GUIA PRÁTICO

Entenda o Provimento CNJ Nº 213/2026

Padrões mínimos de tecnologia da informação e comunicação para os serviços registrais.

PARTE 1

IRTDPJ BRASIL
Instituto de Registro de Títulos e Documentos e de Pessoas Jurídicas do Brasil

ON RTDPJ
Operador Nacional do Registro de Títulos e Documentos e Civil das Pessoas Jurídicas

Expediente Institucional

Operador Nacional de Registro de Títulos e Documentos e de Pessoas Jurídicas (ONRTDPJ)
Presidente: Rainey Barbosa Alves Marinho
Vice-Presidente: Sônia Maria Andrade dos Santos

Instituto de Registro de Títulos e Documentos e de Pessoas Jurídicas do Brasil (IRTDPJBRASIL)
Presidente: Rainey Barbosa Alves Marinho
1º Vice-Presidente: Thyago Ribeiro Soares
2ª Vice-Presidente: Sônia Maria Andrade dos Santos

Apoio técnico:
Consultoria Jurídica do IRTDPJBrasil e do ONRTDPJ; Departamentos de Tecnologia da Informação e Suporte ao Cliente da Central RTDPJ; Departamento de Comunicação e Marketing.

Elaboração: Dixmer Vallini Netto
Revisão técnica: Rodrigo Pinho, Gabriel Hodon e Luiz Carlos Menezes
Editoração: Priscilla Vasconcelos e Catharina Oliveira
Coordenação editorial: Andréa Vieira

Título: Guia prático: Entenda o Provimento CNJ Nº 213/2026

Instituições responsáveis: ONRTDPJ e IRTDPJBRASIL

———————————————————————————————————————

Guia prático: Entenda o Provimento CNJ Nº 213/2026
Março de 2026

Esta publicação é resultado de um trabalho conjunto dos Departamentos Jurídico, Comunicação e Marketing e de Tecnologia da Informação do ONRTDPJ e do IRTDPJBrasil.

Este guia resume as medidas que os cartórios devem observar para implementar os requisitos mínimos do Provimento nº 213/2026.

Fale conosco: comunicacao@irtdpjbrasil.org.br / comunicacao@onrtdpj.org.br

Apresentação

O Provimento nº 213, publicado pelo Conselho Nacional de Justiça (CNJ) em 20 de fevereiro de 2026, estabelece novos parâmetros de infraestrutura tecnológica e define padrões mínimos de tecnologia da informação e comunicação para o funcionamento dos serviços notariais e de registro. O texto atualiza regras anteriormente vigentes, substituindo o Provimento nº 74/2018, e introduz diretrizes voltadas à segurança dos sistemas, ao armazenamento eletrônico de documentos e à proteção das informações registradas.

A regulamentação detalha requisitos relacionados à segurança da informação, como controle de acesso aos sistemas, rastreabilidade das operações realizadas, monitoramento contínuo das atividades e adoção de políticas institucionais para prevenção e tratamento de incidentes. Também são estabelecidas medidas para garantir a integridade e autenticidade dos dados, assegurando a proteção contra perdas, alterações indevidas ou acessos não autorizados. A norma prevê, ainda, ações voltadas à preservação dos acervos digitais e à manutenção da disponibilidade dos serviços, considerando o crescimento do volume de registros realizados em ambiente eletrônico.

Trata-se da norma mais ambiciosa que a Corregedoria Nacional de Justiça já editou em matéria de tecnologia para o serviço extrajudicial. A revogação integral do Provimento nº 74/2018 e a construção de um arcabouço de 26 artigos e quatro anexos demonstram que o regulador entendeu o tamanho do desafio e o enfrentou com seriedade. Não é uma atualização pontual, é uma refundação do marco de segurança digital dos cartórios brasileiros.

Diante da importância e complexidade do Provimento nº 213/2026, o Operador Nacional de Registro de Títulos de Documentos e Civil de Pessoas Jurídicas (ONRTDPJ) e o Instituto de Registro de Títulos de Documentos e de Pessoas Jurídicas do Brasil (IRTDPJBrasil) publicam, conjuntamente, este guia com o objetivo de auxiliar os oficiais registradores na compreensão e implementação das novas diretrizes tecnológicas.

A primeira parte deste guia salienta os pontos mais importantes e as medidas de maior impacto para as serventias extrajudiciais. Para facilitar a compreensão, foi elaborado um glossário de termos técnicos, siglas e documentos necessários para o cumprimento das novas regras.

Por fim, lembramos que a leitura integral do provimento é recomendável e fundamental, pois este guia traz apenas os principais pontos do normativo do CNJ.

Sumário - parte I

Sumário - parte II

1. Visão geral e contexto

O Provimento CNJ nº 213/2026, assinado pelo Ministro Corregedor Nacional de Justiça Mauro Campbell Marques, em 20 de fevereiro de 2026, estabelece os padrões mínimos obrigatórios de Tecnologia da Informação e Comunicação (TIC) para todos os serviços notariais e de registro do Brasil.

O novo mormativo revoga o Provimento nº 74/2018 e eleva significativamente o nível de exigência em segurança digital, continuidade operacional e proteção de dados para as mais de 11.500 serventias extrajudiciais do país.

O que muda de forma mais relevante

O Provimento nº 213/2026 não é uma simples atualização do Provimento nº 74/2018. Trata-se de uma refundação completa do modelo de governança de TIC, com obrigações muito mais detalhadas, prazos graduados por classe econômica da serventia, sistema de comprovação formal (dossiê técnico), parâmetros objetivos de RTO (arquitetura do sistema e estratégia de recuperação de dados) e RPO (frequência de backup), e responsabilidade pessoal e intransferível do delegatário.

2. Classificação das serventias.

O enquadramento é baseado na arrecadação bruta semestral e determina todas as obrigações, prazos e exigências de comprovação aplicáveis. Os limites serão atualizados anualmente pelo IPCA.

Classe	Receita semestral	Subclasses	Perfil típico RTD/RCPJ
Classe1	Até R$ 100.000,00	A / B / C	Pequenas serventias, cidades do interior
Classe 2	De R$ 100 mil a R$ 500.000,00	D / E / F	Serventias médias, cidades médias
Classe 3	Acima de R$ 500.000,00	G / H / I / J	Grandes serventias, capitais

O reenquadramento deve ser reavaliado anualmente. Uma variação de até 10% do limite superior não produz efeito imediato, exigindo confirmação por dois ciclos consecutivos.

Conforme dados do Justiça Aberta, do Conselho Nacional de Justiça (CNJ), praticamente 80% das serventias se enquadram, nas classes 2 e 3, sendo 44,8% das serventias brasileiras na classe 3.

Cartórios		Até R$ 100.000	Entre R$ 100.001 e R$ 500.000	Acima de R$ 500.000
Provido	8.257	1.139	2.742	4.376
Percentual	100%	13,8%	33,2%	53,0%
Vagos	3.255	1.235	1.233	787
Percentual	100%	37,9%	37,9%	24,2%
Total	11.512	2.374	3.975	5.163
Percentual	100%	20,6%	34,5%	44,8%

3. Os cinco grupos técnicos do provimento

O provimento organiza suas exigências em cinco grandes blocos temáticos, todos com parâmetros distintos por classe:

INFRAESTRUTURA FÍSICA E ENERGÉTICA (Anexo I)

Fornecimento de energia estável com SAI/UPS:

- Autonomia mínima de 30 minutos para desligamento seguro (safe shutdown)
- Aterramento técnico com laudo atualizado de profissional habilitado (ART)

Internet: conectividade mínima:

- Classe 1: 2 Mbps — Classe 2: 10 Mbps — Classe 3: 50 Mbps (valores referenciais)
- O critério funcional é a capacidade de realizar backup incremental dentro do RPO da classe

Infraestrutura física: espaço isolado para equipamentos críticos, controle de acesso, proteção contra incêndio e inundações

Suporte técnico contínuo: próprio ou contratado

SEGURANÇA DA INFORMAÇÃO E CONTROLES TÉCNICOS (Anexo II)

Autenticação MFA (multifator): obrigatório para todos os acessos administrativos; vedação absoluta de credenciais compartilhadas.

Proteção - criptografia:

- Dados em trânsito: TLS 1.2 ou superior
- Dados em repouso: AES-256 ou equivalente superior
- Backups externos devem estar criptografados com chave sob custódia exclusiva da serventia.

Firewall stateful com IPS/IDS e segmentação lógica de rede

Gestão de vulnerabilidades: vulnerabilidades críticas tratadas em até 30 dias; exploração ativa exige resposta em até 72 horas

Incidentes críticos: comunicação à Corregedoria competente em até 72 horas

Parâmetros RPO e RTO por classe

Parâmetro	Classe 1	Classe 2	Classe 3
RPO (perda máxima de dados)	24 horas	12 horas	4 horas
RTO (tempo máximo de recuperação)	24 horas	24 horas	8 horas
Backup completo (intervalo máximo)	72 horas	48 horas	24 horas
Teste de restauração	Anual	Anual	Semestral
Pentest*	N/A	N/A	A cada 2 anos

* Pentest ou teste de intrusão é uma prática essencial em segurança da informação. Consiste em simular ataques cibernéticos autorizados contra sistemas, redes ou aplicações para identificar vulnerabilidades.

PROTEÇÃO DO ACERVO DIGITAL E BACKUP (Art. 12 e Etapa 3)

- Backups automatizados e monitorados, com alerta imediato em caso de falha;
- Armazenamento em pelo menos dois ambientes tecnicamente independentes (off-site ou nuvem com redundância geográfica);
- Trilhas de auditoria imutáveis com retenção mínima de cinco anos;
- Mecanismos de integridade verificada dos atos: hash, versionamento bloqueado, WORM ou equivalente;
- SGBD com integridade transacional (logs ativos).

GOVERNANÇA, LGPD E POLÍTICA DE SEGURANÇA (Arts. 3° ao 7° e Anexo III)

- Política Interna de Segurança da Informação formalizada (conteúdo mínimo no Anexo III);
- Plano de Continuidade de Negócios (PCN) e Plano de Recuperação de Desastres (PRD) documentados;
- Encarregado de Dados (DPO) designado quando exigível pela LGPD (Lei 13.709/2018);
- Registro de operações de tratamento de dados pessoais;
- Contratos com fornecedores devem conter cláusulas de: confidencialidade, reversibilidade, portabilidade, gestão de incidentes e conformidade com a LGPD.

INTEROPERABILIDADE E GOVERNANÇA EVOLUTIVA (Art. 19 e Etapa 5)

- Sistemas devem ser aptos a integrar plataformas eletrônicas de fiscalização do CNJ;
- Adoção preferencial de padrões abertos: PDF/A e XML;
- Plano formal de reversibilidade e portabilidade de dados;
- Simulação documentada de extração integral do acervo em formato interoperável;
- Capacitação periódica com registro formal das ações realizadas.

4. Cronograma de implementação (etapas do anexo IV)

O provimento define cinco etapas sequenciais e cumulativas. Os prazos abaixo são contados a partir da data de entrada em vigor.

Etapa	Escopo Principal	Classe 1	Classe 2	Classe 3
ETAPA 1 Governança e Conformidade	Política de SI, MFA, DPO, inventário de ativos, contratos revisados	Até 210 dias	Até 150 dias	Até 90 dias
ETAPA 2 Infraestrutura e Continuidade	SAI/UPS, ambiente físico, PCN, PRD, RTO, RPO definidos	Até 210 dias	Até 150 dias horas	Até 90 dias
ETAPA 3 Proteção do Acervo	Criptografia, backup off-site, firewall IPS/IDS, trilhas imutáveis	Até 36 meses	Até 30 meses	Até 24 meses
ETAPA 4 Monitoramento e Auditoria	Gestão de vulnerabilidades, pentest (Cl. 3), simulações de desastre	Até 36 meses	Até 30 meses	Até 24 meses
ETAPA 5 Interoperabilidade e Gestão Evolutiva	Integração com plataformas CNJ, portabilidade, capacitação contínua	Até 36 meses	Até 30 meses	Até 24 meses

Prorrogação excepcional (Art. 21)

As Corregedorias dos Tribunais de Justiça podem prorrogar os prazos das Etapas 1 e 2 por até 90 dias adicionais, uma única vez, mediante decisão fundamentada, plano de adequação com cronograma e medidas compensatórias imediatas. Para a Classe 1, a análise é simplificada. Para as Classes 2 e 3, exige-se requerimento formal com orçamentos e justificativas técnicas.

5. Documentos obrigatórios por classe

Esta é a relação de todos os documentos e registros que a serventia deve ter disponíveis e manter arquivados pelo prazo mínimo de cinco anos, organizada por nível de exigência.

DOCUMENTOS OBRIGATÓRIOS PARA TODAS AS CLASSES (1, 2 e 3)

Governança e políticas

- Política Interna de Segurança da Informação (conforme conteúdo mínimo do Anexo III);
- Plano de Continuidade de Negócios – PCN (com RTO, RPO, gestão de riscos e prazos de 30 e 90 dias);
- Plano de Recuperação de Desastres – PRD (integrado ou documento separado do PCN);
- Designação formal do responsável técnico interno pela implementação;
- Designação do responsável como controlador de dados pessoais (LGPD);
- Designação de encarregado/DPO, quando exigível.

Inventário e ativos

- Inventário completo de ativos tecnológicos (hardware, software, licenças, certificados, contratos, integrações, banco de dados, histórico de atualizações);
- Documento técnico de arquitetura tecnológica (topologia de rede, ambientes utilizados, fluxos de dados, localização de backups, integrações externas, mecanismos de redundância).

Contratos e conformidade legal

- Contratos revisados com fornecedores de TI contendo cláusulas expressas de: confidencialidade, reversibilidade, portabilidade, disponibilização de documentação técnica, cooperação em transição, gestão de incidentes e conformidade com a LGPD;
- Registro das operações de tratamento de dados pessoais;
- Comprovantes de licenciamento regular de softwares.

Segurança e backup

- Política de backup documentada (automatizada, monitorada, com alertas de falha);
- Registros de execução e monitoramento de rotinas de backup;

- Atas/registros de testes de restauração de backup (conforme modelo do Anexo V);
- Laudo de aterramento elétrico atualizado, assinado por profissional habilitado (ART);
- Plano de contingência energética;
- Registros de trilhas de auditoria pelo prazo mínimo de cinco anos.

Conformidade e declarações

- Declarações de conclusão de cada etapa (1 a 5), assinadas pelo titular da delegação, registradas no sistema Justiça Aberta;
- Declaração anual de conformidade (renovada anualmente no sistema Justiça Aberta com síntese do dossiê);
- Registros de capacitação periódica de colaboradores em segurança e backups.

DOCUMENTOS ADICIONAIS / FORMATO SIMPLIFICADO PARA A CLASSE 1

Para a Classe 1, o dossiê técnico ampliado é dispensado.
A comprovação é feita por:

- Relatório simplificado de implementação assinado pelo titular. Deve conter: identificação da serventia e classe, descrição do requisito e solução adotada, demonstração de equivalência funcional, indicação das evidências disponíveis e declaração formal de responsabilidade;
- Contratos de serviços de TI e notas fiscais correspondentes;
- Registro simplificado de teste de restauração (data, sistemas restaurados, confirmação de integralidade, tempo de recuperação, assinatura do responsável).

DOCUMENTOS ADICIONAIS OBRIGATÓRIOS PARA AS CLASSES 2 e 3

- Dossiê técnico completo por etapa (atas, relatórios, registros de configuração, contratos revisados, registros de capacitação e evidências técnicas);
- Mecanismo idôneo de verificação de integridade do dossiê: lista de hashes dos arquivos, assinada digitalmente pelo responsável;
- Repositório com controle de acesso e registro auditável de alterações (ou armazenamento com imutabilidade/retention lock);
- Ata completa de teste de restauração (conforme modelo do Anexo V, com todos os campos preenchidos: RTO/RPO aferidos, método de verificação de integridade, evidências técnicas, hash do backup restaurado);
- Política formal de gestão de chaves criptográficas (inventário, segregação de custódia e rotação, registro de operações);
- Registro formal de todas as vulnerabilidades identificadas e tratadas (data de identificação, classificação de risco, providências e data de encerramento);
- Relatório de conformidade de auditoria das trilhas (imutabilidade, sincronização de tempo, identificação de usuário, retenção);
- Registros das simulações anuais de desastre para validação do PCN/PRD.

DOCUMENTOS ADICIONAIS OBRIGATÓRIOS PARA CLASSE 3

- Relatório de Pentest (teste de intrusão) a cada dois anos, ou relatório coletivo do ambiente compartilhado, com: escopo, metodologia, resultados, plano de correção e declaração de aderência assinada pelo responsável técnico;
    - Serventias 100% em ambiente SaaS podem substituir por: relatório técnico da empresa desenvolvedora + declaração do titular sobre instalações locais.

- Plano estruturado de evolução de maturidade em segurança (horizonte de até 24 meses), com cronograma formal;

Avaliação técnica de segurança (no prazo máximo de 12 meses da etapa).

DOCUMENTOS DE PORTABILIDADE E REVERSIBILIDADE (Etapa 5: todas as classes)

- Plano formal de reversibilidade e portabilidade de dados;
- Registro/ata de simulação documentada de extração integral do acervo digital em formato interoperável e não proprietário:
    - Classe 3: a cada 24 meses — Classe 2: a cada 30 meses — Classe 1: a cada 36 meses;
    - Imediatamente após mudança relevante de fornecedor ou arquitetura tecnológica.

6. Responsabilidades pessoais do delegatário

Cada delegatário permanece pessoal e indevidamente responsável por:

- Governança local e controle de acessos internos à serventia;
- Gestão de incidentes no âmbito da serventia;
- Integração do PCN/PRD com a solução centralizada;
- Observância da LGPD no tratamento local de dados pessoais;
- Assinatura das declarações de conclusão de etapa no sistema Justiça Aberta;
- Veracidade das informações declaradas (declaração falsa sujeita o delegatário a penalidades).

6.1 Responsabilidade pessoal e intransferível do delegatário

Mesmo que toda a infraestrutura e serviços sejam executadas por colaboradores, prepostos, terceiros ou fornecedores contratados, a responsabilidade jurídica pelo cumprimento do provimento é pessoal e intransferível do delegatário, interino ou interventor (art. 13, § 3º e art. 14).

7. Pontos de atenção e análise crítica

Software End of Life (EOL) | Risco imediato

O art. 4º, § 3º proíbe o uso de qualquer componente tecnológico com suporte oficial encerrado pelo fabricante (End of Life). Sistemas operacionais, bancos de dados e aplicações críticas em EOL são uma fonte comum de vulnerabilidades graves. Exemplos de risco: Windows Server 2012 (EOL desde 2023), SQL Server 2014 (EOL desde 2019), entre outros.

Custódia de chaves criptográficas | Ponto sensível

O provimento exige que, em ambientes de nuvem com MFA de backup, a chave de descriptografia permaneça sob custódia exclusiva da serventia, e não do provedor de armazenamento. Isso significa que soluções em que o próprio provedor gerencia as chaves (server-side encryption sem controle do cliente) não atendem plenamente ao requisito.

Sistema Justiça Aberta | Obrigação de declaração

Todas as serventias deverão declarar o cumprimento de cada etapa no sistema Justiça Aberta (art. 17). A declaração falsa sujeita o responsável a penalidades. Importante ver o Provimento 218/2026, que dispõe especificamente sobre as novas regras do sistema do Conselho Nacional de Justiça.

Fiscalização orientada a risco

O art. 25 estabelece que a fiscalização será orientada por risco, priorizando serventias com maior probabilidade ou impacto de não conformidade. Serventias de maior porte (Classe 3), com alto volume de atos, interconexão tecnológica ou infra compartilhada serão priorizadas.

GLOSSÁRIO E GUIA DE DOCUMENTOS

Provimento CNJ Nº 213/2026

Termos técnicos, siglas e documentos explicados de forma simples.

PARTE 2

IRTDPJ BRASIL
Instituto de Registro de Títulos e Documentos e de Pessoas Jurídicas do Brasil

ON RTDPJ
Operador Nacional do Registro de Títulos e Documentos e Civil das Pessoas Jurídicas

SOBRE ESTE GLOSSÁRIO

Este glossário foi elaborado para facilitar a compreensão do **Provimento CNJ N°213/2026** por parte de delegatários, prepostos, colaboradores e gestores que não necessariamente possuem formação técnica em Tecnologia da Informação ou Segurança da Informação.

Cada verbete apresenta uma definição clara e objetiva e, sempre que possível, uma analogia do dia a dia para ilustrar o conceito.

Os documentos exigidos pelo provimento estão descritos em seção própria, com informações sobre quem elabora, prazos e por quanto tempo devem ser guardados.

IRTDPJ BRASIL
Instituto de Registro de Títulos e Documentos e de Pessoas Jurídicas do Brasil

ON RTDPJ
Operador Nacional do Registro de Títulos e Documentos e Civil das Pessoas Jurídicas

Sumário - parte II

AES-256 (AES-256) — *Criptografia*

Padrão de criptografia considerado um dos mais seguros do mundo atualmente. O número 256 refere-se ao tamanho da chave usada para embaralhar os dados — quanto maior, mais difícil de quebrar. É o padrão mínimo exigido pelo Provimento para dados armazenados.

💡 **Analogia:** *É como uma fechadura com 2^{256} combinações possíveis. Um computador levaria bilhões de anos para tentar todas as combinações.*

Alta Disponibilidade (HA — High Availability) — *Infraestrutura*

Arquitetura de sistemas projetada para funcionar quase ininterruptamente, mesmo quando algum componente falha. Isso é feito por meio de redundância: há sempre um sistema 'reserva' pronto para assumir se o principal falhar.

💡 **Analogia:** *Como um gerador de emergência que liga automaticamente quando a energia cai, o serviço continua sem que o usuário perceba a interrupção.*

ANPD (Autoridade Nacional de Proteção de Dados) — *Órgão Regulador*

Autoridade Nacional de Proteção de Dados é o órgão federal responsável por fiscalizar o cumprimento da Lei Geral de Proteção de Dados (LGPD) no Brasil. Em caso de incidente de segurança, que coloque dados pessoais em risco, a serventia deve comunicar à ANPD.

Antivírus / Antimalware — *Segurança*

Programas que detectam, bloqueiam e removem softwares maliciosos (vírus, trojans, ransomware, spyware etc.) dos computadores. O provimento exige que todas as estações de trabalho e servidores da serventia utilizem esse tipo de proteção.

💡 **Analogia:** Como um segurança na porta de entrada, que inspeciona tudo que entra no computador e bloqueia o que parece suspeito.

ART (Anotação de Responsabilidade Técnica)

Documentação Técnica

Anotação de Responsabilidade Técnica (ART) é um documento emitido pelo CREA ou CFT que atesta que um engenheiro habilitado realizou e se responsabiliza tecnicamente por um serviço. No contexto do provimento, a ART é exigida para o laudo de aterramento elétrico.

Aterramento elétrico

Infraestrutura

Sistema de proteção elétrica que conecta os equipamentos à terra, desviando correntes indesejadas que poderiam danificar os equipamentos ou causar choques. O provimento exige aterramento adequado e laudo técnico atualizado com ART.

💡 **Analogia:** Como um para-raios: desvia a energia perigosa para o chão antes que ela danifique os equipamentos.

Auditoria / Trilha de auditoria (Log de auditoria)

Segurança / Rastreabilidade

Registro automático e detalhado de tudo que acontece em um sistema: quem acessou, o que fez, quando fez, qual o resultado. Esses registros são imutáveis (não podem ser alterados) e devem ser guardados por no mínimo 5 (cinco) anos. São essenciais para investigar incidentes e comprovar a integridade dos atos.

💡 **Analogia:** Como as câmeras de segurança de um banco: gravam tudo, com data e hora, e o vídeo não pode ser apagado.

Autenticação multifator (MFA / AMF)

Segurança de Acesso

Método de verificação de identidade que exige mais de uma forma de comprovação para liberar o acesso a um sistema. Geralmente combina algo que você sabe (senha), com algo que você tem (celular/token) ou algo que você é (biometria). O provimento exige MFA obrigatoriamente para todos os acessos administrativos.

💡 **Analogia:** Como o caixa eletrônico que pede o cartão físico e a senha. Assim, mesmo que alguém saiba sua senha, sem o cartão não consegue acessar.

Backup

Continuidade / Proteção de Dados

Cópia de segurança de todos os dados e sistemas da serventia, armazenada em local separado do sistema principal. Garante que, em caso de falha, ataque ou desastre, os dados possam ser restaurados. O provimento define prazos específicos de execução, armazenamento e teste de restauração.

💡**Analogia:** Como tirar fotocópias de documentos importantes e guardar em outro local seguro. Se o original sumir, você tem a cópia.

Backup completo

Continuidade

Cópia integral de todos os dados do sistema em um determinado momento. É mais demorado e ocupa mais espaço, mas garante uma imagem completa do sistema. Deve ser feito com frequência máxima de 24h (Cl. 3), 48h (Cl. 2) ou 72h (Cl. 1).

Backup incremental

Continuidade

Cópia apenas dos dados que foram modificados desde o último backup (completo ou incremental). É mais rápido e ocupa menos espaço. É usado para reduzir o POR - a janela de perda de dados -, pois captura alterações com mais frequência.

Backup offsite

Continuidade

Cópia de segurança armazenada fisicamente ou logicamente em local diferente do servidor principal da serventia. Garante que, mesmo em caso de desastre físico (incêndio, alagamento), os dados sobrevivam. Pode ser em nuvem, em mídia guardada em outro local ou em servidor remoto.

💡**Analogia:** É como guardar uma cópia das chaves da sua casa na casa de um familiar. Se perder as suas, ainda tem acesso.

Certificado digital

Autenticidade

Documento eletrônico que funciona como uma identidade digital, emitido por uma Autoridade Certificadora (AC). Garante a autenticidade de quem assina um documento eletrônico. A serventia deve manter inventário atualizado de todos os certificados digitais e renová-los antes do vencimento.

💡 **Analogia:** É como uma carteira de identidade eletrônica, que comprova quem você é no mundo digital.

CNJ (Conselho Nacional de Justiça)

Órgão Regulador

O Conselho Nacional de Justiça é o órgão do Poder Judiciário brasileiro, responsável pela supervisão administrativa, financeira e disciplinar dos serviços judiciais e extrajudiciais, incluindo os cartórios. É o órgão que publicou o Provimento nº 213/2026.

Criptografia

Segurança

Processo de transformar dados legíveis em um formato codificado (ilegível) que só pode ser decifrado por quem possui a chave correta. O provimento exige criptografia tanto para dados em trânsito (sendo transmitidos pela internet) quanto para dados em repouso (armazenados em servidores ou backups).

💡 **Analogia:** É como em um cofre digital os dados ficam 'trancados' e só quem tem a chave certa consegue lê-los.

DPO (Data Protection Officer)

LGPD / Governança

Encarregado pelo tratamento de dados pessoais. Pessoa responsável por garantir que a serventia cumpra as obrigações da LGPD: responder aos titulares de dados, comunicar incidentes à ANPD, orientar funcionários e fiscalizar o tratamento de dados pessoais. A designação é obrigatória quando exigida pela legislação.

Dossiê técnico

Documentação / Conformidade

Conjunto organizado de documentos, evidências técnicas e operacionais que demonstra que a serventia cumpriu os requisitos do provimento. Inclui atas, relatórios, registros de configuração, contratos, registros de capacitação etc. Para classes 2 e 3, deve conter hash digital assinado para garantir integridade.

💡**Analogia:** É como o dossiê de uma obra: planta, alvarás, notas fiscais, laudos — tudo reunido para comprovar que foi feito corretamente.

EOL (End of Life)

Infraestrutura / Segurança

Fim de vida útil de um software. Quando um fabricante declara EOL para um produto, ele para de lançar atualizações de segurança. Usar softwares EOL é proibido pelo provimento, pois vulnerabilidades conhecidas ficam sem correção, tornando o sistema um alvo fácil para ataques.

💡**Analogia:** É como usar um carro sem mais peças de reposição disponíveis; qualquer problema e não há mais como fazer o conserto com segurança.

Failover

Infraestrutura

Processo automático pelo qual um sistema secundário (reserva) assume as funções do sistema principal quando este falha, sem intervenção humana e com mínima interrupção. É o mecanismo central da alta disponibilidade.

💡**Analogia:** É como o copiloto de um avião, que assume os controles automaticamente se o piloto tiver algum problema.

Firewall

Segurança

Sistema de segurança que monitora e controla o tráfego de rede, bloqueando acessos não autorizados e filtrando dados suspeitos. O provimento exige firewall stateful (que analisa o contexto das conexões) com IPS/IDS para classes 1, 2 e 3.

💡**Analogia:** É como um porteiro eletrônico: verifica quem quer entrar na rede, deixa passar quem tem autorização e bloqueia os demais.

Hash / Hash criptográfico

Integridade de Dados

Sequência única de caracteres gerada a partir de um arquivo, que funciona como uma 'impressão digital' do conteúdo. Se uma vírgula for alterada no arquivo, o hash muda completamente.
É usado para verificar se arquivos ou documentos foram modificados sem autorização.

💡 **Analogia:** É como a impressão digital de um documento: única para aquele conteúdo específico. Se alguém alterar qualquer coisa, a 'digital' muda.

IaaS (Infrastructure as a Service)

Modelos de Contratação

Infraestrutura como Serviço. Modelo em que a serventia contrata, via internet, capacidade de servidores, armazenamento e rede de um provedor externo (ex.: AWS, Azure, Google Cloud), sem precisar comprar hardware físico.

IDS / IPS

Segurança

IDS (Intrusion Detection System): sistema que detecta tentativas de invasão à rede. IPS (Intrusion Prevention System): além de detectar, bloqueia ativamente a ameaça. O Provimento exige implantação de firewall stateful ou solução equivalente com IPS/IDS.

💡 **Analogia:** Como um sistema de alarme (IDS detecta o intruso) combinado com trancas automáticas (IPS bloqueia a entrada).

Incidente crítico

Segurança / Gestão

Evento de segurança da informação que compromete ou pode comprometer gravemente a disponibilidade, integridade, autenticidade, confidencialidade ou rastreabilidade do acervo. Deve ser comunicado à Corregedoria competente em até 72 horas. Exemplos: ataque de ransomware, vazamento de dados, indisponibilidade prolongada.

Interoperabilidade

Sistemas / Integração

Capacidade de sistemas diferentes trocarem informações de forma padronizada, segura e sem perda de dados. No contexto do provimento, as serventias devem ter sistemas aptos a integrar as plataformas de fiscalização do CNJ, usando formatos abertos como XML e PDF/A.

💡**Analogia:** É como tomadas universais: permitem conectar aparelhos de diferentes marcas e países sem adaptadores especiais.

LGPD (Lei Geral de Proteção de Dados Pessoais)

Legislação

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) define as regras para coleta, armazenamento, tratamento e compartilhamento de dados pessoais no Brasil. As serventias, como controladores de dados, devem observá-la integralmente, incluindo o registro de operações de tratamento e a comunicação de incidentes.

Log

Rastreabilidade

Registro automático gerado pelos sistemas a cada operação realizada: quem fez o quê, quando e qual foi o resultado. Os logs devem ser protegidos contra alteração e guardados por pelo menos 5 anos. São a principal evidência em investigações de incidentes.

💡**Analogia:** É como o diário de bordo de um navio: tudo que aconteceu fica registrado, com hora e responsável.

MFA (MFA / AMF)

Segurança de Acesso

Veja: Autenticação Multifator.

Nuvem / Cloud

Infraestrutura

Serviço de computação (armazenamento, processamento, softwares) prestado via internet por provedores externos, sem a necessidade de servidores físicos locais. O provimento admite o uso de nuvem para backup e infraestrutura, desde que atendidos os requisitos de segurança, criptografia e redundância geográfica.

💡 **Analogia:** Como alugar um cofre em um banco em vez de comprar um para colocar em casa. Conveniente, seguro, mas você precisa confiar no banco.

PCN (Plano de Continuidade de Negócios)

Documentação / Continuidade

Documento que descreve como a serventia continuará operando durante e após um incidente grave. Define riscos identificados, medidas de mitigação, responsáveis, e as ações a serem tomadas nos primeiros 30 e 90 dias após um problema. Deve incluir o RTO e o RPO definidos.

💡 **Analogia:** Como o plano de fuga de emergência de um edifício: todos sabem o que fazer, por onde sair e quem é responsável por cada etapa.

PDF/A

Interoperabilidade

Versão do formato PDF especialmente desenvolvida para arquivamento de longo prazo. Garante que o documento possa ser lido e reproduzido fielmente no futuro, sem depender de softwares ou configurações específicas. É um dos padrões abertos recomendados pelo provimento.

Pentest (Penetration Test)

Segurança / Auditoria

Teste de invasão. Simulação controlada e autorizada de um ataque cibernético ao ambiente tecnológico da serventia, realizada por profissional especializado, para identificar vulnerabilidades antes que hackers as explorem. Obrigatório para serventias de classe 3, a cada 2 anos, caso não operem integralmente em ambiente de solução contratada (SaaS).

💡 **Analogia:** Como contratar um ladrão profissional para testar se as fechaduras e alarmes da sua casa realmente funcionam. Melhor descobrir as falhas você mesmo do que quando for tarde demais.

Point-in-Time Recovery (PITR) — *Backup / Continuidade*

Técnica que permite restaurar um banco de dados para o estado exato em que ele estava em qualquer momento no passado (ex.: 'como estava às 14h23 de ontem'), não apenas no horário do último backup. É uma forma de atender ao RPO de forma mais precisa.

Política de Segurança da Informação (PSI) — *Documentação / Governança*

Documento formal que estabeleça, de forma expressa e estruturada, as diretrizes, objetivos estratégicos, cronogramas, responsabilidades e demais parâmetros que fundamentarão a elaboração, na etapa 2, do Plano de Continuidade de Negócios (PCN) e do Plano de Recuperação de Desastre (PRD). Deve cobrir: controle de acesso, criptografia, backups, gestão de incidentes, proteção de dados (LGPD), gestão de fornecedores, e integração com o PCN e PRD. É obrigatória para todas as classes.

Portabilidade de dados — *Governança / Continuidade*

Direito e capacidade de extrair todos os dados da serventia de um sistema e transferi-los para outro, em formato aberto e utilizável. O provimento exige que contratos garantam essa portabilidade e que seja feita simulação periódica dessa extração.

💡**Analogia:** É como poder transferir seu número de celular para outra operadora sem perder o histórico. Os dados são seus, não do fornecedor.

PRD (Plano de Recuperação de Desastres) — *Documentação / Continuidade*

Documento com as medidas técnicas e operacionais para restaurar sistemas e dados após um incidente grave. Complementa o PCN com detalhes técnicos de como a recuperação será feita, quais sistemas serão restaurados primeiro e em quanto tempo. Deve estar integrado ao PCN.

Redundância geográfica

Infraestrutura / Backup

Armazenamento de cópias dos dados em locais fisicamente distantes (ex.: cidades ou regiões diferentes). Garante que, mesmo em caso de desastre natural ou falha em um datacenter inteiro, os dados em outra localidade permaneçam intactos.

💡 **Analogia:** É como guardar documentos importantes em dois cofres em cidades diferentes. Uma enchente, por exemplo, não vai comprometer os dois ao mesmo tempo.

Relatório simplificado

Documentação / Conformidade

Versão simplificada do Dossiê Técnico, aceita para serventias de Classe 1. Deve conter: identificação da serventia e classe, descrição do requisito e solução adotada, demonstração de equivalência funcional, indicação das evidências disponíveis e declaração de responsabilidade assinada pelo titular da delegação.

Reversibilidade

Contratos / Governança

Garantia contratual e técnica de que todos os dados, configurações e registros da serventia serão devolvidos integralmente ao delegatário em caso de encerramento do contrato com o fornecedor ou troca de sistema, sem necessidade de autorização especial do fornecedor.

💡 **Analogia:** É como o direito de reaver todos os seus documentos, quando você encerra o contrato com uma empresa, sem barreiras nem taxas abusivas.

RPO (Recovery Point Objective)

Continuidade

Ponto de Recuperação Objetivo. Define a quantidade máxima de dados que a serventia aceita perder em caso de incidente. Expresso em tempo: 'no máximo, perder os dados das últimas X horas'. Classe 3: 4h. Classe 2: 12h. Classe 1: 24h. Quanto menor, mais frequente precisa ser o backup.

💡 **Analogia:** Se o RPO é de 4 horas, significa que os backups precisam ser feitos pelo menos a cada 4 horas. Assim, em pior caso, você perde apenas 4 horas de trabalho.

RTO (Recovery Point Objective)

Infraestrutura / Backup

Tempo de Recuperação Objetivo. Define o tempo máximo que a serventia pode ficar paralisada, após um incidente, até que os sistemas sejam restaurados e o serviço seja retomado. Classe 3: 8 horas. Classes 1 e 2: 24 horas. Deve ser documentado no PCN/PRD e comprovado por testes.

💡 **Analogia:** Se o RTO é de 8 horas, a serventia precisa garantir que, em qualquer emergência, voltará a funcionar em no máximo 8 horas.

SAI / UPS

Infraestrutura de Energia

Sistema de Alimentação Ininterrupta (também chamado de nobreak). Equipamento que fornece energia elétrica de forma contínua aos computadores mesmo em caso de queda de energia, por um período suficiente para salvar dados e desligar os equipamentos com segurança. O provimento recomenda autonomia mínima de 30 minutos.

💡 **Analogia:** É como um gerador de emergência portátil, que entra em ação automaticamente quando a luz cai.

SaaS (Software as a Service)

Contratos / Governança

Software como Serviço. Modelo em que o software é acessado via internet, sem instalação local, sendo gerenciado e hospedado pelo fornecedor. Exemplos: Google Workspace, sistemas de cartório em nuvem. O provimento admite esse modelo, com exigências específicas para contrato, segurança e portabilidade.

Segregação de funções

Segurança / Governança

Princípio de controle interno que divide responsabilidades críticas entre pessoas diferentes, evitando que uma única pessoa tenha controle total sobre um processo sensível. No contexto do provimento, aplica-se especialmente à gestão de chaves criptográficas e ao controle de acesso a sistemas críticos.

💡 **Analogia:** Como em um banco, onde quem aprova um empréstimo não é a mesma pessoa que faz o pagamento. O controle mútuo reduz fraudes.

Segregação lógica de rede

Segurança / Infraestrutura

Separação virtual das redes internas da serventia em segmentos distintos, de modo que os computadores de atendimento ao público não se comuniquem livremente com os servidores administrativos. Isso limita o alcance de um possível ataque. Tecnicamente implementada por VLANs ou soluções equivalentes.

💡 **Analogia:** Como dividir um escritório com paredes internas de vidro: as áreas ficam separadas, mas a estrutura é a mesma.

SGBD (Sistema Gerenciador de Banco de Dados)

Infraestrutura de Energia

Sistema Gerenciador de Banco de Dados é o software que organiza, armazena e controla o acesso a todos os dados da serventia. O provimento exige que o SGBD tenha integridade transacional (garante que operações incompletas não corrompam os dados) e logs ativos (registros de tudo que acontece no banco).

SIEM (Security Information and Event Management)

Segurança / Monitoramento

Sistema que coleta, agrega e analisa automaticamente os logs de segurança de diferentes fontes (servidores, firewalls, aplicações), identificando padrões suspeitos e gerando alertas. O provimento cita o SIEM como exemplo de ferramenta para monitoramento avançado, mas admite soluções equivalentes.

Sistema Justiça Aberta — *Conformidade / Declarações*

Plataforma digital do CNJ por meio da qual os responsáveis pelas serventias deverão declarar o cumprimento de cada etapa do Provimento nº 213/2026, renovar anualmente a declaração de conformidade e apresentar síntese do dossiê técnico. Declarações falsas sujeitam o responsável a penalidades.

TIC (Tecnologia da Informação e Comunicação) — *Geral*

Termo que abrange todos os recursos tecnológicos usados para criar, armazenar, transmitir e acessar informações: computadores, servidores, redes, softwares, internet, equipamentos de telecomunicações etc.

TLS (Transport Layer Security) — *Criptografia*

Protocolo de segurança que criptografa as comunicações transmitidas pela internet, protegendo os dados contra interceptação. O provimento exige TLS 1.2 ou superior para todas as transmissões de dados sensíveis. É o protocolo por trás do 'HTTPS' nos sites.

💡**Analogia:** É como enviar uma carta dentro de um envelope lacrado em vez de um cartão-postal aberto. Ninguém no caminho consegue ler o conteúdo.

Tolerância a falhas — *Infraestrutura*

Capacidade de um sistema continuar funcionando (ainda que com desempenho reduzido) quando um de seus componentes apresenta falha parcial. Diferente da alta disponibilidade (que usa redundância completa), a tolerância a falhas permite uma degradação controlada sem parada total.

Vulnerabilidade crítica — *Segurança*

Falha técnica em um software, configuração ou infraestrutura cuja exploração por atacantes pode causar dano grave ao sistema. Vulnerabilidades críticas devem ser corrigidas em no máximo 30 dias. Em caso de exploração ativa comprovada, as medidas de contenção devem ser adotadas em até 72 horas. As medidas adotadas para a contenção e correção de vulnerabilidades críticas devem ser registradas formalmente no dossiê técnico da serventia.

VLAN (Virtual LAN) | *Infraestrutura de Rede*

Rede Local Virtual. Tecnologia que permite separar logicamente uma rede física em múltiplas redes virtuais independentes, sem necessidade de cabeamento adicional. É a forma mais comum de implementar a segmentação lógica de rede exigida pelo provimento para classes 2 e 3.

WORM (Write Once, Read Many) | *Armazenamento / Integridade*

Tecnologia de armazenamento que permite gravar dados apenas uma vez, impedindo qualquer alteração ou exclusão posterior. É usada para garantir a imutabilidade de backups e trilhas de auditoria, assegurando que registros não possam ser adulterados nem mesmo por administradores do sistema.

💡**Analogia:** Como um cofre que só abre para colocar coisas, mas não para tirá-las, garantindo que o que foi guardado permaneça intacto.

XML (eXtensible Markup Language.) | *Interoperabilidade*

Formato aberto e padronizado para representar e trocar dados estruturados entre sistemas diferentes. O provimento recomenda o uso de XML (e de PDF/A) por serem formatos não proprietários, garantindo que os dados possam ser lidos por qualquer sistema no futuro.

GUIA DE DOCUMENTOS OBRIGATÓRIOS

Esta seção descreve cada documento que a serventia deve elaborar, manter e guardar para estar em conformidade com o Provimento Nº 213/2026. Para cada documento são indicados: quem deve elaborar, qual o prazo e por quanto tempo deve ser guardado.

Política Interna de Segurança da Informação

Todas as classes (obrigatório)

Autoridade Nacional de Proteção de Dados é o órgão federal responsável por fiscalizar o cumprimento da Lei Geral de Proteção de Dados (LGPD) no Brasil. Em caso de incidente de segurança, que coloque dados pessoais em risco, a serventia deve comunicar à ANPD.

Quem elabora: Delegatário, com apoio técnico **Prazo:** Etapa 1 (90 a 210 dias da vigência).
Guarda: Permanente, revisar sempre que houver alteração normativa relevante

Plano de Continuidade de Negócios (PCN)

Todas as classes (obrigatório)

Define como a serventia vai continuar operando durante e após uma crise. Deve conter: identificação e avaliação de riscos, medidas de mitigação, RTO e RPO definidos para a classe, e plano de ação para os primeiros 30 e 90 dias após um incidente. Deve ser documentado e testado.

Quem elabora: Delegatário, com apoio técnico **Prazo:** Etapa 2 (mesmo prazo da etapa 1).
Guarda: Permanente, revisar ao menos anualmente e após incidentes

Plano de Recuperação de Desastres (PRD)

Todas as classes (obrigatório)

Documento técnico complementar ao PCN, detalhando os passos exatos para restaurar sistemas e dados após um desastre. Pode ser integrado ao PCN em documento único, desde que contenha todos os elementos exigidos. Deve definir explicitamente o RTO e o RPO.

Quem elabora: Delegatário, com apoio técnico **Prazo:** Etapa 2 (mesmo prazo do PCN).
Guarda: Permanente, revisar após cada teste e após incidentes relevantes

Inventário de Ativos Tecnológicos

Todas as classes (obrigatório)

Listagem completa e atualizada de todos os recursos tecnológicos da serventia: computadores, servidores, roteadores, switches, softwares, licenças, certificados digitais, contratos de TI, integrações com outros sistemas e histórico de atualizações. É a base para a gestão de vulnerabilidades e para auditorias.

Quem elabora: Responsável técnico interno **Prazo:** Etapa 1
Guarda: Manter atualizado permanentemente

Documento de Arquitetura Tecnológica

Todas as classes (obrigatório)

Mapa técnico simplificado do ambiente de TI. Deve conter: topologia básica da rede, ambientes utilizados (local, nuvem, híbrido, SaaS), fluxos de dados críticos, localização dos backups, integrações externas, adotando-se mecanismos de alta disponibilidade ou redundância.

Quem elabora: Responsável técnico interno / Fornecedor **Prazo:** Etapa 2.
Guarda: Manter atualizado sempre que houver mudança relevante

Ata de Teste de Restauração de Backup

Todas as classes (obrigatório)

Registro formal do teste periódico que comprova que o backup pode ser efetivamente restaurado dentro dos parâmetros de RTO e RPO. O modelo completo está no Anexo V do provimento e deve conter: escopo do teste, metodologia, resultados (RTO e RPO aferidos), método de verificação de integridade e assinaturas dos responsáveis.

Quem elabora: Responsável técnico + Delegatário **Prazo:** Classe 3: semestral | classes 1 e 2: anual. **Guarda:** Permanente, revisar após cada teste e após incidentes relevantes

Dossiê Técnico de Conformidade

Classes 2 e 3 (obrigatório)
Classe 1: Relatório Simplificado

Conjunto organizado de todas as evidências que comprovam o cumprimento dos requisitos de cada etapa do Provimento: atas, relatórios, contratos revisados, registros de configuração, registros de capacitação e evidências técnicas (prints, logs, relatórios de sistemas). Para Classes 2 e 3, deve incluir lista de hash assinada digitalmente.

Quem elabora: Responsável técnico + Delegatário **Prazo:** Ao final de cada etapa (1 a 5)
Guarda: Mínimo de 5 anos

Registros de Trilhas de Auditoria (Logs)

Todas as classes (obrigatório)

Conjunto organizado de todas as evidências que comprovam o cumprimento dos requisitos de cada etapa do provimento: atas, relatórios, contratos revisados, registros de configuração, registros de capacitação e evidências técnicas (prints, logs, relatórios de sistemas). Para Classes 2 e 3, deve incluir lista de hash assinada digitalmente.

Quem elabora: Sistema / TI (automático) **Prazo:** Contínuo — desde a vigência do Provimento. **Guarda:** Mínimo de 5 anos (imutáveis)

Registros de Operações de Tratamento de Dados (LGPD)

Todas as classes (obrigatório)

Mapeamento de todas as atividades da serventia que envolvem dados pessoais: quais dados são coletados, para qual finalidade, por quanto tempo ficam armazenados, com quem são compartilhados etc. Exigido pela LGPD para controladores de dados.

Quem elabora: DPO / Delegatário **Prazo:** Etapa 1 e manter atualizado
Guarda: Permanente

Contratos Revisados com Fornecedores de TI

Todas as classes (obrigatório)

Todos os contratos com empresas que tratam, armazenam ou processam dados da serventia devem ser revisados para incluir obrigatoriamente: cláusulas de confidencialidade, reversibilidade, portabilidade de dados em formato interoperável, gestão de incidentes e conformidade com a LGPD, além de serem guardados e atualizados sempre que houver qualquer modificação. Contratos sem as cláusulas citadas não atendem ao Provimento.

Quem elabora: Delegatário / Jurídico **Prazo:** Etapa 1
Guarda: Vigência + 5 anos

Laudo de Aterramento Elétrico com ART

Todas as classes (obrigatório)

Documento técnico emitido por engenheiro habilitado, com Anotação de Responsabilidade Técnica (ART), que atesta que o sistema elétrico da serventia possui aterramento adequado para proteger os equipamentos de TI. Deve ser mantido atualizado.

Quem elabora: Engenheiro habilitado (externo) **Prazo:** Etapa 2 e sempre que houver alteração na infraestrutura elétrica. **Guarda:** Mínimo de 5 anos

Relatório de Conformidade de Auditoria das Trilhas

Classes 2 e 3 (obrigatório)
Classe 1: recomendado

Relatório que atesta formalmente que as trilhas de auditoria da serventia atendem a todos os requisitos técnicos: imutabilidade comprovada, identificação inequívoca do usuário, sincronização de tempo por fonte confiável, retenção mínima de 5 anos e integração com as rotinas de backup.

Quem elabora: Responsável técnico **Prazo:** Etapa 4.
Guarda: Mínimo de 5 anos

Relatório de Pentest (Teste de Intrusão)

Classe 3 (obrigatório, a cada 2 anos)

Relatório produzido após um teste de invasão controlado ao ambiente tecnológico da serventia. Deve conter: escopo, metodologia, resultados, vulnerabilidades encontradas, plano de correção e declaração de aderência assinada pelo responsável técnico. Serventias 100% SaaS podem substituir por relatório da empresa desenvolvedora + declaração do titular.

Quem elabora: Empresa especializada externa (ou relatório coletivo do Operador Nacional)
Prazo: Etapa 4 — a cada 2 anos e após alterações relevantes de infraestrutura
Guarda: Mínimo de 5 anos

Plano de Reversibilidade e Portabilidade de Dados

Todas as classes (obrigatório) - Etapa 5

Documento que descreve como todos os dados da serventia poderão ser extraídos e transferidos para outro sistema em formato aberto e interoperável, sem dependência do fornecedor atual. Deve ser acompanhado de simulação documentada de extração integral do acervo, realizada periodicamente (24 a 36 meses conforme a classe).

Quem elabora: Responsável técnico + Delegatário **Prazo:** Etapa 5
Guarda: Mínimo de 5 anos

Ata de Simulação de Extração do Acervo

Todas as classes (obrigatório — Etapa 5)

Registro formal da simulação de extração integral de todos os dados da serventia em formato interoperável (portabilidade). Comprova que, em caso de troca de fornecedor ou de gestão, os dados podem ser migrados sem perda de integridade, autenticidade ou rastreabilidade.

📝 **Quem elabora**: Responsável técnico + Delegatário 🗓️ **Prazo:** Cl. 3: a cada 24 meses | Cl. 2: a cada 30 meses | Cl. 1: a cada 36 meses 📎 **Guarda:** Mínimo de 5 anos

Declaração de Conclusão de Etapa (1 a 5)

Todas as classes (obrigatório após cada etapa)

Declaração formal, assinada pessoalmente pelo titular da delegação (delegatário, interino ou interventor), atestando que todos os requisitos de uma etapa foram cumpridos integralmente. Deve ser registrada no Sistema Justiça Aberta. Declaração falsa sujeita o responsável a penalidades.

📝 **Quem elabora**: Titular da delegação (pessoalmente)
🗓️ **Prazo:** Ao concluir cada etapa — registrar no sistema Justiça Aberta 📎 **Guarda:** Permanente

Declaração Anual de Conformidade

Todas as classes (obrigatório — anual)

Renovação anual da declaração de conformidade com o provimento, acompanhada de síntese do dossiê técnico com evidências mínimas de conformidade com os requisitos estruturais e operacionais. Deve ser registrada no Sistema Justiça Aberta.

📝 **Quem elabora**: Titular da delegação 🗓️ **Prazo:** Anualmente — no sistema Justiça Aberta
📎 **Guarda:** Permanente

Registros de Capacitação de Colaboradores

Todas as classes (obrigatório)

Documentação formal de todos os treinamentos realizados pela serventia em segurança da informação, operação segura de sistemas e rotinas de backup: lista de participantes, conteúdo abordado, carga horária e data. O provimento exige que a capacitação seja periódica.

📝 **Quem elabora**: Responsável técnico / RH 🗓️ **Prazo:** Continuamente, desde a etapa 2
📎 **Guarda:** Mínimo de 5 anos

TABELA DE REFERÊNCIA RÁPIDA: RPO, RTO E PRAZOS

Resumo visual dos principais parâmetros técnicos e prazos do Provimento, por classe de serventia.

Parâmetro	CLASSE 1	CLASSE 2	CLASSE 3
RPO máximo (perda de dados)	24 horas	12 horas	4 horas
RTO máximo (tempo de recuperação)	24 horas	24 horas	8 horas
Receita semestral máxima	R$ 100.000	R$ 500.000	Acima de R$ 500k
Backup completo (intervalo máximo)	72 horas	48 horas	24 horas
Teste de restauração	Anual	Anual	Semestral
Pentest	Não obrigatório	Não obrigatório	A cada 2 anos
Velocidade mínima de internet	2 Mbps	10 Mbps	50 Mbps
Prazo etapas 1 e 2	210 dias	150 dias	90 dias
Prazo total (etapas 1 a 5)	36 meses	30 meses	24 meses
Nível mínimo de trilhas de auditoria	Essencial	Essencial	Intermediário
Comprovação de conformidade	Relatório simplificado	Dossiê técnico	Dossiê técnico
Simulação de extração do acervo	A cada 36 meses	A cada 30 meses	A cada 24 meses
Retenção mínima de logs e dossiês	5 anos	5 anos	5 anos

ONRTDPJ

Operador Nacional do Registro de Títulos e Documentos e Civil das Pessoas Jurídicas

www.onrtdpj.org.br

@centralonrtdpj

@centralonrtdpj

centralonrtdpj

IRTDPJ BRASIL

Instituto de Registro de Títulos e Documentos e de Pessoas Jurídicas do Brasil

www.irtdpjbrasil.org.br

@irtdpjbrasil

@irtdpjbrasil

irtdpjbrasil