.

5.1 Processos Críticos e Objetivos de Recuperação

Processo	Criticidade	RTO Máximo	RPO Máximo	Impacto da Interrupção	Recursos Mínimos Necessários
Sistema informatizado de gestão registral	CRÍTICA	4 horas	4 horas	Paralisação total dos atos registrares; impossibilidade de prenotação, registro e expedição de certidões; prejuízo aos usuários e risco de perda de prioridade registral	Servidor funcional + backup restaurado + sistema operando
Acervo digital (livros eletrônicos, matrículas, imagens)	CRÍTICA	4 horas	4 horas	Perda irreparável de documentos públicos; comprometimento da publicidade e autenticidade registral; dano ao patrimônio documental nacional	Backup íntegro restaurado + sistema de acesso
Conectividade com a internet e sistemas CNJ (ONR, e-cartório)	ALTA	4 horas	N/A	Impossibilidade de interoperabilidade registral; falha em certidões eletrônicas e consultas nacionais	Link de contingência ativo (50 Mbps mínimo)



Cartório do 1º Ofício de Alta Floresta

Registro de Imóveis

Registro de Títulos e Documentos



Energia elétrica	ALTA	30 minutos (nobreak)	N/A	Interrupção de todos os sistemas; risco de corrupção de dados se desligamento abrupto	Nobreak (UPS) com autonomia mínima 30 min + gerador (recomendado para Classe 3)
Segurança da informação (controle de acesso, MFA)	ALTA	2 horas	N/A	Risco de acesso não autorizado a dados registrais durante contingência	Procedimento manual de controle de acesso documentado
Atendimento ao público (presencial e eletrônico)	MÉDIA	8 horas	N/A	Insatisfação dos usuários; possível atraso no prazo de prenotação (30 dias)	Equipe disponível + procedimento manual de protocolo
Sistema de e-mail e comunicação institucional	MÉDIA	8 horas	24 horas	Dificuldade de comunicação com usuários, advogados e órgãos públicos	Canal alternativo de comunicação (telefone, WhatsApp institucional)
Folha de pagamento e sistemas administrativos	BAIXA	72 horas	24 horas	Impacto administrativo sem prejuízo ao serviço registral	Acesso ao sistema contábil ou dados de backup do contador

6. IDENTIFICAÇÃO, AVALIAÇÃO DE RISCOS E MEDIDAS DE MITIGAÇÃO

Em conformidade com o art. 3º, §2º, do Provimento n. 213/2026, o PCN deve contemplar a identificação e avaliação de riscos e as medidas de mitigação correspondentes.

6.1 Metodologia

Os riscos foram avaliados pela combinação de Probabilidade (1–Alta, 2–Média, 3–Baixa) e Impacto (1–Alto, 2–Médio, 3–Baixo), resultando em quatro níveis: CRÍTICO, ALTO, MÉDIO e BAIXO. O nível de risco determina a prioridade das medidas de mitigação e a sequência de ativação do PRD.

6.2 Matriz de Riscos – Ameaças Tecnológicas

Ameaça / Cenário	Probabilidade	Impacto	Nível de Risco	Medidas de Mitigação	Responsável
Ataque de ransomware / malware com criptografia do acervo	Alta	Crítico	CRÍTICO	Backup imutável offsite (AES-256); antimalware ativo com atualização automática; segmentação de rede; MFA em todos os acessos; bloqueio de execução de scripts não autorizados	Resp. TI
Falha total do servidor principal (hardware)	Média	Crítico	CRÍTICO	Servidor reserva ou contrato de substituição em 4h; backup local restaurável; manutenção preventiva semestral documentada	Resp. TI
Corrompimento ou perda do	Baixa	Crítico	ALTO	Backup incremental com RPO 4h; verificação de integridade	Resp. TI



Cartório do 1º Ofício de Alta Floresta

Registro de Imóveis

Registro de Títulos e Documentos



banco de dados registral				do backup diário; restore testado semestralmente	
Queda prolongada de conectividade com a internet	Alta	Alto	ALTO	Link de internet de contingência (segunda operadora); roteador com failover automático; 50 Mbps mínimo para Classe 3	Resp. TI
Falha de energia elétrica	Alta	Alto	ALTO	Nobreak (UPS) com autonomia mínima 30 min para todos os equipamentos críticos; gerador (recomendado para Classe 3); laudo de aterramento (ART)	Oficial
Falha no sistema de backup (sem cópias válidas)	Baixa	Crítico	ALTO	Teste semestral obrigatório de restauração; monitoramento automático de conclusão dos backups; alertas de falha; dois ambientes independentes	Resp. TI
Acesso não autorizado aos sistemas (invasão lógica)	Média	Alto	ALTO	MFA obrigatório; firewall stateful; logs de acesso imutáveis; revisão semestral de perfis; pentest anual (Etapa 5)	Resp. TI
Exfiltração de dados pessoais (vazamento)	Baixa	Crítico	ALTO	Criptografia TLS 1.3 em trânsito e AES-256 em repouso; DLP; logs de exportação; acesso por menor privilégio	Resp. TI / DPO
Falha ou encerramento do fornecedor de sistema registral	Baixa	Crítico	ALTO	Contrato com cláusula de reversibilidade e portabilidade (arts. 13-15 Prov. 213/2026); extração periódica do acervo em formato interoperável	Oficial
Desastre físico – incêndio	Baixa	Crítico	ALTO	Backup offsite com redundância geográfica; extintores; alarme de incêndio; controle de acesso físico; seguro patrimonial	Oficial
Inundação / alagamento das instalações	Baixa	Alto	MÉDIO	Servidores em posição elevada; backup offsite; plano de evacuação do acervo físico	Oficial
Furto de equipamentos	Baixa	Alto	MÉDIO	Controle de acesso físico (travas, câmeras); disco criptografado (AES-256) em todos os equipamentos; inventário de ativos	Oficial
Erro humano crítico (exclusão ou modificação indevida de registro)	Média	Alto	ALTO	Trilha de auditoria nível ampliado imutável; segregação de funções; MFA; backup com retenção 5 anos para reversão; dupla conferência em atos de risco	Oficial



Cartório do 1º Ofício de Alta Floresta

Registro de Imóveis

Registro de Títulos e Documentos



Ausência / incapacitação do Oficial Registrador	Baixa	Alto	MÉDIO	Interino designado; documentação de procedimentos críticos; acesso às credenciais de emergência em cofre físico seguro	TJMT / Corregedoria
Pandemia ou evento de saúde com redução de pessoal	Baixa	Médio	MÉDIO	Roteiro de trabalho remoto para funções compatíveis; rodízio de equipe; procedimento de atendimento reduzido documentado	Oficial
Falha de fornecedor de nuvem / backup remoto	Baixa	Alto	MÉDIO	Dois ambientes independentes de backup (local + nuvem de fornecedores distintos); SLA contratado; verificação mensal de acesso ao backup remoto	Resp. TI

7. ESTRATÉGIAS DE CONTINUIDADE OPERACIONAL (PCN)

O PCN define como esta serventia continuará prestando o serviço público registral durante a ocorrência de incidentes, minimizando o impacto para os usuários e assegurando o cumprimento dos prazos e obrigações legais.

7.1 Níveis de Contingência

Nível	Situação	Serviços Afetados	Resposta Imediata
NÍVEL 1 – Contingência Parcial	Lentidão ou falha em sistema não crítico; interrupção de internet por menos de 2 horas; falha de um equipamento periférico	Atendimento parcialmente afetado; serviços registrares principais disponíveis	Acionar responsável de TI; ativar link de contingência de internet se necessário; registrar na trilha de incidentes; comunicar usuários se houver fila
NÍVEL 2 – Contingência Total com Atendimento Manual	Falha do sistema registral principal; queda de energia sem resolução em 30 minutos; interrupção de internet por mais de 2 horas	Sistema informatizado indisponível; atendimento somente por protocolo manual	Declarar contingência total; ativar procedimento manual (item 7.2); comunicar usuários; acionar fornecedor; notificar Oficial Registrador
NÍVEL 3 – Desastre Grave / Recuperação de Emergência	Ransomware; perda do acervo digital; sinistro físico (incêndio, inundação); comprometimento grave de dados pessoais	Todos os serviços digitais indisponíveis; possível comprometimento do acervo	Declarar Nível 3; ativar PRD (Capítulo 9); isolar sistemas; comunicar Corregedoria do TJMT em até 72 horas; acionar DPO para avaliação LGPD; não pagar resgate sem orientação jurídica

7.2 Procedimento de Atendimento Manual em Contingência

Quando o sistema informatizado estiver indisponível, esta serventia adotará os seguintes procedimentos manuais:

7.2.1 Protocolo Manual de Títulos

- Utilizar o Livro de Protocolo físico (reserva) para registro manual de apresentação de títulos;
- Registrar: número sequencial, data e hora, nome do apresentante, CPF, natureza do título e identificação do imóvel;
- A prioridade registral será assegurada pela hora de apresentação registrada no protocolo manual;
- Ao restabelecimento do sistema, os protocolos manuais serão imediatamente migrados para o sistema informatizado, preservando data e hora originais.



Cartório do 1º Ofício de Alta Floresta

Registro de Imóveis

Registro de Títulos e Documentos



7.2.2 Expedição de Certidões em Contingência

- Certidões urgentes poderão ser expedidas manualmente a partir dos livros físicos ou cópias de segurança impressas do acervo;
- O escrevente responsável deverá registrar manualmente a emissão e o destinatário para posterior lançamento no sistema;
- Certidões eletrônicas (e-cartório): suspender temporariamente durante a contingência com comunicação ao sistema CNJ.

7.2.3 Comunicação com Usuários

- Afixar aviso nas dependências da serventia informando a situação de contingência e o prazo estimado de retorno;
- Comunicar via WhatsApp institucional, e-mail e, se necessário, redes sociais;
- Orientar os usuários sobre a preservação dos prazos de prenotação (30 dias – art. 205 do CC/2002).

7.3 Continuidade da Conectividade

- **Link principal de internet: mínimo 50 Mbps (Classe 3 – Anexo I, Prov. 213/2026) – [Operadora: Wavemax Internet] | Velocidade Nominal: 800 Mbps;**
- **Link de contingência (segunda operadora ou tecnologia diferente): mínimo 50 Mbps – [Operadora: Amigo Internet] | Velocidade Nominal: 700 Mbps;**
- Roteador com failover automático configurado para alternar para o link de contingência em até 5 minutos de falha do principal;

7.4 Continuidade da Energia

- Nobreak (UPS/SAI) instalado em todos os equipamentos críticos (servidores, switches, computadores principais) com autonomia mínima de 30 minutos – laudo de aterramento elétrico com ART;
- Em caso de interrupção prolongada de energia (acima de 30 minutos): encerramento seguro e controlado dos sistemas, preservando a integridade dos dados;
- Procedimento documentado de desligamento seguro: sequência de shutdown dos sistemas antes do esgotamento do nobreak.

7.5 Continuidade em Caso de Ausência do Oficial Registrador

- Designação de interino conforme art. 20 da Lei n. 8.935/1994 e normas do TJMT;
- Manter as credenciais de acesso de emergência em cofre físico lacrado, de acesso exclusivo do Oficial Registrador e, em caso de incapacitação, do interino designado pela Corregedoria;
- Documentação completa dos procedimentos críticos acessível ao interino;
- Contato prévio com a Corregedoria do TJMT para comunicação imediata em caso de afastamento inesperado.

8. INFRAESTRUTURA DE TI E BACKUP (CLASSE 3)

8.1 Inventário dos Ativos Críticos

Os seguintes ativos de TI são considerados críticos para a continuidade dos serviços registrais e devem ser protegidos, monitorados e incluídos nas rotinas de backup e recuperação:

Ativo	Tipo	Função Crítica	Localização	Responsável
Servidor principal do sistema registral	Servidor Dell T160 Servidor Dell T140 Servidor Dell T110	Execução do sistema informatizado de gestão registral; armazenamento do banco de dados	CPD – Sala do Servidor	Resp. TI
Sistema de gestão registral	Online Engenharia de Sistemas	Práticas de atos registrais; geração de certidões; controle de protocolo	Servidores	Resp. TI / Fornecedor



Cartório do 1º Ofício de Alta Floresta

Registro de Imóveis

Registro de Títulos e Documentos



NAS / Storage local de backup	Hardware	Backup local – primeira cópia de segurança; RPO 4h	CPD / Rack do servidor	Resp. TI
Serviço de backup em nuvem	Serviço externo	Backup remoto – segunda cópia com redundância geográfica; backup imutável	Mundel Tecnologia	Resp. TI / Mundel Tecnologia
Roteador principal	Hardware	Conectividade com a internet e sistemas CNJ	CPD / Rack do servidor	Resp. TI
Roteador de contingência / failover	Hardware	Link de internet reserva com ativação automática	CPD / Rack do servidor	Resp. TI
Switch de rede	Hardware	Interconexão dos equipamentos da serventia	CPD / Rack do servidor	Resp. TI
Nobreak / UPS	Hardware	Fornecimento de energia em contingência – autonomia mínima 30 min	CPD / Rack do servidor	Resp. TI / Oficial
Computadores dos escreventes	Hardware	Acesso ao sistema registral; atendimento ao público	Salão de Atendimento / Setores	Resp. TI
Scanner de documentos	Hardware	Digitalização de títulos e documentos	Salão de Atendimento / Setores	Resp. TI
Firewall / UTM	Hardware/Software	Proteção de rede contra ataques externos; controle de tráfego	CPD Administrado por Mundel Tecnologia	Resp. TI
Sistema de videomonitoramento (CFTV)	Hardware/Software	Segurança física das dependências	CPD	Oficial / Inviolável Monitoramento

8.2 Política de Backup – Parâmetros Obrigatórios Classe 3

Backup completo	Semanal – toda semana (preferencialmente domingos, fora do expediente) – automatizado
Backup incremental	Diário – ao término do expediente OU replicação contínua para atender RPO de 4 horas
Cópia local (Ambiente 1)	NAS / Storage da serventia – cópia imutável (proteção contra ransomware)
Cópia remota (Ambiente 2)	Serviço de nuvem com redundância geográfica – backup imutável – criptografia AES-256
Criptografia dos backups	AES-256 (ou superior) – obrigatório para cópias armazenadas externamente
Imutabilidade	Obrigatória – backups não podem ser modificados ou deletados por ransomware
RPO (perda máxima tolerada)	4 horas (Classe 3 – Anexo I, Prov. 213/2026)



Cartório do 1º Ofício de Alta Floresta

Registro de Imóveis

Registro de Títulos e Documentos



RTO (tempo máximo de recuperação)	8 horas (Classe 3 – Anexo I, Prov. 213/2026)
Teste de restauração	Semestral obrigatório – documentado em formulário próprio (Anexo IV deste PCN)
Retenção – dados operacionais	Mínimo 5 anos
Retenção – livros e atos registraes	PERMANENTE – vedada a eliminação (art. 22, Lei 6.015/1973)
Chaves de criptografia	Custódia exclusiva do Oficial Registrador – armazenadas em cofre físico + gestor de senhas criptografado
Monitoramento dos backups	Alertas automáticos de falha; verificação diária de conclusão bem-sucedida

9. PLANO DE RECUPERAÇÃO DE DESASTRES (PRD)

O PRD define os procedimentos técnicos e operacionais para restauração dos sistemas, dados e operações após incidente grave que resulte em indisponibilidade ou comprometimento do acervo registral. Conforme o art. 2º, XI, do Provimento n. 213/2026, o PRD é o conjunto de medidas técnicas e operacionais voltadas à restauração de sistemas e dados após incidente grave.

9.1 Critérios de Ativação do PRD

O PRD deve ser ativado pelo Oficial Registrador (ou Coordenador de TI na sua ausência imediata) quando ocorrer qualquer uma das seguintes situações:

- Indisponibilidade do sistema registral por mais de 2 horas sem previsão de solução pelo suporte do fornecedor;
- Detecção de ataque de ransomware ou qualquer malware que comprometa a integridade dos dados;
- Perda, corrompimento ou comprometimento do banco de dados registral ou dos livros eletrônicos;
- Desastre físico (incêndio, inundação, explosão) que destrua ou inutilize os equipamentos da serventia;
- Falha total e simultânea de ambos os links de internet por mais de 4 horas;
- Comprometimento grave do controle de acesso (invasão com acesso privilegiado confirmado);
- Qualquer evento que impeça a prestação do serviço registral por prazo superior ao RTO de 8 horas.

9.2 Procedimento Geral de Resposta – Fases

FASE 1 – DETECÇÃO E NOTIFICAÇÃO IMEDIATA (0 a 30 minutos)

1. Qualquer colaborador que identificar anomalia, falha ou suspeita de incidente comunica IMEDIATAMENTE o Coordenador de TI e o Oficial Registrador por telefone/WhatsApp;
2. O Coordenador de TI confirma a existência do incidente e classifica o nível (1, 2 ou 3 – conforme item 7.1);
3. O Oficial Registrador é informado e decide sobre a ativação do PRD;
4. Abertura do Registro de Incidente (Formulário RI – Anexo III deste PCN);
5. Início da contagem do RTO (máximo 8 horas para retorno à operação normal).

FASE 2 – CONTENÇÃO (30 minutos a 2 horas)

6. ISOLAR o sistema ou equipamento afetado da rede para impedir propagação;
7. Em caso de ransomware: desconectar TODOS os computadores da rede (cabo e Wi-Fi) IMEDIATAMENTE – não tentar descriptografar ou pagar resgate sem orientação jurídica;
8. Em caso de invasão lógica: revogar TODOS os acessos ativos e bloquear credenciais comprometidas;
9. Em caso de desastre físico: acionar Bombeiros (193) e/ou SAMU (192); evacuar as dependências com segurança; não retornar antes da liberação das autoridades;
10. Preservar evidências: NÃO desligar equipamentos comprometidos (salvo risco à segurança física) – fotografar telas, preservar logs;
11. Verificar se os backups estão íntegros e disponíveis (ambiente local e remoto).



Cartório do 1º Ofício de Alta Floresta

Registro de Imóveis

Registro de Títulos e Documentos



FASE 3 – AVALIAÇÃO E COMUNICAÇÃO (2 a 4 horas)

12. Avaliar a extensão do incidente: quais sistemas, dados e usuários foram afetados;
13. Determinar se há impacto em dados pessoais de usuários ou colaboradores – acionar o DPO;
14. COMUNICAR A CORREGEDORIA DO TJMT em até 72 horas da ciência do incidente crítico (art. 11, Prov. 213/2026) – meta de excelência: 24 horas;
15. Se houver risco relevante a dados pessoais: NOTIFICAR A ANPD conforme Resolução CD/ANPD n. 15/2024 e Lei Federal n. 15.352/2026;
16. Se titulares de dados forem afetados com risco de dano: comunicar os titulares afetados (art. 48, LGPD);
17. Comunicar os usuários da serventia sobre a situação de contingência (aviso nas dependências, WhatsApp, e-mail);
18. Acionar o suporte do fornecedor do sistema registral conforme SLA contratado.

FASE 4 – ERRADICAÇÃO E RECUPERAÇÃO (4 a 8 horas – RTO máximo)

19. Erradicar a causa raiz do incidente antes de iniciar a recuperação (ex.: remover malware, fechar vulnerabilidade explorada);
20. Em caso de ransomware: reconstruir o ambiente a partir do backup imutável em ambiente limpo – NUNCA restaurar sobre o ambiente comprometido;
21. Selecionar o backup mais recente com integridade verificada (dentro do RPO de 4 horas);
22. Executar o procedimento de restauração conforme o Manual Técnico de Restauração (Anexo V deste PCN);
23. Verificar a integridade dos dados restaurados: conferir matrículas, protocolo e logs de auditoria;
24. Testar o funcionamento completo do sistema antes de reabrir para atendimento;
25. Restaurar os controles de acesso: redefinir TODAS as senhas, revogar e reconfigurar MFA;
26. Reativar gradualmente os serviços, iniciando pelos mais críticos (sistema registral, conectividade).

FASE 5 – RETORNO CONTROLADO À OPERAÇÃO NORMAL

27. Validar que todos os dados restaurados estão íntegros, completos e consistentes;
28. Confirmar que todos os controles de segurança estão ativos (firewall, antimalware, MFA, backup);
29. Confirmar que os logs de auditoria registram corretamente as operações após a restauração;
30. Migrar para o sistema restaurado os protocolos manuais realizados durante a contingência;
31. Declarar o encerramento da contingência ao Oficial Registrador e à equipe;
32. Comunicar o retorno à normalidade à Corregedoria do TJMT e, se aplicável, à ANPD;
33. Comunicar os usuários sobre o restabelecimento do serviço.

FASE 6 – PÓS-INCIDENTE: ANÁLISE DE CAUSA RAIZ E LIÇÕES APRENDIDAS

34. Elaborar o Relatório de Análise de Causa Raiz (RCA) em até 5 dias úteis após o encerramento do incidente (art. 11, §2º, Prov. 213/2026);
35. Documentar: causa raiz identificada, linha do tempo do incidente, ações adotadas, tempo de recuperação alcançado (RTO real), volume de dados perdidos (RPO real), impacto nos usuários e nos dados pessoais;
36. Identificar as lições aprendidas e as melhorias necessárias no PCN/PRD;
37. Implementar as melhorias identificadas em até 30 dias;
38. Atualizar o PCN/PRD se necessário;
39. Arquivar o Relatório no Dossiê Técnico da serventia (retenção mínima 5 anos).

10. PROCEDIMENTOS ESPECÍFICOS POR CENÁRIO

10.1 Ataque de Ransomware

O ransomware é a ameaça cibernética de maior impacto potencial para serventias extrajudiciais, podendo comprometer simultaneamente a disponibilidade e a integridade do acervo registral. O Provimento n. 213/2026 exige medidas preventivas e procedimentos documentados de resposta.

Procedimento específico:

40. IMEDIATAMENTE ao detectar mensagem de ransomware ou comportamento anômalo (arquivos inacessíveis, extensões modificadas): DESCONECTAR todos os equipamentos da rede (cabo e Wi-Fi) – incluindo o servidor;
41. NÃO reiniciar os equipamentos – preservar evidências na memória;
42. NÃO pagar o resgate – não há garantia de recuperação e pode configurar crime;
43. Comunicar o Oficial Registrador e acionar o suporte técnico especializado;



Cartório do 1º Ofício de Alta Floresta

Registro de Imóveis

Registro de Títulos e Documentos



44. Verificar se os backups imutáveis (locais e remotos) estão íntegros – acessar pelo ambiente de nuvem, NÃO pelo ambiente comprometido;
45. Comunicar a Corregedoria do TJMT em até 72 horas;
46. Avaliar com o DPO se há impacto em dados pessoais – notificar ANPD se necessário;
47. Reconstruir o ambiente a partir do backup imutável em hardware limpo ou VM isolada;
48. Restaurar os dados do backup mais recente dentro do RPO (máximo 4 horas de dados perdidos);
49. Contratar análise forense digital se houver suspeita de exfiltração de dados;
50. Registrar boletim de ocorrência policial.

10.2 Falha Total do Servidor Principal

51. Acionar imediatamente o Coordenador de TI;
52. Avaliar se é falha de hardware (HD, memória, fonte) ou de software (sistema operacional, banco de dados);
53. Acionar o suporte do fornecedor de hardware com SLA documentado;
54. Se o reparo ultrapassar 2 horas: acionar servidor reserva (se disponível) ou ambiente em nuvem de contingência;
55. Restaurar o backup mais recente no ambiente alternativo;
56. Verificar integridade do banco de dados registral antes de liberar o acesso;
57. Meta: retorno à operação em até 8 horas (RTO Classe 3).

10.3 Queda de Conectividade com a Internet

58. Verificar se o problema é interno (roteador, cabo) ou externo (operadora);
59. Acionar o failover automático para o link de contingência (segunda operadora);
60. Se o failover não ocorreu automaticamente: configurar manualmente a rota para o link alternativo;
61. Se ambos os links estiverem indisponíveis: acionar 4G/5G (chip dedicado) para operações críticas mínimas (ONR, e-cartório);
62. Contatar a operadora do link principal para abertura de chamado técnico com prioridade;
63. Ativar o procedimento manual de protocolo de títulos durante a indisponibilidade.

10.4 Falha de Energia

64. O nobreak (UPS) assume automaticamente o fornecimento – autonomia mínima 30 minutos;
65. Acionar imediatamente a concessionária de energia (ENERGISA MT ou equivalente) para informar a falta de energia;
66. Se a previsão de retorno for superior a 20 minutos: iniciar o desligamento seguro e controlado dos sistemas na seguinte sequência: (1) fechar todas as sessões ativas do sistema registral; (2) encerrar o banco de dados; (3) desligar o servidor; (4) desligar o switch e o roteador;
67. Ao retorno da energia: aguardar 5 minutos de estabilização; ligar o roteador e switch; ligar o servidor; verificar integridade do banco de dados antes de liberar o acesso aos escreventes;
68. [Se houver gerador]: acionar o gerador manualmente conforme procedimento do fabricante.

10.5 Desastre Físico (Incêndio / Inundação)

69. Prioridade absoluta: segurança das pessoas – evacuar as dependências;
70. Acionar Bombeiros (193) e/ou SAMU (192) conforme a natureza da emergência;
71. NÃO retornar às dependências antes da liberação pelas autoridades competentes;
72. Acionar o Oficial Registrador e informar o TJMT / Corregedoria;
73. Verificar remotamente (pelo celular ou computador alternativo) se os backups em nuvem estão íntegros;
74. Identificar local alternativo de funcionamento temporário (pode ser espaço cedido por outra serventia, escritório de advocacia etc.);
75. Acionar a seguradora: 0800 31 86546 - Número da apólice: 180000000001497668
76. Registrar boletim de ocorrência.

11. PROVIDÊNCIAS DE CURTO E MÉDIO PRAZO (ART. 3º, §2º, PROV. 213/2026)

Em conformidade com o art. 3º, §2º, do Provimento n. 213/2026, o PCN deve definir as providências de curto prazo (até 30 dias) e de médio prazo (até 90 dias) para tratamento de incidentes e restauração da normalidade.



Cartório do 1º Ofício de Alta Floresta

Registro de Imóveis

Registro de Títulos e Documentos



11.1 Providências de Curto Prazo – Até 30 dias do Incidente

Ação	Prazo	Responsável	Evidência
Contenção completa do incidente e erradicação da causa raiz	Imediato / 72h	Resp. TI + Oficial	Relatório técnico de contenção
Restauração dos sistemas a partir de backup íntegro	Até 8h (RTO)	Resp. TI	Log de restauração + teste de integridade
Comunicação à Corregedoria do TJMT	Até 72h da ciência	Oficial Registrador	Protocolo de comunicação
Notificação à ANPD (se houver impacto em dados pessoais)	Prazo Res. CD/ANPD n. 15/2024	DPO	Comprovante de notificação ANPD
Comunicação aos titulares de dados afetados	Conforme avaliação do DPO	DPO	Registros de comunicação
Redefinição de TODAS as senhas e reconfiguração de MFA	Até 24h após contenção	Resp. TI	Log de reconfiguração
Revisão e bloqueio de todos os acessos não autorizados	Até 24h após contenção	Resp. TI	Relatório de revisão de acessos
Comunicar o retorno à normalidade à Corregedoria e usuários	Ao encerrar a contingência	Oficial Registrador	Comunicado formal
Registro de protocolos manuais no sistema restaurado	Até 5 dias úteis após retorno	Escreventes + Resp. TI	Conferência no sistema registral
Abertura de Boletim de Ocorrência (se pertinente)	Até 48h	Oficial Registrador	BO registrado

11.2 Providências de Médio Prazo – Até 90 dias do Incidente

Ação	Prazo	Responsável	Evidência
Elaborar e arquivar o Relatório de Causa Raiz (RCA) e Lições Aprendidas	Até 5 dias úteis após encerramento	Resp. TI + Oficial	RCA arquivado no Dossiê Técnico
Implementar as melhorias identificadas no RCA (patch, configuração, treinamento)	Até 30 dias após o RCA	Resp. TI	Registro de implementação + evidências
Revisar e atualizar o PCN/PRD com base nas lições aprendidas	Até 60 dias	Oficial Registrador	Nova versão do PCN/PRD assinada
Realizar teste de restauração de backup para confirmar que o ambiente restaurado está íntegro	Até 30 dias	Resp. TI	Formulário de Teste de Restauração (Anexo IV)
Contratar análise forense digital (se houve suspeita de exfiltração ou ataque sofisticado)	Até 15 dias	Oficial Registrador	Relatório forense
Atualizar inventário de ativos tecnológicos	Até 30 dias	Resp. TI	Inventário atualizado
Revisar contratos de fornecedores de TI à luz do incidente	Até 90 dias	Oficial Registrador	Aditivos contratuais ou novos contratos



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



Treinamento de toda a equipe com base nas lições aprendidas	Até 60 dias	Oficial Registrador	Lista de presença + conteúdo do treinamento
Atualizar o ROPA (se o incidente afetou dados pessoais)	Até 30 dias	DPO	ROPA versão atualizada
Declarar as ações no Sistema Justiça Aberta (se exigido pela Corregedoria)	Conforme orientação TJMT	Oficial Registrador	Protocolo no Justiça Aberta

12. SIMULAÇÃO DE DESASTRE E TESTES DE CONTINUIDADE

12.1 Testes de Restauração de Backup – Semestrais (Obrigatório Classe 3)

Conforme o Anexo II do Provimento n. 213/2026, esta serventia realizará testes documentados de restauração de backup com periodicidade SEMESTRAL, utilizando o Formulário de Registro de Teste (Anexo IV deste PCN).

- Calendário: primeiro semestre – [mês definido]; segundo semestre – [mês definido];
- Ambiente de teste: preferencialmente em ambiente isolado (VM ou máquina alternativa), sem impacto na produção;
- Verificar: integridade dos dados restaurados, funcionalidade do sistema, RTO e RPO alcançados;
- Documentar: data, ambiente, resultado, tempo de restauração, volume de dados, assinatura do responsável.

12.2 Simulação Anual de Desastre (Disaster Recovery Drill)

Conforme a Etapa 5 do Anexo IV do Provimento n. 213/2026, esta serventia Classe 3 realizará simulação anual completa de desastre:

- Escopo: simular um cenário de desastre real (ex.: ransomware, falha de servidor, queda de energia prolongada) e executar o PRD completo do início ao fim;
- Participantes: Oficial Registrador, Coordenador de TI, todos os escreventes, DPO;
- Medir: tempo efetivo de detecção, tempo de contenção, tempo de restauração (RTO real), volume de dados perdidos (RPO real);
- Documentar: roteiro do exercício, resultados medidos, desvios em relação às metas (RTO 8h / RPO 4h), ações corretivas;
- Arquivar: relatório da simulação no Dossiê Técnico com retenção mínima de 5 anos.

12.3 Calendário de Testes e Revisões

Atividade	Periodicidade	Próxima Data	Responsável
Teste de restauração de backup	Semestral (obrigatório Classe 3)	05/2026	Resp. TI
Simulação anual de desastre (DR Drill)	Anual (Etapa 5 Prov. 213/2026)	05/2027	Oficial + Resp. TI
Revisão desta Política (PCN/PRD)	Anual ou após incidente crítico	05/2027	Oficial Registrador
Revisão do inventário de ativos	Anual	Maio	Resp. TI
Pentest (teste de intrusão)	Anual (Etapa 5 Prov. 213/2026)	05/2027	Resp. TI + Especialista
Verificação de integridade dos backups	Diária (automática)	Diariamente	Sistema automático / Resp. TI
Treinamento de colaboradores em segurança da informação	Anual	Outubro	Oficial Registrador
Revisão de perfis e acessos	Semestral	Janeiro/Julho	Resp. TI + Oficial



Cartório do 1º Ofício de Alta Floresta

Registro de Imóveis

Registro de Títulos e Documentos



Simulação de extração do acervo
(portabilidade)

Anual (Etapa 5)

05/2027

Resp. TI +
Fornecedor

13. TREINAMENTO E CONSCIENTIZAÇÃO

- Todos os colaboradores desta serventia receberão treinamento sobre este PCN/PRD antes de iniciar suas atividades e anualmente de forma recorrente;
- O treinamento abrangerá, no mínimo: como identificar um incidente; quem notificar e como; procedimentos manuais de contingência; proteção contra phishing e engenharia social; uso seguro de senhas e MFA;
- Exercícios práticos (tabletop exercises) serão realizados semestralmente para verificar o conhecimento da equipe sobre os procedimentos de resposta;
- Todo colaborador assina o Termo de Ciência e Compromisso (Anexo II deste PCN) confirmando que conhece e se compromete a cumprir este plano;
- Novos colaboradores recebem treinamento de integração sobre o PCN/PRD antes de receber qualquer credencial de acesso.

14. REVISÃO E ATUALIZAÇÃO DO PCN/PRD

Este PCN/PRD será obrigatoriamente revisado:

- Anualmente – em abril de cada ano, coincidindo com o aniversário desta versão;
- Após a ocorrência de qualquer incidente Nível 2 ou Nível 3, incorporando as lições aprendidas;
- Após mudanças relevantes na infraestrutura tecnológica, nos sistemas ou nos fornecedores;
- Após a publicação de novas normas do CNJ, TJMT ou Corregedoria competente que impactem seu conteúdo;
- Após mudança na titularidade da delegação.

Versão	Data	Responsável	Alterações
5.0	Maio/2026	Lorenço Boing Sobrinho	Versão inicial. Elaborada em conformidade com o Provimento n. 213/2026 (Classe 3), LGPD e ABNT NBR ISO 22301.

15. APROVAÇÃO E VIGÊNCIA

Este Plano de Continuidade de Negócios e Plano de Recuperação de Desastres (PCN/PRD) entra em vigor na data de sua aprovação pelo Oficial Registrador titular desta serventia e tem vigência por prazo indeterminado, até que seja substituído por versão posterior.

O Oficial Registrador é pessoalmente responsável pela governança local, pela implementação deste Plano e pela adoção de todas as medidas nele previstas, conforme o art. 3º, parágrafo único, do Provimento n. 213/2026.

Alta Floresta – MT, 01 de junho de 2026.

Lorenço Boing Sobrinho
Controlador

Carlos Alberto Delagnolli da Silva
Encarregado de Dados (DPO)

ANEXO I – LISTA DE VERIFICAÇÃO DO PCN/PRD (CHECKLIST DE ATIVAÇÃO)

Utilize esta lista na ativação do PCN/PRD para garantir que nenhuma etapa crítica seja omitida.

#	Ação	Responsável	Prazo	Status
1	Identificar e classificar o incidente (Nível 1, 2 ou 3)	Qualquer colaborador / Resp. TI	Imediato	
2	Notificar o Oficial Registrador	Qualquer colaborador	Imediato	



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



3	Abrir o Registro de Incidente (Formulário RI – Anexo III)	Resp. TI	30 min	
4	ISOLAR o sistema afetado da rede	Resp. TI	30 min	
5	Verificar integridade dos backups (local e remoto)	Resp. TI	30 min	
6	Ativar o procedimento manual de protocolo (se necessário)	Escreventes	30 min	
7	Comunicar os usuários sobre a situação de contingência	Oficial / Escreventes	1h	
8	Acionar suporte do fornecedor do sistema registral	Resp. TI	1h	
9	Acionar suporte do fornecedor de backup / nuvem (se necessário)	Resp. TI	1h	
10	Acionar link de contingência de internet (se necessário)	Resp. TI	1h	
11	Comunicar a Corregedoria do TJMT (incidentes Nível 2 e 3)	Oficial Registrador	Até 72h	
12	Acionar o DPO – avaliar impacto em dados pessoais	Oficial / DPO	2h	
13	Notificar a ANPD (se houver risco a dados pessoais)	DPO	Prazo ANPD	
14	Erradicar a causa raiz do incidente	Resp. TI	Antes da restauração	
15	Executar a restauração a partir do backup íntegro	Resp. TI	RTO 8h	
16	Verificar integridade dos dados restaurados	Resp. TI	Após restauração	
17	Redefinir TODAS as senhas e reconfigurar MFA	Resp. TI	Após restauração	
18	Testar o sistema completo antes de liberar o acesso	Resp. TI	Após restauração	
19	Declarar o encerramento da contingência	Oficial Registrador	Após retorno	
20	Comunicar o retorno à normalidade à Corregedoria e usuários	Oficial Registrador	Após retorno	
21	Migrar protocolos manuais para o sistema (se aplicável)	Escreventes + Resp. TI	Até 5 dias úteis	
22	Elaborar o RCA e Lições Aprendidas	Resp. TI + Oficial	Até 5 dias úteis	

ANEXO II – FORMULÁRIO DE REGISTRO DE INCIDENTE

Número do incidente	RI-_____/_____/_____
Data e hora da detecção	____/____/____ às ____:____
Data e hora do início do incidente (estimado)	____/____/____ às ____:____
Detectado por	_____



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



Notificado ao Oficial Registrador em	___/___/___ às ___:___
Nível de contingência ativado	() Nível 1 – Parcial () Nível 2 – Total () Nível 3
Sistemas / dados afetados	
Descrição detalhada do incidente	
Causa raiz identificada	
Houve impacto em dados pessoais?	() Sim – descrever: () Não () Em investigação
Titulares afetados (número estimado)	
PRD ativado?	() Sim – hora de ativação: ___ () Não
Backup utilizado na restauração – data	___/___/___
RTO alcançado (tempo de recuperação efetivo)	___ horas e ___ minutos
RPO alcançado (janela de dados perdidos)	___ horas
Metas de RTO/RPO foram atingidas?	() Sim () Não – justificar:
Corregedoria TJMT comunicada?	() Sim – data/hora: ___ () Não aplicável
ANPD notificada?	() Sim – data/hora: ___ () Não aplicável
Titulares comunicados?	() Sim () Não () Não aplicável
Ações de contenção adotadas	
Ações de erradicação adotadas	
Ações de recuperação adotadas	
Data e hora do encerramento da contingência	___/___/___ às ___:___
Impacto estimado nos usuários	
Lições aprendidas	
Melhorias a implementar	
Responsável pela resposta	
Assinatura do Oficial Registrador	
RCA elaborado?	() Sim – data: ___/___/___ () Pendente

ANEXO III – FORMULÁRIO DE TESTE DE RESTAURAÇÃO DE BACKUP

Periodicidade obrigatória para Classe 3: SEMESTRAL (Anexo II, Prov. 213/2026). Recomenda-se periodicidade trimestral.

Número do teste	BKP-TEST-___/___
Data do teste	___/___/___
Responsável pelo teste	
Aprovador (Oficial Registrador)	



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



Sistema / ambiente testado	
Data do backup restaurado	___/___/___ – horário: ___:___:___
Tipo de backup restaurado	☐ Completo ☐ Incremental ☐ Point-in-time recovery
Ambiente de restauração	☐ Ambiente de produção ☐ VM / ambiente de teste isolado
Criptografia verificada?	☐ Sim – padrão: AES-256 ☐ Não verificado
Imutabilidade do backup confirmada?	☐ Sim ☐ Não ☐ Não aplicável
Tempo de restauração medido (RTO real alcançado)	___ horas e ___ minutos
RPO verificado (janela de perda de dados)	___ horas e ___ minutos
Meta RTO (8h) atingida?	☐ Sim ☐ Não – detalhar: _____
Meta RPO (4h) atingida?	☐ Sim ☐ Não – detalhar: _____
Integridade dos dados verificada?	☐ Sim – todos os dados íntegros ☐ Parcial – detalhar: ☐ Não
Funcionalidade do sistema testada após restauração?	☐ Sim – sistema funcional ☐ Parcial ☐ Não
Resultado do teste	☐ APROVADO ☐ REPROVADO ☐ APROVADO COM RESSALVAS
Falhas ou anomalias encontradas	
Ações corretivas adotadas (se reprovado ou com ressalvas)	
Prazo para correção (se aplicável)	___/___/___
Arquivo de log do teste (referência para o Dossiê Técnico)	
Assinatura do Coordenador de TI	
Assinatura do Oficial Registrador	



Cartório do 1º Ofício de Alta Floresta

Registro de Imóveis

Registro de Títulos e Documentos



ANEXO IV – SEQUÊNCIA DE RESTAURAÇÃO (MANUAL TÉCNICO RESUMIDO)

Este anexo destina-se ao Coordenador de TI e descreve a sequência técnica de restauração dos sistemas após ativação do PRD. Deve ser revisado e adaptado conforme o sistema registral específico desta serventia.

IV.1 Pré-Requisitos

- Ambiente limpo disponível (hardware reserva, VM ou ambiente em nuvem isolado);
- Acesso às credenciais de backup (armazenadas no cofre físico do Oficial Registrador);
- Acesso confirmado ao backup remoto (nuvem) – verificar via celular antes de iniciar;
- Confirmação de que a causa raiz foi erradicada antes de iniciar a restauração.

IV.2 Sequência de Restauração

1. Acessar o ambiente de backup remoto (nuvem) – NÃO usar o ambiente comprometido;
2. Identificar o backup mais recente dentro do RPO de 4 horas e verificar hash de integridade;
3. Instalar o sistema operacional limpo no ambiente de recuperação;
4. Instalar o sistema de gestão registral na versão correta (confirmar versão com o fornecedor);
5. Restaurar o banco de dados a partir do backup selecionado;
6. Verificar a integridade do banco de dados restaurado (checksums, registros recentes, consistência);
7. Restaurar os arquivos de imagem (documentos digitalizados) a partir do backup;
8. Verificar a consistência entre o banco de dados e os arquivos de imagem;
9. Reconfigurar as integrações com sistemas externos (ONR, e-cartório, Receita Federal);
10. Reconfigurar os controles de acesso: criar novas credenciais para todos os usuários, habilitar MFA;
11. Reconfigurar o firewall e os controles de segurança de rede;
12. Reativar as rotinas de backup (local e remoto) e verificar a primeira execução;
13. Realizar testes funcionais completos com o Oficial Registrador antes de liberar o acesso à equipe;
14. Liberar o acesso gradualmente: primeiro o Oficial Registrador, depois os escreventes autorizados;
15. Documentar o RTO efetivo alcançado no Registro de Incidente (Anexo III).

IV.3 Critérios de Validação antes do Retorno

- Banco de dados íntegro e consistente – verificar os últimos registros praticados antes do incidente;
- Sistema registral abrindo e autenticando normalmente para todos os perfis;
- Trilhas de auditoria registrando corretamente as operações após a restauração;
- Backup local e remoto configurados e executando corretamente;
- Firewall e antimalware ativos e atualizados;
- MFA habilitado para todos os usuários;
- Integrações com ONR e sistemas CNJ funcionando;
- Nenhum processo ou arquivo suspeito em execução no sistema restaurado.