OPERADOR NACIONAL DO REGISTRO CIVIL DAS PESSOAS NATURAIS

Guia Rápido de Implementação do Provimento nº 213/2026

Orientações práticas essenciais para serventias do Registro Civil

Versão preliminar

13 de março de 2026

Expediente Institucional

Operador Nacional do Registro Civil das Pessoas Naturais (ON-RCPN)

Presidente: Luis Carlos Vendramin Junior

Vice-Presidente: Gustavo Fiscarelli

Apoio técnico

Laboratório de Pesquisa e Desenvolvimento do Registro Civil das Pessoas Naturais (LabREC)

Supervisor: Prof. Ricardo Custódio

Corpo técnico de apoio:

- Bernardo Pandolfi Costa
- Frederico Schardong
- Gabriel Holstein Meireles
- Gustavo Zambonin
- Lucas Mayr de Athayde
- Maurício Korath

Título: Guia Rápido de Implementação do Provimento nº 213/2026

Instituição responsável: ON-RCPN

Apoio técnico: LabREC

Versão: 0.3

Data: 13 de março de 2026

Este guia rápido resume as medidas essenciais que as serventias devem observar para implementar, de forma simples e prática, os requisitos mínimos do Provimento nº 213/2026.

Apresentação

O presente *Guia Rápido de Implementação do Provimento nº 213/2026* foi elaborado pelo Operador Nacional do Registro Civil das Pessoas Naturais (ON-RCPN), com apoio técnico do Laboratório de Pesquisa e Desenvolvimento do Registro Civil (LabREC), para orientar as serventias do Registro Civil das Pessoas Naturais na adoção das medidas de segurança da informação estabelecidas pelo Conselho Nacional de Justiça.

O Provimento nº 213/2026 representa um marco regulatório na proteção do acervo registral digital brasileiro, ao definir requisitos mínimos de segurança da informação, continuidade operacional e gestão tecnológica aplicáveis a todas as serventias, com exigências proporcionais à capacidade econômica de cada unidade.

Este guia traduz esses requisitos normativos em orientações práticas e operacionais, organizadas em vinte e uma seções e seis apêndices. O documento abrange desde a classificação econômica das serventias e os prazos vinculantes de implementação até a descrição detalhada dos controles técnicos exigidos tais como controle de acessos e autenticação multifator, criptografia de dados em trânsito e em repouso, rotinas automatizadas de *backup* com proteção contra *ransomware*, registro de eventos com trilhas de auditoria imutáveis, segmentação de rede com *firewall stateful*, gestão de vulnerabilidades e documentação de conformidade.

Para cada controle, o guia apresenta o fundamento normativo no Provimento, o nível de exigência por classe de serventia (Classes 1, 2 e 3), as formas práticas de implementação com recursos amplamente disponíveis e as evidências mínimas que devem compor o dossiê técnico da unidade. Roteiros visuais de implementação, organizados por classe e por etapa, permitem ao delegatário acompanhar o progresso da adequação de forma objetiva.

O documento inclui ainda modelos prontos para uso imediato: política básica de segurança da informação, registros de rotinas de *backup* e de testes de restauração, controle de usuários autorizados, registro de incidentes de segurança e arquitetura mínima recomendada para a infraestrutura tecnológica das serventias.

As recomendações aqui reunidas priorizam a simplicidade operacional e a viabilidade econômica, reconhecendo a diversidade das serventias brasileiras. A proposta não é impor soluções tecnológicas complexas, mas demonstrar que a conformidade com o Provimento nº 213 pode ser alcançada de forma gradual, organizada e sustentável, utilizando recursos já disponíveis nos sistemas operacionais, nos equipamentos de rede e nas plataformas registrais em uso.

Este guia possui caráter orientativo. Em caso de divergência, prevalece sempre o texto normativo do Provimento nº 213 e das demais normas editadas pelo Conselho Nacional de Justiça e pelas Corregedorias competentes.

Sumário

1 Introdução e finalidade do guia

Objetivo prático do guia

Este guia apresenta, em linguagem simples e direta, as medidas mínimas que uma serventia do Registro Civil deve adotar para iniciar a implementação das exigências de segurança da informação previstas no Provimento nº 213/2026 do Conselho Nacional de Justiça. As orientações aqui reunidas traduzem os requisitos normativos em práticas operacionais acessíveis, compatíveis com a realidade tecnológica da maioria das serventias brasileiras.

A crescente digitalização dos serviços prestados pelas serventias do Registro Civil das Pessoas Naturais ampliou significativamente a importância da segurança da informação, da proteção dos dados registrais e da continuidade operacional dos sistemas utilizados no cotidiano das unidades.

Nesse contexto, o Provimento nº 213 do Conselho Nacional de Justiça estabelece requisitos mínimos de segurança da informação e de gestão tecnológica aplicáveis às serventias do Registro Civil, com o objetivo de reduzir riscos operacionais, proteger o acervo registral e garantir a continuidade da prestação dos serviços à sociedade.

Embora o Provimento trate de diversos aspectos técnicos e organizacionais, a maior parte das medidas previstas pode ser implementada por meio de práticas simples e amplamente disponíveis nos sistemas operacionais, nas infraestruturas de rede e nos próprios sistemas registrais utilizados pelas serventias.

Este guia foi elaborado justamente para traduzir essas exigências em orientações práticas e operacionais, facilitando sua compreensão e implementação no ambiente cotidiano das serventias.

Adicionalmente, o guia adota, sempre que juridicamente possível, a lógica de implementação proporcional e, quando cabível, centralizada, nos termos do art. 13, §§4º a 7º do Provimento nº 213.

1.1 Objetivo do documento

O objetivo deste documento é apresentar, em linguagem clara e acessível, um conjunto de orientações práticas para auxiliar as serventias do Registro Civil das Pessoas Naturais na implementação das exigências estabelecidas pelo Provimento nº 213 do Conselho Nacional de Justiça.

O guia busca identificar as medidas essenciais de segurança da informação que devem ser adotadas pelas serventias, indicando formas simples e viáveis de implementação, compatíveis com a realidade tecnológica da maioria das unidades registrais brasileiras.

Para isso, o documento organiza os requisitos do Provimento em um conjunto reduzido de controles fundamentais, apresenta orientações práticas para sua implementação e sugere formas simples de documentação que permitam demonstrar a adoção das medidas de segurança recomendadas.

A proposta não é introduzir soluções tecnológicas complexas ou de alto custo, mas orientar a adoção consistente de boas práticas que contribuam para:

- proteger os dados registrais contra acesso indevido ou perda de informação;
- reduzir riscos tecnológicos associados ao uso de sistemas digitais;

- garantir maior estabilidade e continuidade na prestação dos serviços registrais;
- facilitar a demonstração de conformidade com os requisitos do Provimento nº 213.

Dessa forma, o guia pretende servir como referência prática para delegatários, interinos, interventores e profissionais de tecnologia da informação que atuam nas serventias, apoiando a implementação gradual e sustentável das medidas de segurança previstas na regulamentação aplicável.

1.2 Público-alvo

Este guia foi elaborado principalmente para oficiais de registro civil, substitutos, escreventes e profissionais de tecnologia da informação que atuam nas serventias do Registro Civil das Pessoas Naturais (RCPN).

Seu objetivo é apoiar a implementação prática das exigências estabelecidas pelo Provimento nº 213 do Conselho Nacional de Justiça, traduzindo seus requisitos técnicos e organizacionais em orientações claras, objetivas e aplicáveis no cotidiano das serventias.

O documento também pode ser útil para empresas desenvolvedoras de sistemas registrais, equipes técnicas de associações de classe, bem como para profissionais responsáveis pela operação e manutenção da infraestrutura tecnológica utilizada pelos cartórios.

Considerando a grande heterogeneidade existente entre as serventias brasileiras, tanto em termos de infraestrutura tecnológica quanto de disponibilidade de suporte especializado, este guia foi concebido com foco na simplicidade operacional. As recomendações aqui apresentadas priorizam soluções amplamente disponíveis em sistemas operacionais e plataformas comerciais comuns, evitando arquiteturas complexas ou que exijam gestão técnica avançada.

Assim, o guia busca servir como uma referência prática para a adoção de medidas de segurança da informação, continuidade operacional e proteção de dados compatíveis com as exigências do Provimento nº 213.

1.3 O que este guia não substitui

Este guia possui caráter orientativo e foi elaborado para auxiliar as serventias do Registro Civil das Pessoas Naturais na compreensão e na implementação prática das exigências estabelecidas pelo Provimento nº 213 do Conselho Nacional de Justiça.

Entretanto, este documento não substitui o próprio texto normativo do Provimento, que permanece como a referência jurídica e regulatória oficial. Em caso de dúvida interpretativa ou eventual divergência entre as orientações aqui apresentadas e o texto normativo, deve prevalecer sempre o disposto no Provimento nº 213 e nas demais normas aplicáveis editadas pelo Conselho Nacional de Justiça e pelas Corregedorias competentes.

Este guia também não substitui eventuais manuais técnicos, normas complementares ou orientações operacionais que venham a ser publicadas pelo Operador Nacional do Registro Civil das Pessoas Naturais (ON-RCPN), pelas associações representativas do setor ou pelos próprios fornecedores de sistemas utilizados pelas serventias.

Por fim, este documento não pretende esgotar todas as possibilidades técnicas existentes para a implementação dos controles de segurança e de gestão previstos no Provimento. As recomendações aqui apresentadas representam caminhos práticos e simplificados, adequados à realidade da maioria das serventias, podendo ser complementadas por soluções

técnicas equivalentes ou mais avançadas, desde que observados os requisitos estabelecidos na regulamentação aplicável.

1.4 Organização do guia

Este guia está estruturado em vinte e uma seções e seis apêndices, organizados de forma progressiva: as seções iniciais situam o leitor quanto ao propósito e ao contexto normativo do documento; as seções intermediárias detalham os controles técnicos que devem ser implementados; e as seções finais oferecem instrumentos práticos de planejamento, documentação e verificação contínua. Os apêndices reúnem modelos prontos para uso imediato nas serventias. A seguir, descreve-se o conteúdo de cada parte.

A **Seção 1** - *Introdução e finalidade do guia* - apresenta o contexto que motivou a elaboração deste documento. Explica que a crescente digitalização dos serviços registrais ampliou a importância da segurança da informação e que o Provimento n.º 213/2026 do Conselho Nacional de Justiça (CNJ) estabelece os requisitos mínimos a serem adotados pelas serventias. Define o objetivo do guia, identifica seu público-alvo - delegatários, escreventes e responsáveis técnicos das serventias - e esclarece que o documento é um instrumento de apoio à implementação, não substituindo o texto normativo original nem a assistência técnica especializada.

A **Seção 2** - *Como usar este guia* - orienta o leitor sobre as diferentes formas de consultar o documento conforme a sua necessidade imediata. Propõe três roteiros de leitura: uma leitura rápida de cinco minutos para uma visão geral das prioridades; uma leitura voltada ao início da implementação, com foco nos controles essenciais; e uma leitura para manutenção da conformidade, destinada a serventias que já iniciaram o processo e precisam verificar a situação atual.

A **Seção 3** - *Visão geral do Provimento 213* - contextualiza a norma do ponto de vista regulatório, descrevendo sua finalidade, os riscos operacionais e de segurança que ela busca reduzir, e os principais impactos práticos para as serventias. Explica o que efetivamente muda na rotina das unidades registrais e o que permanece inalterado, oferecendo ao leitor uma compreensão clara do alcance e dos limites da norma.

A **Seção 4** - *Classificação da serventia* - descreve o critério econômico utilizado para enquadrar cada serventia em uma das três classes previstas no Provimento (Classe 1, Classe 2 e Classe 3). Explica as subclasses existentes, a possibilidade de reenquadramento periódico e o impacto direto do enquadramento sobre o conjunto de controles que a serventia deverá implementar. A seção orienta o delegatário a identificar corretamente sua classe antes de planejar qualquer ação.

A **Seção 5** - *Prazos de implementação* - informa os prazos estabelecidos pelo Provimento para a conclusão das etapas iniciais obrigatórias e para a implementação integral de todos os controles. Aborda também as condições para solicitação de prorrogação excepcional e o procedimento de declaração de conformidade no Sistema Justiça Aberta, que é a plataforma do CNJ destinada ao acompanhamento da adequação das serventias.

A **Seção 6** - *O que cada classe precisa implementar* - detalha, de forma comparativa, os controles exigidos para cada uma das três classes de serventias. Apresenta os requisitos específicos da implementação essencial (Classe 1), da implementação intermediária (Classe 2) e da implementação ampliada (Classe 3), além de um quadro resumo que facilita a identificação das diferenças e das obrigações adicionais a cada nível de enquadramento.

A **Seção 8** - *Roteiro visual de implementação por classe* - apresenta, por meio de diagramas e fluxos simplificados, o caminho de implementação adequado a cada classe de serventia. O roteiro visual permite que o delegatário identifique rapidamente quais etapas já foram concluídas, quais estão em andamento e quais ainda precisam ser iniciadas, servindo como painel de acompanhamento do processo de conformidade.

A **Seção 9** - *Checklist rápido de conformidade* - oferece uma lista de verificação objetiva que permite ao responsável pela serventia avaliar, em poucos minutos, o estágio atual de adequação às exigências do Provimento. Os itens do checklist são organizados por tema e indicam se cada controle é obrigatório para todas as classes ou apenas para determinados níveis de enquadramento.

A **Seção 10** - *Os 10 controles essenciais* - apresenta, de forma sintética e acessível ao delegatário, os dez controles de segurança considerados fundamentais para qualquer serventia, independentemente de sua classe. Abrange: proteção da infraestrutura elétrica por meio de nobreaks; disponibilidade de conexão estável à internet com rede organizada; utilização de sistemas operacionais com suporte vigente; criação de contas individualizadas para cada usuário; adoção de autenticação forte para acessos críticos; criptografia dos dados em trânsito e em repouso; realização de backup automático e externo; testes periódicos de restauração; e manutenção de documentação mínima de conformidade.

A **Seção 11** - *Implementação prática dos controles* - complementa a seção anterior com orientações operacionais detalhadas para a adoção de cada controle. Aborda a infraestrutura elétrica, a configuração de rede e conectividade, a atualização de sistemas operacionais, a gestão de acessos, a aplicação de criptografia e a organização do backup com armazenamento externo, descrevendo procedimentos concretos e compatíveis com a realidade tecnológica das serventias.

A **Seção 12** - *Acessos, autenticação e senhas* - aprofunda os requisitos relacionados à gestão de identidades e ao controle de acesso aos sistemas da serventia. Trata da obrigatoriedade de contas individualizadas, das políticas de senha adequadas ao nível de risco, da autenticação multifator (MFA) para acessos a sistemas críticos e do uso do sistema de autenticação IdRC disponibilizado pelo ON-RCPN para as serventias integradas à plataforma federada.

A **Seção 13** - *Criptografia de dados* - detalha os requisitos e as formas práticas de aplicar criptografia tanto aos dados em trânsito quanto aos dados em repouso. Orienta sobre a seleção de protocolos e algoritmos adequados, a gestão de chaves criptográficas e sua revisão periódica, e a obrigatoriedade de cifrar os backups externos. Oferece orientações graduadas conforme a classe da serventia.

A **Seção 14** - *Backup e continuidade operacional* - trata do planejamento e da execução das rotinas de backup como pilar central da continuidade operacional da serventia. Explica os conceitos de Recovery Time Objective (RTO) e Recovery Point Objective (RPO), descreve como configurar o backup automático, a necessidade de dois ambientes independentes de armazenamento, a proteção dos backups contra ataques de ransomware e a importância dos testes regulares de restauração. Inclui orientações para elaboração de um plano simplificado de continuidade operacional.

A **Seção 15** - *Registro de eventos e auditoria* - apresenta os requisitos relacionados à geração, ao armazenamento e à análise dos registros de eventos (logs) dos sistemas da serventia. Explica quais eventos devem ser registrados, por quanto tempo os logs devem ser retidos e quais são os níveis mínimos de auditoria exigidos por classe. Orienta também

sobre análise básica de eventos para detecção de acessos indevidos ou comportamentos anômalos.

A **Seção 16** - *Proteção contra malware e manutenção dos sistemas* - aborda as medidas de proteção contra software malicioso, a atualização sistemática dos sistemas e aplicativos e as boas práticas operacionais para reduzir a superfície de ataque. Trata ainda do teste de intrusão (*pentest*), obrigatório para serventias de Classe 3, descrevendo quando ele é exigido, as hipóteses de dispensa ou simplificação e o que o relatório do teste deve demonstrar.

A **Seção 18** - *Documentação mínima de conformidade* - orienta a serventia sobre como organizar o dossiê técnico que comprova a adoção das medidas de segurança. Detalha os elementos mínimos que o dossiê deve conter, a forma de organizar as evidências, o procedimento de declaração de conformidade no Sistema Justiça Aberta e a necessidade de revisão e atualização periódica dos documentos.

A **Seção 19** - *Roteiro prático de início imediato* - oferece um plano de ação em quatro etapas sequenciais para serventias que estão iniciando o processo de adequação: diagnóstico inicial da situação atual; organização dos acessos e dos sistemas; proteção dos dados por meio de criptografia e backup; e verificação final com produção da documentação de conformidade. O roteiro é apresentado de forma objetiva, com ações concretas para cada etapa.

A **Seção 20** - *Modelo simplificado de dossiê técnico* - apresenta um modelo pronto de dossiê que a serventia pode adotar imediatamente, descrevendo sua finalidade, a estrutura mínima recomendada e as orientações para atualização e manutenção contínua do documento ao longo do tempo.

A **Seção 21** - *Checklist final de verificação periódica* - apresenta uma lista consolidada de todos os controles abordados no guia, organizada para uso em revisões regulares da conformidade. Sugere uma periodicidade de revisão para cada categoria de controle, auxiliando a serventia a manter a adequação de forma sustentada após a implementação inicial.

A **Seção 22** - *Considerações finais* - encerra a parte principal do guia com uma síntese das principais mensagens do documento, reforçando que a segurança da informação é um processo contínuo e que as medidas descritas representam um ponto de partida, não um estado definitivo. Incentiva as serventias a manterem a cultura de segurança no cotidiano e a buscarem apoio técnico sempre que necessário.

A **Seção 24** - *Glossário de termos técnicos* - reúne as definições dos principais termos e siglas utilizados ao longo do guia, em linguagem acessível ao público não especializado. O glossário permite que o leitor consulte rapidamente o significado de conceitos técnicos sem precisar recorrer a fontes externas, favorecendo a compreensão do documento por qualquer profissional da serventia.

Além das seções principais, o guia disponibiliza seis apêndices com modelos prontos para uso imediato:

O **Apêndice A** - *Modelo de Política Básica de Segurança da Informação* - apresenta um modelo de política de segurança que a serventia pode adotar e adaptar à sua realidade, cobrindo princípios gerais, diretrizes básicas, padrões criptográficos, responsabilidades e critérios de revisão periódica do documento.

O **Apêndice B** - *Registro de Rotinas de Backup* - fornece um formulário simplificado

para documentar as rotinas de backup executadas pela serventia, com os campos de informação recomendados e um modelo de preenchimento.

O **Apêndice C** - *Registro de Teste de Restauração de Backup* - oferece um modelo de registro para documentar os testes periódicos de restauração realizados pela serventia, descrevendo o procedimento recomendado e o formato de registro dos resultados.

O **Apêndice D** - *Registro de Usuários Autorizados* - apresenta um formulário para controle dos usuários com acesso aos sistemas da serventia, com orientações sobre como manter esse registro atualizado como parte da gestão de acessos.

O **Apêndice E** - *Registro de Incidentes de Segurança* - disponibiliza um modelo de registro para documentar os incidentes de segurança ocorridos na serventia, incluindo a classificação por grau de gravidade, as obrigações de comunicação às autoridades competentes e exemplos de tipos de incidentes que devem ser registrados.

O **Apêndice F** - *Arquitetura mínima recomendada para serventias* - descreve os princípios e componentes de uma arquitetura de tecnologia da informação adequada às necessidades das serventias, abordando a organização da rede local, a configuração de firewall com prevenção e detecção de intrusão, a segmentação lógica da rede por classe e um exemplo simplificado de arquitetura que pode ser adotado como referência.

2 Como usar este guia

Como utilizar este guia na prática

Para utilizar este guia de forma objetiva, recomenda-se a seguinte sequência de leitura:

a) identificar a classe econômica da serventia;
b) compreender os controles essenciais de segurança apresentados neste documento;
c) implementar gradualmente as medidas prioritárias relacionadas à proteção dos sistemas e dos dados registrais;
d) manter registros e evidências mínimas das práticas adotadas pela serventia.

Essa abordagem permite que as medidas previstas no Provimento nº 213/2026 sejam implementadas de forma gradual, organizada e compatível com a realidade operacional de cada unidade.

Este documento foi estruturado para permitir diferentes formas de consulta, dependendo do objetivo do leitor e do estágio de implementação das medidas de segurança na serventia.

Alguns leitores podem desejar apenas compreender rapidamente as exigências gerais do Provimento nº 213, enquanto outros precisarão utilizar o guia como referência prática para organizar a implementação dos controles de segurança e da documentação mínima exigida.

Por essa razão, o guia foi organizado de forma progressiva, permitindo tanto uma leitura rápida quanto uma consulta mais detalhada para fins de implementação ou de manutenção da conformidade.

De forma geral, recomenda-se a seguinte sequência de utilização do guia:

a) identificar a classe da serventia;
b) compreender os controles essenciais de segurança;
c) implementar gradualmente as medidas prioritárias;

d) manter registros e evidências mínimas das práticas adotadas.

2.1 Leitura em 5 minutos

Para uma visão geral das exigências do Provimento nº 213, recomenda-se iniciar pela leitura do *Checklist rápido de conformidade* apresentado na Seção 9.

Esse checklist resume, de forma direta, as principais medidas de segurança que devem ser observadas pelas serventias do Registro Civil das Pessoas Naturais.

Na prática, a implementação consistente dessas medidas já reduz significativamente os riscos tecnológicos enfrentados pelas serventias e atende aos princípios fundamentais estabelecidos pelo Provimento.

A maior parte dessas medidas pode ser implementada utilizando recursos já disponíveis nos sistemas operacionais, nos equipamentos de rede e nos próprios sistemas registrais utilizados no cotidiano das unidades.

2.2 Leitura para início de implementação

Para as serventias que desejam iniciar ou organizar a implementação das medidas previstas no Provimento nº 213, recomenda-se a leitura das seções que apresentam os controles essenciais de segurança e suas respectivas orientações práticas de implementação.

Essas seções explicam, de forma simplificada, quais medidas devem ser adotadas para reduzir riscos operacionais, proteger os dados registrais e garantir a continuidade do funcionamento dos sistemas utilizados pela serventia.

O guia também apresenta um roteiro prático de implementação, sugerindo uma sequência de ações que pode ser realizada em etapas, permitindo que as medidas sejam adotadas de forma gradual e organizada.

2.3 Leitura para manutenção da conformidade

Após a implementação inicial dos controles de segurança, o guia pode ser utilizado como referência para a manutenção periódica das práticas de segurança adotadas pela serventia.

Nesse contexto, recomenda-se a utilização do checklist de verificação periódica e dos modelos de documentação apresentados nos apêndices do documento.

Esses instrumentos ajudam a registrar rotinas operacionais importantes, como a realização de *backups*, testes de restauração, controle de acessos e registro de incidentes, permitindo demonstrar de forma clara a adoção das práticas de segurança recomendadas pelo Provimento nº 213.

3 Visão geral do Provimento 213

Ideia central do Provimento nº 213

O Provimento nº 213 estabelece padrões mínimos de tecnologia da informação e de segurança da informação para as serventias notariais e de registro.
Seu objetivo é garantir que os sistemas utilizados na atividade registral operem de forma segura, preservando a integridade, a disponibilidade, a autenticidade e a rastreabilidade dos dados e dos atos praticados.
A norma também busca assegurar a continuidade da prestação dos serviços registrais, reduzindo riscos tecnológicos como perda de dados, indisponibilidade de sistemas e acessos indevidos às informações.

O Provimento nº 213 do Conselho Nacional de Justiça estabelece um conjunto de requisitos mínimos relacionados à segurança da informação, à proteção dos dados registrais e à continuidade operacional das serventias do Registro Civil das Pessoas Naturais.

A norma busca garantir que os sistemas utilizados pelas serventias operem de forma segura, confiável e resiliente, reduzindo riscos tecnológicos que possam comprometer o acervo registral ou interromper a prestação dos serviços à sociedade.

Embora o Provimento trate de diversos aspectos técnicos e organizacionais, a maior parte das medidas previstas pode ser implementada por meio de práticas simples e amplamente disponíveis nos sistemas operacionais, na infraestrutura de rede e nas plataformas registrais utilizadas pelas serventias.

3.1 Finalidade regulatória do Provimento

O objetivo central do Provimento nº 213 é estabelecer padrões mínimos de segurança da informação e de gestão tecnológica aplicáveis às serventias do Registro Civil das Pessoas Naturais.

Esses padrões buscam assegurar que os sistemas utilizados na atividade registral estejam protegidos contra riscos como perda de dados, acesso indevido às informações registrais, indisponibilidade de sistemas e falhas operacionais.

A norma também busca fortalecer a confiança institucional no sistema registral brasileiro, garantindo que o acervo digital das serventias seja preservado com níveis adequados de segurança e confiabilidade.

3.2 Riscos que o Provimento busca reduzir

A informatização das serventias ampliou significativamente a superfície de risco associada à operação dos sistemas registrais.

Entre os principais riscos tecnológicos que o Provimento busca reduzir, destacam-se:

- perda de dados registrais por falhas de *hardware* ou *software*;
- indisponibilidade dos sistemas utilizados pelas serventias;
- acesso indevido a informações registrais sensíveis;
- corrupção ou alteração não autorizada de dados;
- interrupção da prestação dos serviços registrais.

A adoção consistente de práticas básicas de segurança da informação, como controle de acessos, criptografia, *backups* e registros de auditoria, contribui significativamente para mitigar esses riscos.

3.3 O que muda na prática

A principal mudança introduzida pelo Provimento nº 213 é a formalização de um conjunto mínimo de práticas de segurança da informação que passam a ser obrigatórias no funcionamento das serventias do Registro Civil.

Na prática, isso significa que a gestão da infraestrutura tecnológica deixa de ser apenas uma atividade operacional e passa a exigir também a adoção de procedimentos básicos de segurança, controle e continuidade dos serviços.

Entre as mudanças mais relevantes no cotidiano das serventias, destacam-se:

- maior controle sobre quem acessa os sistemas e quais operações podem ser realizadas;
- utilização mais consistente de mecanismos de proteção, como criptografia, autenticação forte e registros de auditoria;
- realização sistemática de cópias de segurança dos dados e verificação periódica da possibilidade de restauração;
- manutenção regular de sistemas e equipamentos, incluindo atualizações de segurança;
- definição de procedimentos para lidar com incidentes tecnológicos.

Em termos operacionais, a maioria dessas medidas pode ser implementada utilizando recursos já existentes nos sistemas operacionais, nos equipamentos de rede e nos próprios sistemas registrais.

3.4 O que não muda

A implementação das medidas previstas no Provimento nº 213 não altera a natureza jurídica nem os princípios fundamentais que regem a atividade registral.

As competências legais do oficial de registro civil, os procedimentos registrais previstos na legislação e a validade jurídica dos atos praticados pelas serventias permanecem inalterados.

O Provimento também não exige a adoção de tecnologias complexas ou infraestruturas de alto custo. A norma estabelece objetivos de proteção da informação, permitindo que sua implementação seja realizada por meio de soluções tecnológicas simples e amplamente disponíveis.

Assim, o Provimento nº 213 não altera a essência da atividade registral. Ele apenas estabelece um conjunto mínimo de cuidados tecnológicos necessários para proteger o acervo registral e garantir a continuidade dos serviços prestados pelas serventias.

3.5 Correspondência entre este guia e o Provimento nº 213

Este guia foi elaborado com o objetivo de traduzir, em linguagem prática, os requisitos técnicos e organizacionais estabelecidos pelo Provimento nº 213 do Conselho Nacional de Justiça.

Embora o documento apresente orientações operacionais simplificadas, todas as recomendações aqui descritas correspondem diretamente às obrigações normativas estabelecidas pelo Provimento e por seus anexos.

A tabela a seguir apresenta uma correspondência indicativa entre os principais temas abordados neste guia e os dispositivos normativos do Provimento nº 213.

Tabela 1: Correspondência entre o guia e o Provimento nº 213

Tema tratado no guia	**Seção deste guia**	**Base normativa no Provimento 213**
Classificação da serventia	Seção 4	Art. 2º (classe da serventia) e Anexos
Política de segurança da informação e governança tecnológica	Seção 18 e Apêndice A	Art. 3º e Art. 6º
Gestão de acessos e autenticação	Seção 12	Art. 5º
Proteção de dados pessoais e conformidade com a LGPD	Seção 18	Art. 7º
Arquitetura tecnológica e proteção perimetral	Seção 11 e Apêndice F	Art. 8º e Anexos
Criptografia de dados	Seção 13	Art. 9º
Backup e continuidade operacional	Seção 14	Art. 3º e Anexos
Registro de eventos e auditoria	Seção 15	Art. 10
Proteção contra malware e gestão de vulnerabilidades	Seção 16	Art. 8º e Anexos
Portabilidade e interoperabilidade	Seção 17	Art. 8º
Documentação de conformidade e dossiê técnico	Seções 18 e 20	Art. 4º e Anexos

Esta correspondência tem caráter indicativo e busca facilitar a identificação da relação entre as orientações práticas deste guia e os requisitos normativos do Provimento nº 213.

Em caso de dúvida interpretativa, prevalece sempre o texto normativo do referido Provimento e de seus anexos.

4 Classificação da serventia

Por que as serventias são classificadas

O Provimento nº 213 adota um modelo de proporcionalidade regulatória para a implementação das medidas de segurança da informação nas serventias.
Isso significa que todas as unidades devem observar os mesmos princípios fundamentais de proteção dos sistemas e dos dados registrais, mas o nível de formalização dos controles e a complexidade das soluções tecnológicas podem variar conforme a capacidade econômica da serventia.
Assim, a classificação em classes permite que as exigências de tecnologia da informação sejam aplicadas de forma compatível com a realidade operacional de cada unidade.

O Provimento nº 213 adota um critério de classificação das serventias com base em sua capacidade econômica. Essa classificação permite que as exigências relacionadas à

organização tecnológica e à segurança da informação sejam implementadas de forma proporcional à realidade operacional de cada unidade.

Em termos práticos, isso significa que todas as serventias devem adotar os princípios fundamentais de segurança da informação previstos na norma, porém a forma de implementação desses controles pode variar de acordo com o porte da unidade.

Essa abordagem busca garantir que as exigências regulatórias sejam compatíveis com a diversidade existente entre as serventias brasileiras, evitando a imposição de soluções tecnológicas complexas ou de alto custo para unidades de menor porte.

4.1 Critério econômico de enquadramento

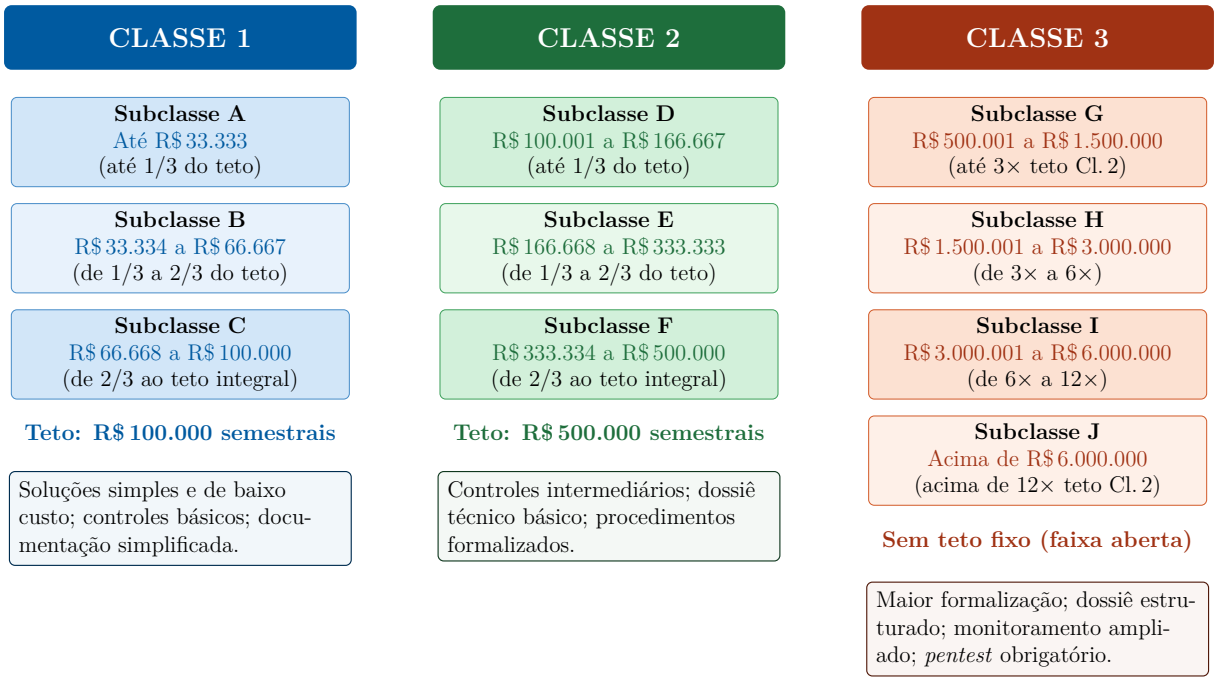
Primeiro passo para usar este guia

Antes de iniciar a implementação das medidas de segurança descritas neste guia, identifique a classe econômica da sua serventia conforme os critérios estabelecidos no Provimento nº 213.
A classe da unidade orientará o nível de formalização dos controles tecnológicos e das práticas de segurança da informação esperadas pela regulamentação.
Nas seções seguintes, este guia apresenta orientações práticas para implementação dessas medidas de forma compatível com a realidade operacional de cada classe de serventia.

O Provimento estabelece a classificação das serventias com base na receita semestral da unidade, permitindo identificar diferentes níveis de maturidade tecnológica e de formalização dos controles de segurança.

A Figura 1 apresenta a classificação econômica completa das serventias prevista no art. 16 do Provimento nº 213, incluindo as dez subclasses e as faixas de arrecadação semestral calculadas com base nos limites estabelecidos pelo normativo.

Figura 1: Classificação econômica das serventias e subclasses (art. 16 do Provimento nº 213).



Os limites de arrecadação são corrigidos anualmente pelo IPCA (art. 16, §2º). As faixas calculadas são aproximações baseadas nos valores vigentes na data de publicação do Provimento; os valores de referência para cada ciclo devem ser conferidos junto à Corregedoria Nacional de Justiça.

Essa classificação não altera os princípios fundamentais de segurança da informação previstos na regulamentação, mas orienta a forma como esses controles podem ser implementados em cada contexto operacional.

4.2 Subclasses e reenquadramento periódico

As subclasses (A a J) são subdivisões internas das três classes principais e possuem, no atual texto do Provimento, uma função primariamente classificatória e prospectiva: identificam com maior precisão o porte econômico da serventia, permitindo que normas futuras da Corregedoria Nacional possam graduar exigências com granularidade mais fina dentro de cada classe.

Para fins de implementação das medidas previstas neste guia, o que importa de imediato é a classe (1, 2 ou 3), não a subclasse isoladamente. Contudo, há três regras dos §§1º a 3º do art. 16 que toda serventia precisa conhecer:

- **Reenquadramento anual** (§1º): o enquadramento deve ser reavaliado todos os anos, com base na arrecadação do semestre imediatamente anterior, produzindo efeitos para o período subsequente. A serventia é responsável por acompanhar sua arrecadação e verificar se houve mudança de faixa;
- **Correção anual pelo IPCA** (§2º): os limites de arrecadação das classes são atualizados a cada ano pelo IPCA, ou por outro índice oficial que venha a substituí-lo. Portanto, os valores nominais constantes deste guia servem como referência para o primeiro ciclo, devendo ser conferidos na Corregedoria Nacional nos ciclos seguintes;
- **Proteção contra variações transitórias** (§3º): a migração de classe ou subclasse não produz efeitos imediatos quando a variação da arrecadação não ultrapassa 10% do limite superior da faixa anterior. Nesses casos, exige-se a confirmação da nova faixa por dois ciclos consecutivos antes de o reenquadramento produzir efeitos. Essa regra protege a serventia contra oscilações pontuais de arrecadação que não reflitam uma mudança estrutural de porte.

Exemplo prático da proteção contra variações transitórias

Uma serventia na Subclasse C (Classe 1, teto R$ 100.000) registra arrecadação semestral de R$ 103.000 - uma variação de apenas 3% acima do limite. Como esse valor não supera os 10% do teto da faixa anterior (que seriam R$ 10.000 acima do teto, ou seja, R$ 110.000), o reenquadramento para a Classe 2 não se produz automaticamente: a serventia precisará confirmar essa nova arrecadação em dois ciclos semestrais consecutivos para que a mudança de classe se efetive. Enquanto isso, permanece obrigada apenas pelas exigências da Classe 1.

4.3 Leitura prática por classe

Em serventias de menor porte, especialmente aquelas classificadas como Classe 1, recomenda-se priorizar soluções tecnológicas simples e amplamente disponíveis, como re-

cursos nativos dos sistemas operacionais e ferramentas básicas de proteção de rede e de armazenamento de dados.

Nas serventias classificadas como Classe 2, espera-se uma maior formalização dos procedimentos de segurança, incluindo organização mais estruturada das rotinas de *backup*, controle de acessos e documentação mínima das práticas adotadas.

Já nas serventias classificadas como Classe 3, a norma pressupõe maior maturidade organizacional e tecnológica, com níveis mais elevados de monitoramento, formalização de procedimentos e gestão da infraestrutura tecnológica.

4.4 Impacto do enquadramento na implementação

Independentemente da classe da serventia, os princípios fundamentais de segurança da informação previstos no Provimento nº 213 permanecem os mesmos.

Todas as unidades devem adotar práticas básicas de proteção dos sistemas e dos dados registrais, incluindo controle de acessos, criptografia, realização de *backups* e manutenção de registros de auditoria.

O que varia entre as classes é principalmente o grau de formalização dos processos e o nível de sofisticação das soluções tecnológicas utilizadas.

Assim, mesmo as serventias de menor porte podem alcançar níveis adequados de conformidade adotando práticas simples, consistentes e bem documentadas, utilizando recursos já disponíveis na maioria dos sistemas operacionais e plataformas tecnológicas utilizadas no ambiente registral.

5 Prazos de implementação

Atenção: os prazos são normativos e vinculantes

O Provimento nº 213 estabelece prazos obrigatórios para a implementação das medidas de segurança da informação pelas serventias.
O não cumprimento injustificado desses prazos pode ensejar procedimento administrativo disciplinar, conforme o art. 24 do Provimento.
Os prazos começam a contar da data de publicação do Provimento: 23 de fevereiro de 2026.

O Provimento nº 213 organiza a implementação de suas exigências em cinco etapas sequenciais e cumulativas, definidas no Anexo IV. Cada etapa pressupõe o cumprimento integral da etapa anterior e deve ser declarada no Sistema Justiça Aberta pelo titular da delegação.

A implementação segue dois horizontes de prazo, ambos contados da data de entrada em vigor do Provimento.

5.1 Prazo para as etapas iniciais obrigatórias (Etapas 1 e 2)

As duas primeiras etapas, que cobrem governança, conformidade legal, infraestrutura básica e continuidade operacional, devem ser concluídas nos seguintes prazos:

Tabela 2: Prazos para conclusão das Etapas 1 e 2 (arts. 20 do Provimento nº 213).

Classe da serventia	Prazo (dias corridos)	Data-limite aproximada
Classe 3	90 dias	24 de maio de 2026
Classe 2	150 dias	22 de julho de 2026
Classe 1	210 dias	21 de setembro de 2026

O que é exigido nas Etapas 1 e 2?
Etapa 1 - Governança e conformidade legal (Anexo IV, itens 1.1 a 1.9): designação formal de responsáveis (segurança da informação, controlador de dados e DPO quando aplicável); aprovação e publicização interna da Política de Segurança da Informação; implementação de autenticação individualizada e multifator (MFA) para acessos administrativos; registro das operações de tratamento de dados pessoais (art. 7º, §1º); inventário completo de ativos tecnológicos, integrações, certificados digitais, softwares e contratos; regularização do licenciamento de software e revisão dos contratos com fornecedores, assegurando cláusulas expressas de confidencialidade, reversibilidade, portabilidade integral do acervo em formato interoperável, cooperação em transição, gestão de incidentes e conformidade com a Lei Geral de Proteção de Dados (LGPD); definição de procedimento de comunicação de incidentes críticos à Corregedoria competente no prazo máximo de 72 horas, com meta de diligência reforçada de 24 horas (Anexo IV, itens 1.5 e 1.6); e produção de declaração formal de conclusão da Etapa 1, registrada no Sistema Justiça Aberta.
Etapa 2 - Infraestrutura e continuidade operacional (Anexo IV, itens 2.1 a 2.9): implementação de *nobreak* (SAI/UPS) com autonomia mínima de 30 minutos; estabelecimento de plano de contingência energética compatível com a classe; adequação do ambiente físico com controle de acesso restrito e proteção contra incêndio, inundações e variações térmicas; garantia de conectividade compatível com a classe (mínimo 2 Mbps para Classe 1, 10 Mbps para Classe 2 e 50 Mbps para Classe 3), com roteador, *switch* e, quando necessário, múltiplos *links*; formalização do Plano de Continuidade de Negócios (PCN) e do Plano de Recuperação de Desastres (PRD), com identificação de riscos, medidas de mitigação e definição expressa de RTO e RPO compatíveis com a classe; proteção básica de *endpoint* (antivírus/antimalware) em todas as estações e servidores; e formalização de documento técnico simplificado da arquitetura tecnológica adotada, contendo topologia básica de rede, ambientes utilizados, fluxos de dados críticos, localização dos *backups*, integrações externas relevantes e mecanismos de alta disponibilidade ou redundância. A declaração de conclusão das Etapas 1 e 2 deve ser registrada no Sistema Justiça Aberta.

5.2 Prazo para implementação integral (Etapas 1 a 5)

A conclusão de todas as cinco etapas do Provimento deve ocorrer nos seguintes prazos máximos, contados também da data de publicação:

Tabela 3: Prazos máximos para implementação integral de todas as etapas (art. 23 do Provimento nº 213).

Classe da serventia	Prazo máximo	Data-limite aproximada
Classe 3	24 meses	fevereiro de 2028
Classe 2	30 meses	agosto de 2028
Classe 1	36 meses	fevereiro de 2029

Etapa 3 - Proteção do acervo digital (Anexo IV, itens 3.1 a 3.9): criptografia para dados em trânsito (TLS 1.2+), em repouso (AES-256) e nos *backups* externos; gestão formal de chaves criptográficas (inventário, segregação de custódia, rotação, registro de operações e revisão periódica dos padrões adotados); *firewall stateful* com IPS/IDS e segmentação lógica de rede (VLANs para Classes 2 e 3; medida idônea simplificada para Classe 1); rotinas automatizadas de *backup* completo e incremental com periodicidades por classe (máx. 24 h, 48 h e 72 h, respectivamente), em dois ambientes tecnicamente independentes; monitoramento automático das rotinas de *backup* com alertas e registro formal de falhas; proteção anti-*ransomware* por WORM, versionamento bloqueado ou isolamento lógico; uso de SGBD com integridade transacional e *logs* ativos; e implantação de trilhas de auditoria técnicas imutáveis, com identificação inequívoca do usuário, data/hora e sincronização por fonte confiável (NTP), integradas às rotinas de *backup* e recuperação.
Etapa 4 - Monitoramento, auditoria e validação de controles (Anexo IV, itens 4.1 a 4.9): emissão de relatório de conformidade das trilhas de auditoria (imutabilidade, identificação, sincronização temporal, retenção mínima e integração com *backup* comprovadas); rotina documentada de atualização periódica de sistemas e aplicações; gestão formal de vulnerabilidades (críticas: até 30 dias; exploração ativa: até 72 horas; com registro formal das providências); simulação anual de desastre para validação do PCN/PRD; testes documentados de restauração de *backup* (semestrais para Classe 3, anuais para Classes 1 e 2); avaliações técnicas periódicas de segurança; teste de intrusão (*pentest*) a cada 2 anos para Classe 3 (ver hipóteses de dispensa na Seção 16.7); e documentação de análise de causa raiz e lições aprendidas para todos os incidentes.
Etapa 5 - Interoperabilidade e governança evolutiva (Anexo IV, itens 5.1 a 5.7): integração com plataformas eletrônicas de fiscalização; adoção de padrões abertos e neutralidade tecnológica; capacitação periódica da equipe com registro formal; manutenção de registros auditáveis por mínimo de 5 anos; formalização de plano de reversibilidade e portabilidade com simulação documentada de extração integral do acervo (a cada 24, 30 ou 36 meses conforme a classe); e revisão formal da Política de Segurança sempre que houver alteração normativa relevante ou evolução tecnológica.

5.3 Prorrogação excepcional

O art. 21 do Provimento admite, em caráter excepcional, a prorrogação dos prazos das Etapas 1 e 2 por até 90 dias adicionais, mediante decisão fundamentada da Corregedoria do Tribunal de Justiça competente.

Para obter a prorrogação, a serventia deve:

- apresentar plano formal de adequação com cronograma definido e indicação de responsáveis;

- implementar imediatamente medidas compensatórias mínimas de redução de risco, conforme orientação técnica da Corregedoria.

Para as serventias da Classe 1, o requerimento de prorrogação está sujeito a análise simplificada pela Corregedoria competente.

5.4 Declaração no Sistema Justiça Aberta

O art. 17 do Provimento exige que cada serventia declare, em campo próprio do Sistema Justiça Aberta, o cumprimento de cada etapa concluída.

Essa declaração deve ser:

- renovada anualmente;
- acompanhada de síntese do dossiê técnico com evidências mínimas de conformidade;
- firmada pelo titular da delegação, interino ou interventor.

Atenção: declaração falsa

O art. 17, §2º do Provimento estabelece que a declaração falsa, objetivamente verificada em inspeções ou correições, sujeita o responsável às penalidades previstas em lei.

6 O que cada classe precisa implementar

Recomendação prática

Passo 1: identifique a classe econômica da sua serventia, conforme os critérios estabelecidos pelo Provimento nº 213.
Passo 2: consulte nesta seção o nível de implementação esperado para a sua classe.
Passo 3: utilize as seções seguintes como orientação prática para implementar os controles de segurança e organizar a documentação mínima de conformidade.

O Provimento nº 213 adota o princípio da proporcionalidade regulatória, estabelecendo que as exigências relacionadas à tecnologia da informação e à segurança dos sistemas devem considerar a realidade operacional das diferentes serventias.

Embora os princípios fundamentais de segurança da informação sejam comuns a todas as unidades, o nível de formalização, de monitoramento e de complexidade das soluções tecnológicas pode variar de acordo com a classe econômica da serventia.

Esta seção apresenta uma interpretação prática dessa proporcionalidade, indicando como as medidas descritas neste guia podem ser aplicadas em cada classe de serventia.

6.1 Classe 1 - Implementação essencial

As serventias classificadas como Classe 1 geralmente possuem estrutura operacional reduzida e recursos tecnológicos limitados. Nesses casos, o objetivo principal é garantir a adoção consistente das medidas essenciais de proteção dos sistemas e dos dados registrais.

Recomenda-se priorizar soluções simples e amplamente disponíveis, preferencialmente utilizando recursos já presentes nos sistemas operacionais, nos equipamentos de rede e nos próprios sistemas registrais utilizados pela serventia.

Entre as medidas prioritárias para serventias de Classe 1 destacam-se:

- designação formal de responsável pela segurança da informação e pelo tratamento de dados pessoais;
- aprovação e divulgação interna da Política de Segurança da Informação, com os elementos mínimos do Anexo III;
- uso de contas individualizadas de acesso aos sistemas, vedadas credenciais compartilhadas;
- autenticação multifator (MFA) obrigatória para acessos administrativos e a sistemas críticos;
- inventário completo de ativos tecnológicos, softwares e contratos com fornecedores;
- regularização do licenciamento de software e revisão dos contratos com fornecedores, assegurando cláusulas de confidencialidade, reversibilidade e portabilidade do acervo;
- procedimento documentado de comunicação de incidentes críticos à Corregedoria competente no prazo máximo de 72 horas (meta de diligência: 24 horas);
- utilização de nobreak (SAI/UPS) com autonomia mínima de 30 minutos e plano de contingência energética;
- ambiente físico com controle de acesso restrito e proteção básica contra incêndio, inundações e variações térmicas;
- conectividade mínima de 2 Mbps compatível com os sistemas utilizados, com roteador e *switch*;
- formalização do PCN e do PRD com RTO e RPO de até 24 horas;
- proteção de *endpoint* (antivírus/antimalware) em todas as estações;
- documento simplificado da arquitetura tecnológica adotada;
- manutenção de sistemas operacionais com suporte vigente (sem componentes *End of Life*);
- realização de *backups* automáticos dos dados registrais com armazenamento em dois ambientes independentes;
- realização periódica de testes de restauração de *backup*;
- manutenção de registros básicos de atividades dos sistemas (*logs*), com retenção mínima de 5 anos.

Para serventias dessa classe, a documentação de conformidade pode ser mantida em formato simplificado, conforme os modelos apresentados nos apêndices deste guia.

6.2 Classe 2 - Implementação intermediária

As serventias classificadas como Classe 2 normalmente possuem maior volume de operações e infraestrutura tecnológica mais estruturada.

Nesses casos, espera-se uma maior formalização das práticas de segurança da informação e da gestão da infraestrutura tecnológica.

Além das medidas previstas para a Classe 1, as serventias de Classe 2 devem adotar os seguintes requisitos adicionais:

- conectividade mínima de 10 Mbps com roteador, *switch* e, quando necessário, múltiplos *links*;
- PCN e PRD com RPO máximo de 12 horas e RTO máximo de 24 horas, acompanhados de dossiê técnico básico;
- documento técnico formalizado da arquitetura tecnológica adotada (topologia, am-

bientes, fluxos, *backups*, integrações e mecanismos de redundância);
- *firewall stateful* com IPS/IDS e segmentação lógica formal da rede local mediante VLANs ou solução tecnicamente equivalente, separando o ambiente administrativo dos dispositivos de atendimento ao público. Este requisito é obrigatório (art. 8º, inciso VII, alínea a; ver Seção F.3);
- proteção perimetral com inspeção ativa de tráfego, geração e retenção de registros auditáveis e capacidade de detecção de ameaças (Anexo II, §4º);
- *backup* completo com intervalo máximo de 48 horas mais *backup* incremental compatível com RPO de 12 horas;
- gestão formal de chaves criptográficas com inventário, segregação de custódia, controle de acesso, rotação periódica e registro de operações;
- trilhas de auditoria imutáveis com identificação do usuário, data/hora, sincronização por fonte confiável (NTP) e retenção mínima de 5 anos (nível Essencial ou Intermediário);
- testes anuais documentados de restauração de *backup* e simulação anual do PCN/PRD;
- dossiê técnico com mecanismo de verificação de integridade (*hash* dos arquivos assinado digitalmente pelo responsável técnico, Anexo IV, item IV).

Essas medidas contribuem para aumentar a rastreabilidade das operações realizadas nos sistemas e facilitar a verificação da conformidade com os requisitos do Provimento nº 213.

6.3 Classe 3 - Implementação ampliada

As serventias classificadas como Classe 3 possuem maior capacidade econômica e, em geral, operam infraestruturas tecnológicas mais complexas e com maior volume de dados registrais.

Por essa razão, espera-se nessas unidades um nível mais elevado de maturidade na gestão da segurança da informação e da continuidade operacional.

Além das medidas previstas para as Classes 1 e 2, as serventias de Classe 3 devem adotar os seguintes requisitos adicionais:

- conectividade mínima de 50 Mbps com roteador, *switch* e múltiplos *links*;
- PCN e PRD com RPO máximo de 4 horas e RTO máximo de 8 horas, com mecanismos de alta disponibilidade (HA) ou tolerância a falhas e dossiê técnico estruturado;
- proteção perimetral com inspeção ativa de tráfego em nível de rede, geração e retenção de registros auditáveis, e capacidade de detecção e bloqueio de ameaças avançadas, inclusive por análise comportamental (Anexo II, §4º, incisos I a III);
- *firewall stateful* com IPS/IDS e segmentação formal obrigatória por VLANs ou equivalente;
- *backup* completo com intervalo máximo de 24 horas mais *backup* incremental compatível com RPO de 4 horas, em dois ambientes com redundância geográfica;
- SGBD com integridade transacional e *logs* ativos;
- gestão formal de chaves criptográficas com inventário, segregação de custódia, controle de acesso, rotação periódica, registro de operações e revisão periódica dos padrões adotados;
- trilhas de auditoria imutáveis com identificação inequívoca do usuário, data/hora, sincronização NTP e retenção mínima de 5 anos (nível Intermediário ou superior);
- testes **semestrais** documentados de restauração de *backup* e simulação anual do

PCN/PRD;
- gestão formal e documentada de vulnerabilidades, com tratamento de vulnerabilidades críticas em até 30 dias e de exploração ativa em até 72 horas;
- avaliações técnicas periódicas de segurança;
- documentação de análise de causa raiz e lições aprendidas para todos os incidentes;
- teste de intrusão (*pentest*) ou metodologia equivalente a cada 2 anos ou sempre que houver alteração relevante de infraestrutura. Ver hipóteses de dispensa para ambientes SaaS na Seção 16.7;
- capacitação periódica da equipe com registro formal;
- plano formal de reversibilidade e portabilidade com simulação documentada de extração integral do acervo a cada 24 meses;
- dossiê técnico com *hash* dos arquivos e assinatura digital do responsável técnico, guardado em repositório com controle de acesso e registro auditável de alterações (Anexo IV, item IV).

Essas medidas contribuem para aumentar o nível de confiabilidade e de resiliência dos sistemas utilizados pela serventia.

6.4 Resumo comparativo por classe

A Tabela 4 apresenta um resumo simplificado das expectativas de implementação dos principais controles de segurança para cada classe de serventia.

Tabela 4: Nível esperado de implementação dos controles por classe de serventia.

Controle ou prática	Classe 1	Classe 2	Classe 3
Proteção elétrica por nobreak	Obrigatório	Obrigatório	Obrigatório
Contas individualizadas de acesso	Obrigatório	Obrigatório	Obrigatório
Autenticação multifator (MFA)	Obrigatório para acessos administrativos e críticos	Obrigatório para acessos administrativos e críticos	Obrigatório para acessos administrativos e críticos
Criptografia de dados	Obrigatório	Obrigatório	Obrigatório
Backup automático	Obrigatório	Obrigatório	Obrigatório
Teste de restauração de *backup*	Periódico	Periódico e documentado	Periódico e documentado
RPO máximo admissível	24 horas	12 horas	4 horas
RTO máximo admissível	24 horas	24 horas	8 horas
Registros de eventos (logs)	Nível essencial	Nível essencial ou intermediário	Nível intermediário ou superior
Retenção mínima de *logs*	5 anos	5 anos	5 anos
Documentação de conformidade	Relatório simplificado	Dossiê técnico básico	Dossiê técnico estruturado
Firewall stateful com IPS/IDS	obrigatório	obrigatório	obrigatório
Segmentação lógica de rede	Medida idônea simplificada (impedir comunicação irrestrita entre rede admin e rede pública)	VLANs ou equivalente formal	VLANs ou equivalente formal
Teste de intrusão (*pentest*)	Não exigido	Não exigido	obrigatório a cada 2 anos (dispensável em SaaS integral)

Essa tabela não substitui a leitura detalhada das seções técnicas do guia, mas serve como referência rápida para compreender o nível de organização tecnológica esperado em cada classe de serventia.

7 Soluções centralizadas e papel do ON-RCPN

Ponto central do Provimento nº 213

O Provimento nº 213 admite que parte relevante dos controles técnicos de segurança da informação seja implementada de forma **centralizada**, por meio de plataforma nacional estruturada, solução coletiva ou ambiente tecnológico mantido por entidade representativa e/ou por Operador Nacional regularmente instituído (art. 13, §§4º a 7º).
Essa possibilidade é especialmente relevante para as serventias do Registro Civil das Pessoas Naturais, pois permite racionalizar custos, padronizar controles estruturais e reduzir a necessidade de contratação individual de soluções complexas, sem afastar a responsabilidade local do delegatário.

7.1 O que significa implementação centralizada

A implementação centralizada ocorre quando determinados controles técnicos previstos no Provimento não são implantados isoladamente por cada serventia, mas sim por uma infraestrutura comum mantida por entidade apta a atender múltiplas unidades usuárias.

Nos termos do art. 13, §4º, isso pode ocorrer por meio de:

- plataforma nacional estruturada;
- solução coletiva;
- ambiente tecnológico mantido por entidade representativa de notários e/ou registradores;
- ambiente tecnológico mantido por Operador Nacional regularmente instituído.

Nesses casos, admite-se a **centralização material da implementação dos controles técnicos**, desde que a conformidade seja demonstrável, formal e auditável.

7.2 Qual é o papel do ON-RCPN

No âmbito do Registro Civil das Pessoas Naturais, o ON-RCPN pode exercer papel estruturante na disponibilização de soluções nacionais comuns, capazes de atender simultaneamente a múltiplas serventias.

Esse papel pode abranger, entre outros exemplos:

- serviços nacionais de autenticação e controle de identidade digital, como o IdRC;
- componentes estruturais de segurança, autenticação, integração e rastreabilidade;
- documentação técnica coletiva de conformidade;
- relatórios técnicos auditáveis referentes à infraestrutura comum;
- padronização de requisitos mínimos para integração segura das serventias usuárias.

A existência de solução estruturante mantida pelo ON-RCPN reduz a carga individual de implementação de controles complexos pelas serventias, principalmente quando esses controles dizem respeito à infraestrutura comum e não a procedimentos exclusivamente locais.

Um exemplo concreto dessa lógica de implementação centralizada é o IdRC, serviço de autenticação no âmbito do Registro Civil.

O IdRC é exemplo de componente de autenticação disponibilizado em lógica nacional

centralizada, sem prejuízo dos controles locais de acesso e governança que permanecem sob responsabilidade da serventia.

7.3 O que pode ser comprovado de forma coletiva

De acordo com o art. 13, §5º, a implementação centralizada não dispensa a serventia do dever de conformidade, mas autoriza que a comprovação de requisitos estruturais seja realizada por meio de certificação, relatório ou documentação coletiva emitida pela entidade mantenedora.

Na prática, podem ser objeto de comprovação coletiva, quando efetivamente centralizados:

- controles estruturais da plataforma nacional;
- requisitos técnicos da infraestrutura comum;
- mecanismos de autenticação centralizada;
- testes, validações ou avaliações técnicas do ambiente compartilhado;
- evidências de segurança referentes ao núcleo tecnológico mantido de forma central.

Essa lógica também é reforçada pelo art. 13, §7º, segundo o qual a validação técnica estrutural, realizada uma única vez por meio de relatório técnico abrangente e auditável, pode produzir efeito para todas as serventias usuárias quanto aos requisitos estruturais.

7.4 O que continua sendo responsabilidade da serventia

A centralização de controles técnicos não transfere a responsabilidade funcional da serventia.

Permanece pessoal e indelegável a responsabilidade do delegatário, interino ou interventor pelo cumprimento integral do Provimento (art. 13, §3º; art. 14, parágrafo único).

Assim, continuam sob responsabilidade local da serventia, entre outros:

- governança local da segurança da informação;
- controle de acessos internos;
- gestão de perfis e credenciais dos usuários da unidade;
- resposta a incidentes ocorridos no ambiente local;
- integração da solução centralizada aos planos de continuidade e recuperação da serventia;
- observância da legislação de proteção de dados pessoais no contexto das operações locais;
- manutenção das evidências mínimas no dossiê técnico ou relatório simplificado.

Em outras palavras, a serventia pode se beneficiar de uma infraestrutura nacional ou coletiva, mas não pode deixar de exercer supervisão, governança e controle operacional sobre seu próprio ambiente.

7.5 Evidências mínimas que a serventia deve manter

Quando utilizar solução centralizada, coletiva, compartilhada ou estruturalmente mantida pelo ON-RCPN ou por outra entidade apta, a serventia deve manter em seu dossiê técnico evidências atualizadas de:

a) adesão formal à plataforma ou solução utilizada;
b) identificação objetiva dos controles implementados centralmente;
c) compatibilidade da solução com a classe da serventia;
d) documentação coletiva, certificação ou relatório técnico emitido pela entidade mantenedora;
e) delimitação dos controles que permanecem sob responsabilidade local;
f) medidas locais efetivamente adotadas pela serventia.

Essas evidências são importantes para demonstrar, em eventual fiscalização correicional, que a serventia não deixou de cumprir o Provimento, mas apenas adotou modelo autorizado de implementação centralizada.

7.6 Contratação e requisitos contratuais mínimos

Sempre que a solução centralizada ou coletiva envolver contratação de terceiros, individual ou coletiva, deverão constar cláusulas mínimas de:

- confidencialidade;
- reversibilidade;
- portabilidade de dados;
- gestão de incidentes;
- observância integral da LGPD.

Esses elementos decorrem expressamente do art. 13, §6º, e devem ser observados mesmo quando a serventia participa de arranjo coletivo ou utiliza plataforma nacional comum.

7.7 Interpretação prática para as serventias do RCPN

Para as serventias do Registro Civil, a principal consequência prática dessa disciplina é a seguinte: nem todo controle técnico precisa ser implementado isoladamente em cada unidade, desde que exista solução centralizada válida, auditável e compatível com o Provimento.

Isso é particularmente importante para serventias pequenas, que nem sempre dispõem de equipe técnica própria ou escala econômica para contratação individual de soluções sofisticadas.

Nesses casos, o uso de infraestrutura nacional ou coletiva pode ser a forma mais eficiente, proporcional e juridicamente adequada de alcançar conformidade, desde que a serventia preserve sua governança local e mantenha documentação comprobatória atualizada.

8 Roteiro visual de implementação por classe

Como utilizar os roteiros visuais

Os roteiros apresentados nesta seção traduzem as cinco etapas do Anexo IV do Provimento nº 213 em fluxos visuais organizados por classe de serventia.
Cada bloco do roteiro corresponde a um item específico do Anexo IV, na mesma ordem sequencial estabelecida pelo Provimento. O número à esquerda de cada bloco (por exemplo, **1.3** ou **3.2**) identifica exatamente o item normativo correspondente, permitindo consulta direta ao texto do Provimento em caso de dúvida.
Esses roteiros podem ser utilizados como painel de acompanhamento do processo de conformidade: à medida que cada item é concluído, a serventia pode registrar o progresso e identificar rapidamente quais atividades ainda precisam ser realizadas.

O Provimento nº 213 organiza a implementação de seus requisitos em cinco etapas sequenciais e cumulativas, definidas no Anexo IV. Cada etapa pressupõe o cumprimento integral da etapa anterior, e sua conclusão deve ser declarada no Sistema Justiça Aberta pelo titular da delegação (art. 17).

Para facilitar a visualização desse processo, esta seção apresenta roteiros gráficos de implementação, organizados por classe de serventia e agrupados em duas figuras para cada classe:

- a primeira figura reúne as **Etapas 1 e 2**, que correspondem à implementação inicial obrigatória e devem ser concluídas nos prazos mais curtos estabelecidos pelo art. 20 do Provimento (ver Seção 5);
- a segunda figura apresenta as **Etapas 3 a 5**, que completam a implementação integral dos requisitos do Provimento e possuem prazos máximos mais longos, definidos no art. 23.

8.1 Como ler os roteiros

Cada bloco nos roteiros contém três informações:

a) o **número do item** do Anexo IV do Provimento (por exemplo, **1.3** ou **3.2**), que permite localizar o requisito normativo correspondente no texto oficial;
b) uma **descrição resumida** da atividade a ser realizada;
c) uma **referência à seção deste guia** (indicada pelo símbolo §) onde o tema é explicado com maior detalhe e com orientações práticas de implementação.

As **setas contínuas** indicam a sequência de execução dentro de cada etapa. As **setas tracejadas** indicam a transição entre etapas, reforçando que a etapa seguinte só pode ser formalmente declarada após o cumprimento integral da anterior.

Nas figuras das Classes 2 e 3, os blocos com **borda espessa** e marcação **[Cl.2+]** ou **[Cl.3]** identificam controles que são exclusivos ou possuem exigências reforçadas para a respectiva classe, como parâmetros mais rigorosos de RPO/RTO, segmentação formal de rede por VLANs ou realização obrigatória de *pentest*.

Os roteiros da Classe 1 não possuem marcação de borda espessa, pois representam o conjunto base de requisitos aplicável a todas as serventias.

8.2 Classe 1 – Roteiro de implementação

As Figuras 2 e 3 apresentam o roteiro completo de implementação para as serventias da **Classe 1**.

A Classe 1 corresponde às serventias de menor porte econômico. Embora os princípios de segurança sejam os mesmos para todas as classes, a Classe 1 dispõe de prazos mais longos para implementação e admite soluções simplificadas em diversos requisitos, como documentação em formato de relatório simplificado, segmentação de rede por medida idônea (sem obrigatoriedade de VLANs formais) e dispensa de *pentest*.

8.2.1 Etapas 1 e 2 – Governança, infraestrutura e continuidade

A Figura 2 apresenta as duas primeiras etapas do processo de implementação, que devem ser concluídas até 210 dias após a publicação do Provimento.

A **Etapa 1** (coluna esquerda) concentra as atividades de organização institucional: designação formal de responsáveis, aprovação da Política de Segurança da Informação, implantação de autenticação individualizada com MFA para acessos administrativos, registro de tratamento de dados pessoais, definição de procedimentos para comunicação de incidentes, inventário de ativos e revisão de contratos com fornecedores. Ao final, a serventia produz a declaração de conclusão da Etapa 1 no Sistema Justiça Aberta.

A **Etapa 2** (coluna direita) trata da base material que sustenta os sistemas: infraestrutura elétrica com nobreak, plano de contingência energética, adequação do ambiente físico, conectividade compatível com a classe, formalização do PCN e do PRD com RPO e RTO de 24 horas, garantia de equipamentos e suporte técnico, proteção básica de *endpoint*, e formalização do documento de arquitetura tecnológica. A etapa encerra-se com a declaração de conclusão no Sistema Justiça Aberta.

8.2.2 Etapas 3 a 5 – Proteção, monitoramento e governança evolutiva

A Figura 3 apresenta as três etapas finais, que completam a implementação integral do Provimento.

A **Etapa 3** (coluna esquerda) consolida a proteção técnica do acervo digital: criptografia completa (dados em trânsito, em repouso e nos *backups*) com gestão formal de chaves; rotinas automatizadas de *backup* completo e incremental em dois ambientes independentes; monitoramento automático das rotinas de cópia; implantação de *firewall stateful* com IPS/IDS e segmentação lógica de rede; proteção de *endpoint*; SGBD com integridade transacional; mecanismos de tolerância a falhas; e trilhas de auditoria imutáveis.

A **Etapa 4** (coluna central) valida empiricamente os controles implementados: relatório de conformidade das trilhas de auditoria; rotina documentada de atualização de sistemas; gestão formal de vulnerabilidades com prazos definidos; simulação anual de desastre; testes anuais de restauração de *backup*; avaliações técnicas de segurança; e documentação de análise de causa raiz para todos os incidentes. O *pentest* não é exigido para a Classe 1.

A **Etapa 5** (coluna direita) integra a serventia ao ecossistema de fiscalização e institucionaliza a governança contínua: interoperabilidade com plataformas de fiscalização; adoção de padrões abertos; capacitação periódica da equipe; revisão formal da Política de

Figura 2: Roteiro de implementação – **Classe 1**, Etapas 1 e 2. Ver Seções 5, 4.2, 14, F.3.

Segurança; manutenção de registros auditáveis por 5 anos; plano de reversibilidade com simulação de extração do acervo a cada 36 meses; e declaração de conclusão integral.

8.3 Classe 2 – Roteiro de implementação

As Figuras 4 e 5 apresentam o roteiro completo de implementação para as serventias da **Classe 2** (arrecadação semestral entre R$ 100.001 e R$ 500.000).

Em relação à Classe 1, a Classe 2 possui prazos mais curtos, parâmetros mais exigentes de RPO (12 horas) e RTO (24 horas), e requisitos adicionais como segmentação formal de rede por VLANs, dossiê técnico básico com verificação de integridade e documento de arquitetura mais detalhado.

Os blocos com **borda espessa** e marcação **[Cl.2+]** identificam os controles que possuem exigências reforçadas ou exclusivas para a Classe 2 em comparação com a Classe 1.

8.3.1 Etapas 1 e 2 – Governança, infraestrutura e continuidade

A Figura 4 apresenta as duas primeiras etapas, que devem ser concluídas em no máximo 150 dias após a publicação do Provimento.

A estrutura das atividades é a mesma da Classe 1 (itens 1.1 a 1.9 e itens 2.1 a 2.9 do Anexo IV), porém com parâmetros diferenciados nos itens marcados com borda espessa: conectividade mínima de 10 Mbps (item 2.4), PCN/PRD com RPO de 12 horas e RTO de 24 horas acompanhado de dossiê técnico básico (item 2.5), e documento de arquitetura tecnológica formalizado com maior detalhamento (item 2.8).

8.3.2 Etapas 3 a 5 – Proteção, monitoramento e governança evolutiva

A Figura 5 apresenta as etapas finais.

Em relação à Classe 1, os controles reforçados para a Classe 2 incluem: *backup* completo a cada 48 horas com RPO de 12 horas (item 3.2); segmentação formal de rede por VLANs (item 3.4); trilhas de auditoria no nível Essencial com requisitos de integridade (item 3.8); testes anuais documentados de restauração (item 4.5); e simulação de extração do acervo a cada 30 meses (item 5.6). O *pentest* não é exigido para a Classe 2.

8.4 Classe 3 – Roteiro de implementação

As Figuras 6 e 7 apresentam o roteiro completo de implementação para as serventias da **Classe 3** (arrecadação semestral acima de R$ 500.000).

A Classe 3 possui os prazos mais curtos de implementação e os requisitos mais exigentes do Provimento. Os parâmetros de RPO (4 horas) e RTO (8 horas) exigem mecanismos de alta disponibilidade e *backups* incrementais frequentes. A segmentação de rede por VLANs é obrigatória, as trilhas de auditoria devem atingir o nível Intermediário, e o *pentest* é obrigatório a cada dois anos.

Os blocos com **borda espessa** e marcação **[Cl.3]** são numerosos nesta classe, refletindo o nível mais elevado de exigência normativa.

Figura 3: Roteiro de implementação – **Classe 1**, Etapas 3 a 5. Ver Seções 14, F.3, 15, 16 e 18.

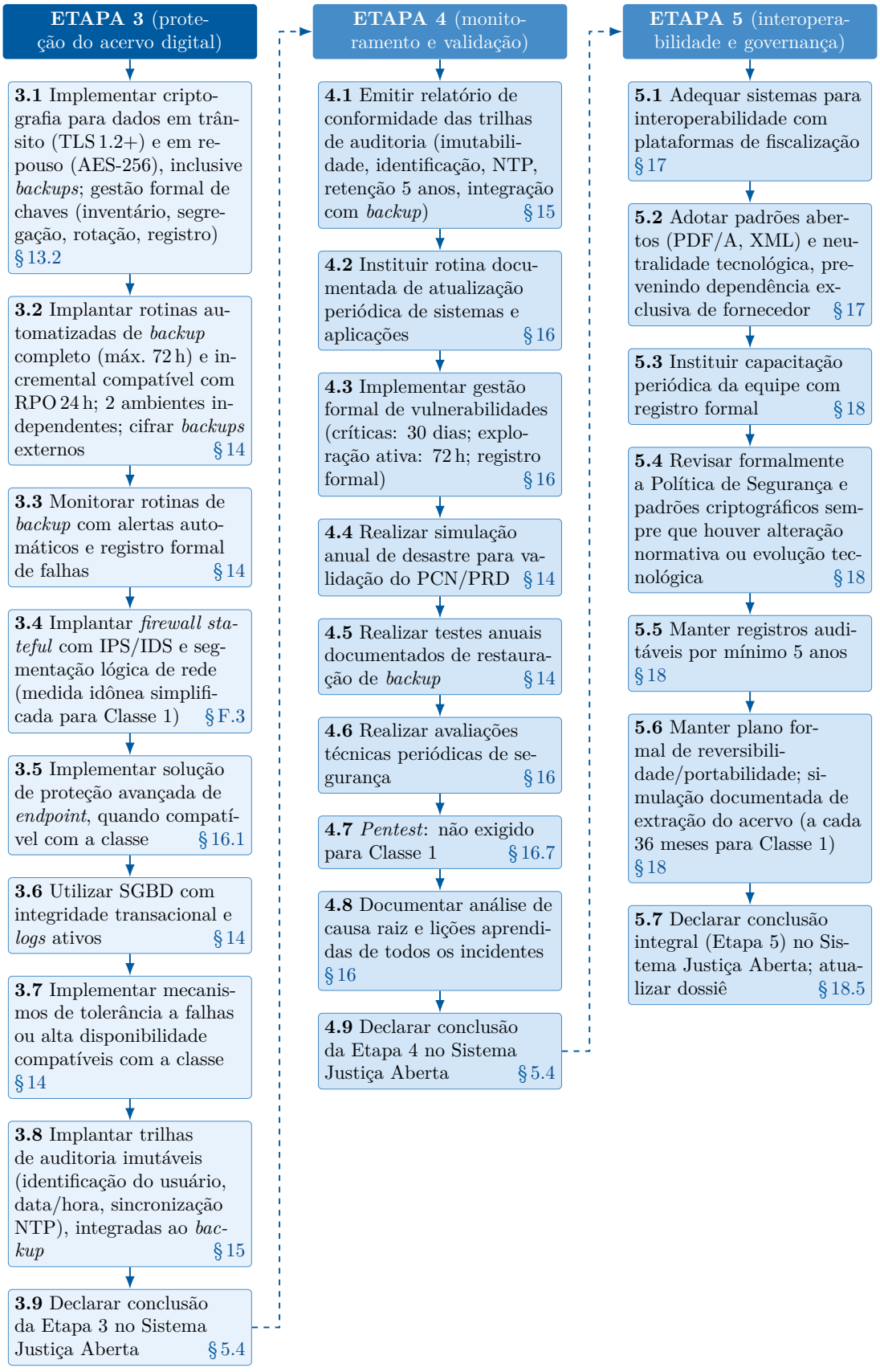
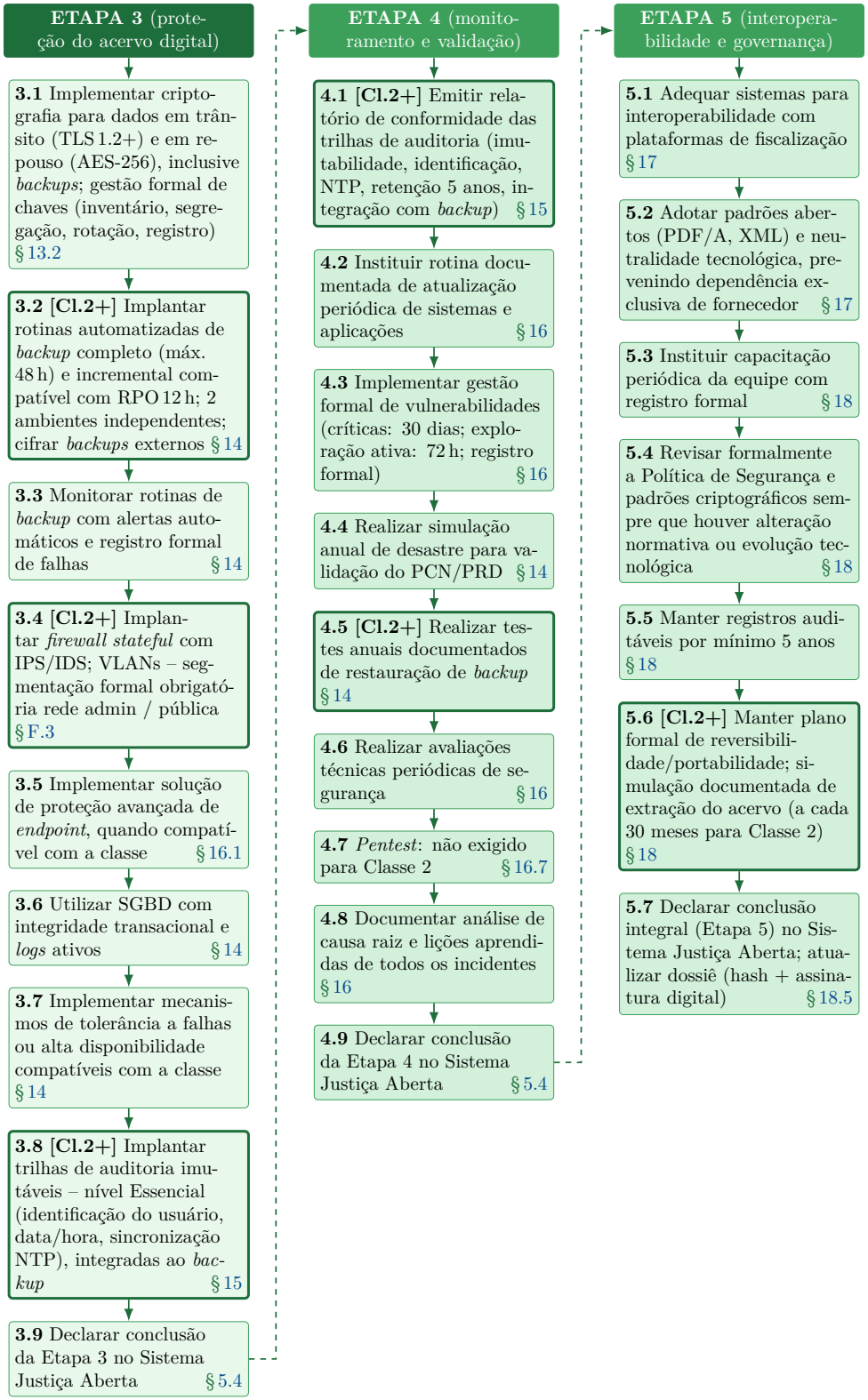


Figura 4: Roteiro de implementação – **Classe 2**, Etapas 1 e 2. Itens com borda espessa são exclusivos ou reforçados na Classe 2. Ver Seções 5, 4.2, 14, F.3.

Figura 5: Roteiro de implementação – **Classe 2**, Etapas 3 a 5. Itens com borda espessa são exclusivos ou reforçados na Classe 2. Ver Seções 14, F.3, 15, 16 e 18.



8.4.1 Etapas 1 e 2 – Governança, infraestrutura e continuidade

A Figura 6 apresenta as duas primeiras etapas, que devem ser concluídas em até 90 dias – prazo mais curto entre todas as classes, exigindo ação imediata).

A estrutura segue os mesmos itens do Anexo IV (1.1 a 1.9 e 2.1 a 2.9), com exigências reforçadas em diversos pontos: procedimento formal de comunicação de incidentes com prazo obrigatório de 72 horas e meta reforçada de 24 horas (itens 1.5 e 1.6); revisão rigorosa de contratos com fornecedores incluindo documentação técnica para migração (item 1.8); conectividade mínima de 50 Mbps com múltiplos *links* (item 2.4); PCN/PRD com RPO de 4 horas e RTO de 8 horas com mecanismos de alta disponibilidade (item 2.5); proteção avançada de *endpoint* com monitoramento comportamental (item 2.7); e documento de arquitetura tecnológica detalhado com indicação de HA (item 2.8).

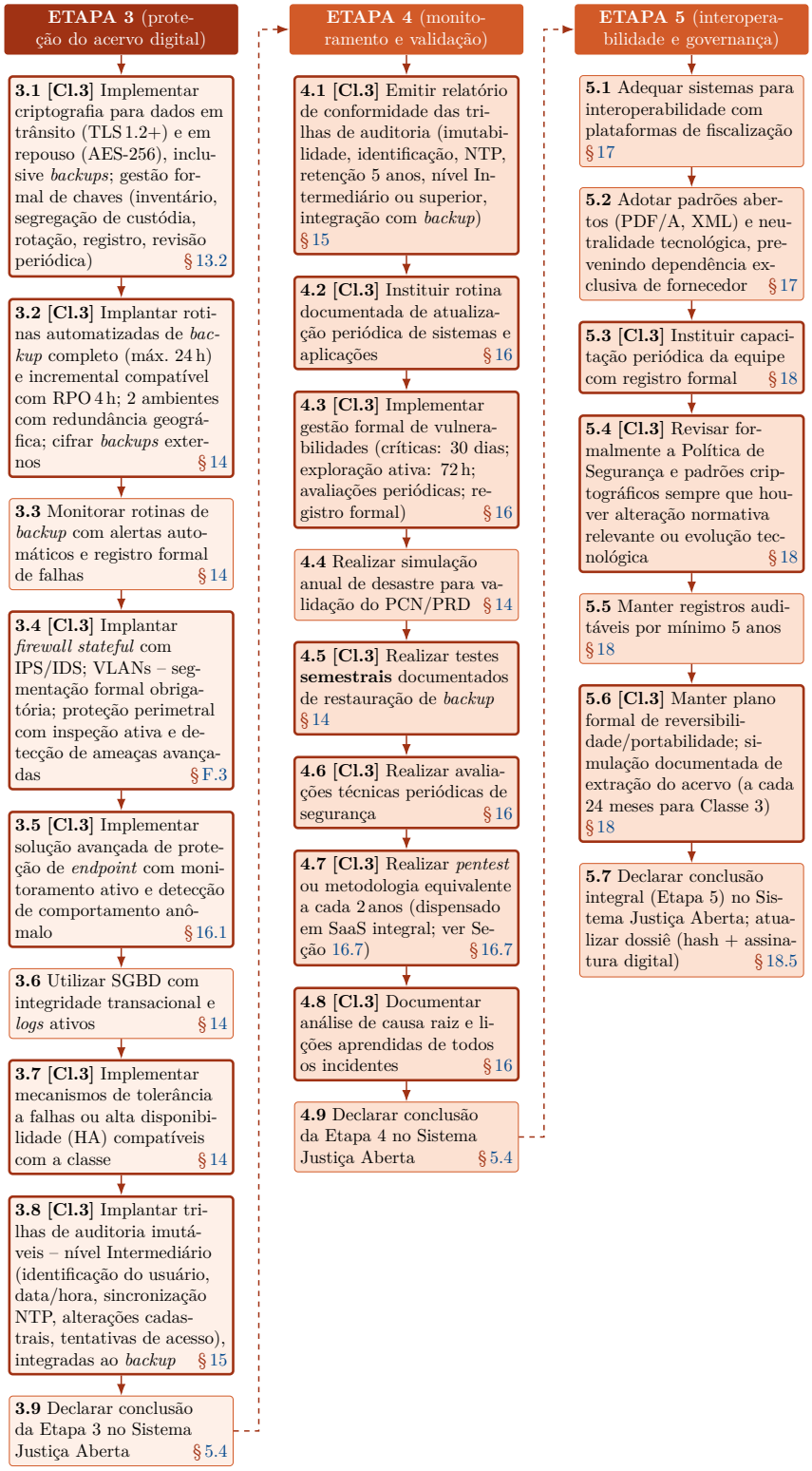
8.4.2 Etapas 3 a 5 – Proteção, monitoramento e governança evolutiva

A Figura 7 apresenta as etapas finais, com prazo máximo até 24 meses – o mais curto entre todas as classes.

A maioria dos blocos da Classe 3 possui borda espessa, refletindo o nível de exigência significativamente superior: criptografia com gestão de chaves incluindo segregação de custódia (item 3.1); *backup* completo a cada 24 horas com RPO de 4 horas e redundância geográfica (item 3.2); proteção perimetral com inspeção ativa e detecção de ameaças avançadas (item 3.4); proteção de *endpoint* com monitoramento comportamental (item 3.5); alta disponibilidade (item 3.7); trilhas de auditoria no nível Intermediário (item 3.8); testes **semestrais** de restauração (item 4.5); avaliações técnicas periódicas (item 4.6); *pentest* obrigatório a cada 2 anos (item 4.7); e simulação de extração do acervo a cada 24 meses (item 5.6).

Figura 6: Roteiro de implementação – **Classe 3**, Etapas 1 e 2. Itens com borda espessa são exclusivos ou reforçados na Classe 3. Ver Seções 5, 4.2, 14, 16.7 e F.3.

Figura 7: Roteiro de implementação – **Classe 3**, Etapas 3 a 5 (até fev/2028). Itens com borda espessa são exclusivos ou reforçados na Classe 3. Ver Seções 14, 16.7, F.3, 15, 16 e 18.



9 Checklist rápido de conformidade

Como utilizar este checklist

O checklist apresentado nesta seção reúne as principais medidas de segurança da informação previstas no Provimento nº 213.
Ele deve ser utilizado como uma verificação rápida das condições básicas de segurança tecnológica da serventia.
Se todos os itens da lista estiverem implementados, a unidade já terá adotado um conjunto mínimo de práticas compatíveis com os princípios fundamentais de segurança da informação estabelecidos pela norma.
Recomenda-se revisar este checklist periodicamente, especialmente após mudanças na infraestrutura tecnológica ou na equipe da serventia.
Prioridade inicial de governança O Provimento nº 213 estabelece que as primeiras medidas de conformidade dizem respeito à organização da governança de segurança da informação na serventia.
Antes da implementação de controles técnicos mais complexos, é necessário garantir que existam responsáveis designados, documentação mínima de segurança da informação e identificação dos ativos e sistemas utilizados pela unidade.
Por essa razão, o checklist inicia pelos elementos de governança previstos na Etapa 1 do Provimento.

Se a serventia cumprir os itens apresentados na Tabela 5, já estará em conformidade básica com os requisitos essenciais de segurança da informação previstos no Provimento nº 213 do Conselho Nacional de Justiça.

Este checklist resume as principais práticas que devem ser observadas no funcionamento cotidiano da infraestrutura tecnológica da serventia.

Recomenda-se que esta lista seja utilizada periodicamente como instrumento de verificação das condições de segurança dos sistemas e da organização tecnológica da unidade.

Se todos os itens da Tabela 5 estiverem implementados, a serventia já terá adotado um conjunto mínimo de práticas de segurança compatível com os princípios fundamentais estabelecidos pelo Provimento nº 213.

Nas seções seguintes, cada um desses controles será explicado com maior detalhe, apresentando orientações práticas para sua implementação.

10 Os 10 controles essenciais

Ideia central desta seção

Embora o Provimento nº 213 trate de diversos aspectos relacionados à tecnologia da informação e à segurança dos sistemas das serventias, na prática é possível sintetizar suas exigências em um conjunto reduzido de controles fundamentais.
Os dez controles apresentados nesta seção representam um núcleo mínimo de boas práticas de segurança da informação aplicáveis à maioria das serventias do Registro Civil.
A implementação consistente dessas medidas já contribui significativamente para proteger os dados registrais, reduzir riscos tecnológicos e assegurar a continuidade dos serviços prestados pela serventia.

Tabela 5: *Checklist* rápido de conformidade com os controles essenciais.

Controle essencial	**Verificado**
Cada usuário possui login próprio nos sistemas da serventia, evitando contas compartilhadas.	☐
Senhas fortes são utilizadas e a MFA está habilitada para todos os acessos administrativos e funcionalidades críticas.	☐
Computadores e servidores utilizam sistemas operacionais que ainda recebem atualizações de segurança.	☐
A comunicação entre sistemas utiliza protocolos seguros como HTTPS ou TLS.	☐
Equipamentos que armazenam dados registrais utilizam criptografia de disco ou de volume.	☐
Backups automáticos estão configurados para os sistemas e dados registrais, com periodicidade compatível com o RPO da classe da serventia.	☐
Os *backups* são armazenados em dois ambientes tecnicamente independentes, com ao menos um protegido contra *ransomware* por *Write Once, Read Many* (WORM), versionamento bloqueado ou isolamento lógico.	☐
Os *backups* destinados a ambientes externos ou serviços de nuvem são criptografados antes do envio (AES-256 ou equivalente), com chave sob custódia exclusiva da serventia.	☐
Testes periódicos de restauração de *backup* são realizados para verificar a recuperação dos dados.	☐
Os sistemas mantêm registros de atividades relevantes (*logs* de acesso e operações), protegidos contra alteração não autorizada e retidos por no mínimo 5 anos (Anexo II, item 3, inciso IV).	☐
Existe um procedimento documentado para gestão de incidentes, com classificação por gravidade (crítico, alto, médio, baixo) e previsão de comunicação à Corregedoria em até 72 horas para incidentes críticos (art. 11; Anexo II, item 4).	☐

O Provimento nº 213 estabelece diversos requisitos relacionados à segurança da informação, continuidade operacional e proteção dos dados registrais no âmbito das serventias do Registro Civil das Pessoas Naturais.

Embora a norma trate de diferentes aspectos técnicos e organizacionais, na prática é possível sintetizar suas exigências em um conjunto reduzido de controles fundamentais que, quando implementados de forma consistente, já proporcionam um nível adequado de proteção para a maioria das serventias.

Os controles apresentados a seguir representam um núcleo mínimo de boas práticas de segurança da informação aplicáveis ao ambiente tecnológico das serventias.

A adoção consistente dessas medidas contribui significativamente para:

- reduzir riscos de perda ou corrupção de dados registrais;
- prevenir acessos indevidos às informações;
- aumentar a disponibilidade e a confiabilidade dos sistemas;
- garantir maior continuidade na prestação dos serviços registrais.

10.1 Visão geral para o delegatário

O delegatário é o responsável final pela organização, funcionamento e segurança da serventia.

No contexto do Provimento nº 213, isso significa assegurar que a infraestrutura tecnológica utilizada pelo cartório opere de forma segura, confiável e capaz de preservar a integridade e a disponibilidade do acervo registral.

Na prática, o Provimento não exige que o delegatário possua conhecimento técnico aprofundado em tecnologia da informação. Entretanto, espera-se que ele garanta que determinadas medidas básicas de segurança sejam adotadas e mantidas pela serventia, seja por meio da equipe interna, seja com o apoio de fornecedores de sistemas e prestadores de serviços de tecnologia.

O papel do delegatário é, portanto, principalmente de supervisão e de garantia institucional. Cabe a ele assegurar que existam procedimentos mínimos para proteção dos sistemas e dos dados e que as rotinas essenciais, como atualização de sistemas, realização de *backups* e controle de acessos, estejam efetivamente sendo executadas.

10.2 Energia protegida por nobreak

Equipamentos críticos utilizados pela serventia devem estar conectados a sistemas de proteção elétrica, como nobreaks (Uninterruptible Power Supply - UPS).

Essa proteção evita desligamentos abruptos em caso de queda de energia, reduzindo o risco de perda de dados, interrupção de operações registrais ou danos físicos aos equipamentos.

Em geral, recomenda-se proteger por nobreak:

- servidores ou computadores que executam o sistema registral;
- equipamentos de rede, como modem e roteador;
- estações utilizadas para operações críticas.

10.3 Internet estável e rede organizada

A conectividade com a internet tornou-se essencial para o funcionamento dos sistemas registrais modernos e para a comunicação com plataformas eletrônicas e serviços institucionais.

Por essa razão, a serventia deve manter uma infraestrutura mínima de rede local organizada, com roteadores adequadamente configurados e acesso protegido por mecanismos básicos de segurança.

Sempre que possível, recomenda-se evitar a exposição direta de computadores internos à internet.

10.4 Sistemas operacionais com suporte vigente

Computadores e servidores utilizados pela serventia devem operar com sistemas operacionais que ainda estejam dentro do período de suporte do fabricante.

Sistemas fora de suporte deixam de receber atualizações de segurança, tornando os equipamentos mais vulneráveis a falhas e ataques cibernéticos.

Manter as atualizações automáticas ativadas é uma das medidas mais simples e eficazes para reduzir riscos de segurança.

10.5 Contas individualizadas para cada usuário

Cada pessoa que utiliza os sistemas da serventia deve possuir uma conta de acesso individual.

O uso de contas compartilhadas dificulta a identificação de quem realizou determinada operação e compromete a rastreabilidade das atividades realizadas nos sistemas.

Contas individualizadas permitem manter registros confiáveis de acesso e facilitam auditorias e investigações em caso de incidentes.

10.6 Autenticação forte para acessos críticos

O Provimento nº 213 estabelece a autenticação multifator (MFA - *Multi-Factor Authentication*) como obrigatória para acessos administrativos, acessos a sistemas, bases de dados e funcionalidades críticas (art. 5º, §2º e Anexo II, item 1, inciso II).

A autenticação por fator único, apenas senha, é admitida exclusivamente para perfis de menor risco e desde que haja justificativa técnica documentada no dossiê da serventia. Em qualquer hipótese, é vedado o uso de credenciais compartilhadas ou genéricas.

Esse mecanismo combina a senha do usuário com um segundo fator de verificação, como um código temporário gerado em aplicativo autenticador ou enviado ao dispositivo do usuário.

Na prática, recomenda-se habilitar MFA obrigatoriamente para:

- acessos administrativos aos sistemas registrais;
- acessos remotos à infraestrutura da serventia;
- acesso a bancos de dados e painéis de gestão;
- operações que envolvam dados registrais sensíveis.

A implementação de MFA para acessos administrativos integra a **Etapa 1 do Anexo IV** do Provimento, sendo portanto um dos requisitos de prazo mais urgente (ver Seção 5).

10.7 Criptografia de dados em trânsito

A comunicação entre sistemas deve utilizar protocolos seguros, garantindo que os dados transmitidos pela rede estejam protegidos contra interceptação e não possam ser interpretados por terceiros caso capturados durante a transmissão.

O Provimento nº 213 exige protocolos equivalentes a TLS 1.2 ou superior para dados em trânsito (Anexo II, item 2, inciso I). O uso de versões anteriores, SSL, TLS 1.0 e TLS 1.1, é vedado, pois essas versões possuem vulnerabilidades conhecidas e são consideradas depreciadas pela comunidade técnica.

Na prática, isso significa que os sistemas utilizados pela serventia devem ser acessados exclusivamente por endereços iniciados por `https://`, e a versão de TLS utilizada deve ser verificada junto ao fornecedor do sistema registral. A versão recomendada é o TLS 1.3, por ser a mais atual e segura.

Atualmente, a maioria dos sistemas registrais e plataformas eletrônicas modernas já utiliza TLS 1.2 ou TLS 1.3 por padrão. Entretanto, sistemas mais antigos podem ainda operar com versões depreciadas, sendo necessário verificar e atualizar a configuração.

10.8 Criptografia de dados em repouso

Equipamentos que armazenam dados registrais devem utilizar criptografia de disco ou de volume.

Essa medida protege as informações em caso de perda, furto ou acesso indevido ao equipamento físico.

O Provimento nº 213 exige que a criptografia de dados em repouso possua robustez equivalente, no mínimo, ao padrão *Advanced Encryption Standard* (AES-256) com chave de 256 bits) ou padrão tecnicamente equivalente ou superior (Anexo II, item 2, inciso II).

Na prática, as ferramentas nativas dos sistemas operacionais modernos já atendem a esse requisito quando configuradas corretamente:

- **BitLocker** (Windows Pro/Enterprise): utiliza AES-256 quando configurado com o modo XTS-AES 256, que deve ser verificado nas configurações de política de grupo (*Group Policy*) do sistema;
- **Criptografia de Dispositivo** (Windows Home): utiliza AES-128 por padrão em alguns dispositivos. Para ambientes que exijam AES-256, recomenda-se verificar junto ao fornecedor do sistema a configuração aplicável;
- **FileVault** (macOS): utiliza AES-128 em modo XTS, considerado tecnicamente equivalente ao AES-256 para fins práticos de proteção de disco;
- **LUKS** (Linux): suporta AES-256, que deve ser especificado explicitamente durante a configuração, pois versões mais antigas podem usar padrões menos robustos por padrão.

Em caso de dúvida sobre a configuração aplicada, recomenda-se consultar o fornecedor do sistema registral ou o responsável técnico de TI da serventia.

Os sistemas operacionais modernos oferecem mecanismos nativos de criptografia de

disco, que variam conforme o sistema utilizado:

- **Windows:** a forma mais simples é verificar se a Criptografia de Dispositivo já está habilitada em Configurações → Privacidade e Segurança → Criptografia de Dispositivo. Essa função está disponível em todas as edições do Windows, incluindo a edição Home, em equipamentos com hardware compatível. Em edições Windows Pro ou superior, o recurso equivalente e mais avançado é o *BitLocker*, acessível pelo Painel de Controle.
- **macOS:** Macs com processador Apple Silicon (linha M1/M2/M3 e posteriores) ou chip de segurança T2 já possuem criptografia de disco ativa por padrão. Em modelos mais antigos, recomenda-se ativar o *FileVault* em Configurações do Sistema → Privacidade e Segurança → *FileVault*.
- **Linux:** a criptografia de disco via LUKS pode ser ativada durante a instalação do sistema operacional. A maioria das distribuições, como Ubuntu, apresenta essa opção de forma simples no assistente de instalação. A configuração após a instalação é mais complexa e recomenda-se apoio técnico especializado.

10.9 *Backup* automático e externo

A realização de *backups* regulares é uma das medidas mais importantes para proteger o acervo registral.

O Provimento nº 213 estabelece requisitos específicos que vão além da simples realização de cópias de segurança. As rotinas de *backup* devem ser automáticas, armazenar os dados em pelo menos dois ambientes tecnicamente independentes e garantir que ao menos um desses ambientes esteja protegido contra *ransomware* e exclusão indevida (Anexo IV, item 3.2 do Provimento).

Essas exigências são detalhadas na Seção 14 deste guia.

10.10 Teste periódico de restauração

Não basta apenas realizar *backups*. É fundamental verificar se os dados podem ser efetivamente recuperados.

Testes periódicos de restauração permitem confirmar que os arquivos de *backup* não estão corrompidos e que o processo de recuperação funciona corretamente.

10.11 Documentação mínima de conformidade

A serventia deve manter registros simples que demonstrem a adoção das práticas de segurança previstas no Provimento.

Essa documentação pode incluir, por exemplo:

- descrição das rotinas de *backup*;
- lista de usuários autorizados;
- registro de testes de restauração;
- registro de incidentes de segurança, com classificação por gravidade e registro de eventual comunicação à Corregedoria (obrigatória em até 72 horas para incidentes críticos).

A documentação não precisa ser extensa ou complexa. O objetivo é demonstrar que as práticas de segurança são conhecidas, aplicadas e verificáveis.

11 Implementação prática dos controles

Aplicação prática dos controles

Nesta parte do guia mostramos como implementar, na prática, os controles de segurança apresentados anteriormente.
As seções a seguir apresentam orientações práticas para a implementação dos controles de segurança descritos neste guia.
O objetivo é demonstrar como essas medidas podem ser adotadas no ambiente cotidiano das serventias, utilizando recursos tecnológicos amplamente disponíveis nos sistemas operacionais, nos equipamentos de rede e nos próprios sistemas registrais.
Sempre que possível, recomenda-se priorizar soluções simples, estáveis e bem documentadas, compatíveis com a realidade operacional da unidade.

Os controles essenciais apresentados na seção anterior podem ser implementados utilizando recursos amplamente disponíveis nos sistemas operacionais, nos equipamentos de rede e nas próprias plataformas tecnológicas utilizadas pelas serventias.

Na maioria dos casos, não é necessário adotar soluções tecnológicas complexas ou infraestruturas especializadas. A implementação adequada de boas práticas básicas de segurança da informação já é suficiente para reduzir significativamente os riscos operacionais associados ao uso de sistemas digitais.

As orientações a seguir apresentam exemplos práticos de implementação dos controles essenciais no ambiente tecnológico das serventias.

11.1 Infraestrutura elétrica

A estabilidade da energia elétrica é um elemento fundamental para a segurança e o funcionamento adequado dos sistemas utilizados pela serventia.

Quedas abruptas de energia podem causar perda de dados, corrupção de arquivos, interrupção de operações registrais e até danos físicos aos equipamentos.

O Provimento nº 213 (Anexo I, item 1) exige, para todas as classes, os seguintes requisitos de infraestrutura elétrica:

- **Nobreak (SAI/UPS) com autonomia mínima de 30 minutos:** deve garantir o salvamento de dados em memória, o encerramento seguro das transações ativas e o desligamento ordenado dos equipamentos (*safe shutdown*) em caso de queda de energia. Devem ser protegidos por nobreak: servidor ou computador principal que executa o sistema registral; equipamentos de rede (modem, roteador, *switch*); e computadores utilizados em operações críticas. Recomenda-se verificar periodicamente o estado das baterias, pois possuem vida útil limitada e precisam ser substituídas após alguns anos de uso;
- **Plano de contingência energética:** cada serventia deve possuir um plano documentado que descreva os procedimentos a adotar em caso de falha prolongada no fornecimento de energia. Para Classe 1, um procedimento simples e escrito é

suficiente. Para Classes 2 e 3, o plano deve integrar o PCN/PRD e prever medidas proporcionais à criticidade das operações, podendo incluir gerador, *link* de internet redundante via dados móveis ou transferência temporária de operações para ambiente alternativo;

- **Aterramento técnico adequado:** a infraestrutura elétrica que suporta ativos críticos de tecnologia da informação deve possuir aterramento funcional e tecnicamente aferido, mantido laudo atualizado subscrito por profissional habilitado com anotação de responsabilidade técnica (art. 12, §8º do Provimento).

Evidência mínima para o dossiê técnico (Etapa 2): nota fiscal ou contrato de aquisição do nobreak; especificação técnica da autonomia; e documento ou e-mail do fornecedor confirmando a capacidade de *safe shutdown*. Para o plano de contingência energética, basta um documento interno assinado pelo delegatário descrevendo os procedimentos adotados.

11.2 Rede e conectividade

A conectividade com a internet é essencial para o funcionamento dos sistemas registrais modernos, para a comunicação com centrais eletrônicas e para o acesso a serviços institucionais.

O Provimento nº 213 (Anexo I, item 2) estabelece velocidades mínimas de referência por classe, com caráter funcional: considera-se atendido o requisito quando a serventia demonstrar, por testes documentados, que a infraestrutura contratada permite a conclusão do *backup* incremental e a sincronização de dados dentro do RPO estabelecido para sua classe, independentemente da largura de banda nominal.

Tabela 6: Velocidades mínimas de referência e requisitos de rede por classe (Anexo I, item 2 do Provimento nº 213).

Classe	Velocidade mínima	Requisitos adicionais
Classe 1	2 Mbps	Roteador e *switch*. Alta disponibilidade de *link* não é obrigatória quando o RTO/RPO for atendido por *backup* periódico testado com restauração em até 24 horas (Anexo I, item 2.1).
Classe 2	10 Mbps	Roteador, *switch* e, quando necessário, múltiplos *links* ou tecnologia equivalente que assegure desempenho efetivo compatível com a classe.
Classe 3	50 Mbps	Roteador, *switch* e múltiplos *links* obrigatórios. Conectividade deve suportar RTO de 8 horas e RPO de 4 horas com mecanismos de HA.

Além da velocidade, a rede interna da serventia deve observar os seguintes requisitos:

- **Roteador e *switch*:** obrigatórios para todas as classes. O roteador gerencia as conexões internas e externas; o *switch* interliga os dispositivos da rede interna. Um simples roteador doméstico pode acumular ambas as funções em serventias de Classe 1, mas não substitui um *firewall* dedicado;
- **Proteção básica do equipamento de rede:** proteger o acesso administrativo ao roteador e ao *switch* com senha forte; manter o *firmware* atualizado; e evitar a exposição direta de servidores e computadores internos à internet sem passagem pelo *firewall*;

- ***Firewall stateful* com IPS/IDS e segmentação lógica de rede:** esses controles são obrigatórios para todas as classes, mas pertencem à **Etapa 3** do cronograma de implementação (Anexo IV, item 3.4 e art. 8º, inciso VII). Portanto, devem ser planejados já na Etapa 2, inclusive com a documentação da arquitetura tecnológica prevista abaixo, mas somente implementados formalmente na Etapa 3. Os requisitos detalhados constam da Seção F.3 deste guia.

Evidência mínima para o dossiê técnico (Etapa 2): contrato ou fatura do serviço de internet com indicação da velocidade contratada; e teste documentado de velocidade efetiva (captura de tela de serviço de medição, como fast.com ou speedtest.net, com data e horário visíveis).

11.3 Ambiente físico e proteção estrutural

O Provimento nº 213 (Anexo I, item 3) exige que os equipamentos críticos de tecnologia da informação estejam instalados em ambiente físico adequado.

Para serventias que operam infraestrutura local, são obrigatórios:

- **Espaço físico isolado para equipamentos críticos:** servidores, *switches*, roteadores e nobreaks devem estar em local com controle de acesso restrito, que impeça o manuseio por pessoas não autorizadas. Em serventias de menor porte, um armário com chave ou uma sala de uso exclusivo do técnico de TI já atende ao requisito de forma proporcional;
- **Proteção contra incêndios, inundações e variações térmicas:** o ambiente deve dispor, no mínimo, de extintor de incêndio adequado a equipamentos elétricos (CO_2 ou pó químico seco classe C), instalação em local sem risco de infiltração ou inundação e ventilação adequada para evitar superaquecimento dos equipamentos;
- **Organização física:** cabeamento organizado e identificado, equipamentos fixados adequadamente e ausência de materiais inflamáveis próximos aos ativos de TI.

Para serventias que operam **integralmente em nuvem ou em arquitetura SaaS**, sem infraestrutura local significativa, a exigência de ambiente físico é suprida pela documentação contratual que comprove ou ao menos indicie a adoção, pelo fornecedor, de controles equivalentes de segurança física e ambiental (Anexo I, item 3, inciso I). Nesse caso, basta incluir no dossiê técnico o contrato com o fornecedor ou declaração que mencione as certificações de segurança do *data center* utilizado (ex.: ISO 27001, SOC 2).

Evidência mínima para o dossiê técnico (Etapa 2): fotografia ou descrição escrita do local de instalação dos equipamentos, com indicação das medidas de controle de acesso e proteção adotadas; ou, para solução em nuvem, cópia do contrato ou declaração do fornecedor sobre segurança física do ambiente.

11.4 Sistemas operacionais e atualizações

Computadores e servidores utilizados pela serventia devem operar com sistemas operacionais que ainda estejam dentro do período de suporte do fabricante.

Sistemas fora de suporte deixam de receber atualizações de segurança, tornando os equipamentos mais vulneráveis a falhas e ataques cibernéticos.

Na prática, recomenda-se:

- manter habilitadas as atualizações automáticas do sistema operacional;
- atualizar regularmente navegadores e aplicativos utilizados no cartório;
- substituir sistemas operacionais obsoletos;
- evitar o uso de computadores muito antigos que não suportem versões atualizadas do sistema.

A aplicação regular de atualizações de segurança é uma das medidas mais simples e eficazes para reduzir riscos tecnológicos.

11.5 Licenciamento e suporte

Todos os softwares utilizados pela serventia devem possuir licenciamento regular para uso comercial, quando aplicável.

É admitida a utilização de software livre ou de código aberto, desde que compatível com as exigências de segurança da informação e manutenção de atualizações de segurança.

Não devem ser utilizados sistemas operacionais, bancos de dados ou aplicações cujo suporte oficial pelo fabricante tenha sido encerrado (End of Life – EOL).

11.6 Portabilidade e reversibilidade

Os sistemas utilizados pela serventia devem permitir a extração integral do acervo registral em formato estruturado e interoperável, sem dependência técnica do fornecedor.

Os contratos com fornecedores de tecnologia devem prever cláusulas expressas de portabilidade de dados, reversibilidade de serviços e cooperação em eventual processo de migração tecnológica.

11.7 Documento de arquitetura tecnológica

O Provimento nº 213 (Anexo IV, item 2.8) exige que cada serventia formalize, na Etapa 2, um documento técnico simplificado que descreva sua arquitetura tecnológica adotada.

Esse documento não precisa ser extenso. Seu objetivo é registrar, de forma verificável, como a infraestrutura da serventia está organizada, de modo a facilitar tanto a gestão interna quanto eventual fiscalização correicional.

O documento deve conter, no mínimo:

- **Topologia básica de rede:** descrição ou diagrama simples dos equipamentos conectados e de como estão organizados (roteador, *switch*, computadores, servidor, impressoras, *firewall*);
- **Indicação dos ambientes utilizados:** se a serventia opera em infraestrutura local, em nuvem, em ambiente híbrido, em solução SaaS fornecida por terceiro ou em arquitetura compartilhada com outras serventias;
- **Fluxos de dados críticos:** indicação de como os dados registrais trafegam entre os sistemas (ex.: sistema registral local sincroniza com serviço em nuvem; *backup* incremental é enviado para serviço de armazenamento externo);

- **Localização física ou lógica dos *backups*:** identificação dos ambientes onde as cópias de segurança são mantidas, com indicação do provedor ou mídia utilizada;
- **Integrações externas relevantes:** sistemas nacionais, plataformas eletrônicas e serviços de terceiros com os quais a serventia se comunica (ex.: central de serviços do RCPN, IdRC, plataformas estaduais);
- **Mecanismos de alta disponibilidade ou redundância:** indicação das soluções adotadas para tolerância a falhas, quando existentes.

Para serventias de Classe 1, um texto descritivo de uma a duas páginas ou um diagrama simples desenhado à mão ou em ferramenta básica (inclusive editor de texto com formas geométricas) é plenamente suficiente, desde que cubra os elementos acima e seja assinado pelo delegatário ou responsável técnico.

Evidência mínima para o dossiê técnico (Etapa 2): o próprio documento de arquitetura, com data e assinatura do delegatário ou responsável técnico. Para Classes 2 e 3, recomenda-se que o documento seja assinado digitalmente e que seu *hash* conste do registro de integridade do dossiê.

11.8 Gestão de acessos

O controle adequado de acesso aos sistemas utilizados pela serventia depende da correta identificação de cada usuário.

Cada funcionário deve possuir sua própria conta de acesso aos sistemas do cartório, protegida por senha individual.

Entre as práticas recomendadas estão:

- evitar contas genéricas, como “atendimento” ou “cartorio”;
- remover acessos de usuários que deixarem a serventia;
- conceder apenas as permissões necessárias para cada função;
- habilitar MFA obrigatoriamente para todos os acessos administrativos e a funcionalidades críticas, conforme exige o art. 5º, §2º do Provimento nº 213.

Essas medidas contribuem para garantir rastreabilidade das operações realizadas nos sistemas registrais.

11.9 Criptografia

A criptografia é utilizada para proteger informações digitais tanto durante a transmissão de dados pela rede quanto no armazenamento das informações em computadores e servidores.

Para a criptografia em trânsito, recomenda-se utilizar sistemas que operem exclusivamente por meio de comunicação segura baseada em HTTPS ou TLS.

Já para a proteção dos dados armazenados, recomenda-se utilizar criptografia de disco ou de volume nos equipamentos que armazenam dados registrais.

Essa proteção pode ser ativada diretamente nos sistemas operacionais. Na maioria dos equipamentos modernos, a criptografia já está disponível de forma nativa e de fácil ativação:

- **Windows:** verificar se a Criptografia de Dispositivo está habilitada em Configu-

rações → Privacidade e Segurança → Criptografia de Dispositivo (disponível em todas as edições, incluindo Home). Em Windows Pro ou superior, o *BitLocker* oferece opções adicionais de gestão.
- **macOS:** Macs modernos com Apple Silicon ou chip T2 já têm criptografia ativa por padrão. Em modelos mais antigos, ativar o *FileVault* em Configurações do Sistema → Privacidade e Segurança.
- **Linux:** ativar o LUKS durante a instalação do sistema, utilizando a opção disponível no assistente de instalação da distribuição utilizada.

Sempre que possível, deve-se utilizar os mecanismos de criptografia já integrados aos sistemas operacionais, evitando a necessidade de gestão manual de chaves criptográficas.

11.10 Gestão de chaves criptográficas

Requisito da Etapa 3 para todas as classes (Anexo IV, item 3.1).
O Provimento nº 213 exige que a criptografia seja acompanhada de gestão formal das chaves utilizadas. A chave que não é gerenciada é um risco equivalente à ausência de criptografia.

O art. 9º, §3º e o Anexo IV, item 3.1 determinam que a gestão de chaves criptográficas observe controles de acesso restritos, segregação de funções e registro de utilização, conforme política interna formalizada. A mera adoção de algoritmos fortes não é suficiente: a segurança criptográfica depende igualmente da gestão adequada das chaves utilizadas.

A política interna de gestão de chaves deve contemplar, no mínimo, os seguintes elementos (Anexo IV, item 3.1, incisos I a VI):

- **Inventário atualizado:** relação de todas as chaves e certificados digitais ativos, com indicação de finalidade, algoritmo, sistema a que pertencem, data de emissão e data de expiração;
- **Segregação de custódia:** as chaves de criptografia dos *backups* externos e dos dados em repouso não devem estar sob controle exclusivo de um único usuário nem armazenadas no mesmo ambiente que os dados protegidos; em particular, as chaves de *backup* devem ser mantidas separadamente das credenciais de acesso aos sistemas principais;
- **Controle formal de acesso:** apenas responsáveis formalmente designados, com autorização documentada, devem ter acesso às chaves e aos mecanismos de descriptografia;
- **Rotação e renovação periódica:** política documentada que defina os intervalos máximos de uso de cada chave e o procedimento de renovação, especialmente após incidentes, alterações de pessoal, suspeita de comprometimento ou proximidade do vencimento de certificados digitais;
- **Registro de operações:** log auditável das operações de geração, renovação, revogação e uso de chaves, com identificação do responsável e da data;
- **Revisão periódica dos padrões adotados:** verificação, ao menos anual, de que os algoritmos e comprimentos de chave utilizados permanecem seguros, com substituição obrigatória de padrões que se tornem vulneráveis (Anexo II, item 2, inciso V; Anexo III, item 4.9, inciso IV).

Quanto aos padrões técnicos exigidos (Anexo II, item 2):

- para **dados em trânsito**: utilizar exclusivamente TLS 1.2 ou superior; TLS 1.3 é o recomendado; versões anteriores (SSL, TLS 1.0, TLS 1.1) são vedadas;
- para **dados em repouso**: criptografia com robustez equivalente, no mínimo, a AES-256; as ferramentas nativas dos sistemas operacionais modernos atendem a esse requisito quando configuradas corretamente;
- para **backups externos**: aplicar criptografia AES-256 antes do envio para armazenamento externo ou em nuvem, mantendo a chave sob custódia exclusiva da serventia e não do provedor de nuvem.

É vedada a utilização de algoritmos, versões ou modos de operação depreciados ou vulneráveis, como MD5, SHA-1, DES, 3DES, RC4 e versões antigas de SSL e TLS (Anexo II, item 2, inciso III).

Para serventias de Classe 1, admite-se gestão simplificada, desde que as chaves dos *backups* externos estejam documentadas e sob custódia exclusiva da serventia e exista registro mínimo de certificados e de sua validade. Para serventias de Classes 2 e 3, a política de gestão de chaves deve integrar o dossiê técnico e ser formalmente documentada, com todos os elementos acima.

11.11 *Backup* e armazenamento externo

A realização de cópias de segurança é essencial para proteger o acervo registral contra falhas de *hardware*, erros humanos ou incidentes tecnológicos.

O Provimento nº 213 exige que os *backups* sejam realizados de forma automática e armazenados em pelo menos dois ambientes tecnicamente independentes, com ao menos um deles protegido contra *ransomware* e exclusão indevida.

Entre as práticas obrigatórias estão:

- programar *backups* automáticos com periodicidade compatível com o RPO da classe da serventia (ver Seção 14);
- incluir no *backup* os bancos de dados do sistema registral, documentos digitais, imagens registrais e configurações essenciais dos sistemas;
- manter cópias em dois ambientes independentes, por exemplo, um armazenamento local e um serviço de nuvem, ou dois serviços de nuvem em regiões geográficas distintas;
- garantir que ao menos um ambiente de *backup* esteja protegido contra *ransomware*, por meio de WORM, versionamento bloqueado, isolamento lógico ou mecanismo equivalente;
- criptografar os *backups* antes do envio para armazenamento externo, mantendo a chave sob custódia exclusiva da serventia.

Além da realização dos *backups*, é fundamental realizar testes periódicos de restauração para verificar se os dados podem ser recuperados corretamente em caso de incidente (ver Seção 14).

12 Acessos, autenticação e senhas

Base normativa no Provimento nº 213: Art. 5º.

Princípio fundamental de controle de acesso

Regra básica: cada pessoa deve acessar os sistemas da serventia utilizando sua própria conta de usuário.
Nos sistemas utilizados pela serventia, deve ser sempre possível identificar qual usuário realizou cada operação.
Por esse motivo, cada pessoa deve possuir uma conta individual de acesso, com permissões compatíveis com as funções que exerce.
O uso de contas compartilhadas deve ser evitado, pois dificulta a rastreabilidade das ações realizadas nos sistemas e pode comprometer a segurança do acervo registral.
Sempre que possível, recomenda-se utilizar mecanismos de autenticação mais robustos, como MFA.
Para atender à obrigatoriedade de MFA, sempre que o sistema registral utilizado pela serventia for compatível, recomenda-se a utilização do IdRC, que implementa autenticação segura baseada em padrões modernos de identidade digital e suporta autenticação multifator de forma integrada.

O controle adequado de acesso aos sistemas utilizados pela serventia é um dos elementos mais importantes da segurança da informação no ambiente registral.

A correta identificação dos usuários, a utilização de mecanismos seguros de autenticação e a adoção de políticas adequadas de senhas contribuem para prevenir acessos indevidos, proteger dados registrais e garantir a rastreabilidade das operações realizadas nos sistemas.

O Provimento nº 213 estabelece a necessidade de adoção de mecanismos de controle de acesso que permitam identificar os usuários dos sistemas e proteger adequadamente os ambientes tecnológicos das serventias.

12.1 Contas individualizadas

Cada pessoa que utiliza os sistemas da serventia deve possuir uma conta de acesso individual.

O uso de contas compartilhadas dificulta a identificação de quem realizou determinada operação e compromete a rastreabilidade das atividades realizadas nos sistemas registrais.

Por esse motivo, recomenda-se que cada escrevente, substituto ou funcionário da serventia utilize sua própria conta de acesso, protegida por senha pessoal e intransferível.

Entre as práticas recomendadas estão:

- criar uma conta de usuário para cada funcionário que utiliza os sistemas da serventia;
- evitar contas genéricas, como “atendimento” ou “cartorio”;
- remover ou desativar imediatamente as contas de pessoas que deixarem a serventia;
- conceder apenas os níveis de acesso necessários para cada função exercida.

12.2 Política de senhas

As senhas continuam sendo um dos mecanismos mais utilizados para proteção de acesso aos sistemas.

Uma política adequada de senhas contribui para reduzir o risco de acesso indevido aos sistemas e às informações registrais.

Na prática, recomenda-se que as senhas:

- possuam pelo menos 8 a 12 caracteres;
- combinem letras, números e, quando possível, caracteres especiais;
- não utilizem informações óbvias, como datas de nascimento ou nomes;
- não sejam reutilizadas em múltiplos sistemas;
- não sejam compartilhadas entre usuários.

Sempre que possível, os sistemas devem exigir a criação de senhas com nível mínimo de complexidade e permitir sua alteração periódica.

12.3 Autenticação multifator

A autenticação multifator (MFA - *Multi-Factor Authentication*) combina a senha do usuário com um segundo fator de verificação, como um código temporário gerado por aplicativo autenticador ou outro mecanismo equivalente.

Esse modelo reduz significativamente o risco de acesso indevido, mesmo quando uma senha é comprometida.

MFA é obrigatória, não opcional.
O art. 5º, §2º e o Anexo II, item 1, inciso II do Provimento nº 213 estabelecem a autenticação multifator como obrigatória para acessos administrativos, de gestão de sistemas, bancos de dados e funcionalidades críticas.
A autenticação por fator único é admitida apenas para perfis de menor risco, desde que haja justificativa técnica documentada no dossiê da serventia. Credenciais compartilhadas ou genéricas são vedadas em qualquer hipótese.

A MFA é obrigatória especialmente para:

- **acessos administrativos** aos sistemas registrais e de gestão, sem exceção;
- **acessos remotos** à infraestrutura da serventia;
- **acesso a bancos de dados** e painéis de configuração de sistemas;
- **funcionalidades críticas** que envolvam dados registrais sensíveis ou operações irreversíveis.

Para os demais perfis de usuário, como escreventes com acesso operacional cotidiano sem privilégios administrativos, a serventia pode admitir autenticação por fator único, desde que documente tecnicamente essa decisão no dossiê de segurança e avalie periodicamente a necessidade de revisão.

A implementação de MFA para acessos administrativos é requisito da Etapa 1 do Anexo IV do Provimento, integrando o prazo mais urgente de conformidade (ver Seção 5).

12.4 Uso do sistema de autenticação IdRC

Sempre que possível, recomenda-se que as serventias utilizem o Sistema de Autenticação (IdRC) do Registro Civil como mecanismo centralizado de autenticação para acesso aos sistemas registrais e às plataformas institucionais.

O IdRC implementa padrões modernos de autenticação e autorização baseados nos protocolos *OpenID Connect* e *OAuth 2.0*.

A utilização do IdRC permite:

- autenticação segura e padronizada de usuários;
- integração com múltiplos sistemas registrais;
- suporte a MFA;
- maior controle e rastreabilidade dos acessos aos sistemas;
- simplificação da gestão de identidades digitais.

A adoção de um mecanismo centralizado de autenticação como o IdRC contribui para aumentar o nível de segurança dos sistemas utilizados pelas serventias e facilita o atendimento aos requisitos de controle de acesso previstos no Provimento nº 213.

Sempre que os sistemas registrais ou plataformas institucionais suportarem integração com o IdRC, recomenda-se priorizar sua utilização como mecanismo principal de autenticação dos usuários.

13 Criptografia de dados

Base normativa no Provimento nº 213: Art. 9º.

Princípio básico da criptografia

Regra simples: dados sensíveis devem ser protegidos tanto durante a transmissão quanto durante o armazenamento.
A criptografia é utilizada para proteger dados contra acesso não autorizado, tanto durante a transmissão entre sistemas quanto quando as informações estão armazenadas em computadores ou servidores.
De forma simplificada, existem dois contextos principais de proteção criptográfica:

- **dados em trânsito**: quando as informações são transmitidas pela rede, devendo ser protegidas por protocolos seguros como HTTPS ou TLS;
- **dados em repouso**: quando os dados estão armazenados em discos, servidores ou dispositivos de *backup*, podendo ser protegidos por criptografia de disco ou de volume.

A utilização consistente desses mecanismos contribui para proteger o acervo registral contra interceptação de dados, acessos indevidos e exposição de informações sensíveis.

A criptografia é um dos mecanismos mais importantes para proteger informações digitais. Ela permite que os dados sejam armazenados ou transmitidos de forma segura, impedindo que terceiros não autorizados consigam compreender seu conteúdo.

No contexto das serventias do Registro Civil das Pessoas Naturais, a criptografia é utilizada principalmente em dois cenários:

- durante a transmissão de dados entre sistemas e serviços (*dados em trânsito*);
- no armazenamento de informações em computadores, servidores ou mídias de *backup* (*dados em repouso*).

O Provimento nº 213 estabelece que dados sensíveis e informações registrais devem ser protegidos por mecanismos criptográficos adequados, especialmente quando transmitidos por redes de comunicação ou armazenados em dispositivos eletrônicos.

13.1 Criptografia de dados em trânsito

Dados em trânsito são aqueles transmitidos entre sistemas, computadores ou serviços conectados em rede.

Sem proteção adequada, essas informações podem ser interceptadas durante a transmissão, permitindo que terceiros tenham acesso ao conteúdo dos dados.

A criptografia em trânsito garante que, mesmo que os dados sejam capturados durante a comunicação, eles não possam ser interpretados por pessoas não autorizadas.

Para proteger a comunicação entre sistemas, o Provimento nº 213 exige a utilização de protocolos equivalentes a TLS 1.2 ou superior (Anexo II, item 2, inciso I).

Versões de TLS: o que é exigido e o que é vedado

- **TLS 1.3** - versão mais recente e segura; recomendada;
- **TLS 1.2** - versão mínima exigida pelo Provimento; aceita;
- **TLS 1.1, TLS 1.0, SSL** - versões depreciadas com vulnerabilidades conhecidas; vedadas pelo Provimento (Anexo II, item 2, inciso III).

Na prática, os sistemas utilizados pela serventia devem ser acessados exclusivamente por endereços iniciados por `https://`. A versão de TLS efetivamente utilizada pode ser verificada junto ao fornecedor do sistema registral ou por ferramentas de diagnóstico de rede disponíveis gratuitamente.

A maioria das plataformas registrais modernas já utiliza TLS 1.2 ou TLS 1.3 por padrão. Entretanto, sistemas mais antigos podem ainda operar com versões depreciadas, sendo necessário verificar e exigir atualização do fornecedor.

Recomenda-se ainda a utilização de certificados digitais válidos, emitidos por autoridades certificadoras confiáveis, e que os sistemas operem exclusivamente por meio de comunicação criptografada, sem fallback para conexões não seguras.

13.2 Criptografia de dados em repouso

Dados em repouso são aqueles armazenados em computadores, servidores ou dispositivos de armazenamento.

Caso um equipamento seja perdido, furtado ou acessado indevidamente, essas informações podem ficar expostas se não estiverem protegidas.

A criptografia de disco protege os dados armazenados no equipamento, garantindo que as informações não possam ser acessadas sem autorização.

Recomenda-se que computadores e servidores que armazenam dados registrais utilizem criptografia de disco ou de volume.

O Provimento nº 213 exige que a criptografia de dados em repouso possua robustez equivalente, no mínimo, ao padrão AES-256 (Anexo II, item 2, inciso II). As ferramentas nativas dos sistemas operacionais modernos atendem a esse requisito, observadas as considerações de configuração indicadas a seguir.

Na prática, em equipamentos modernos, essa proteção frequentemente já está ativa por padrão ou pode ser habilitada com poucos cliques, sem necessidade de conhecimento técnico avançado:

- **Windows:** verificar em Configurações → Privacidade e Segurança → Criptografia de Dispositivo. Essa opção está disponível em todas as edições do Windows, incluindo a edição Home, desde que o equipamento possua hardware compatível (chip TPM). Em edições Pro ou superior, o *BitLocker* oferece controle adicional sobre quais unidades serão criptografadas.
- **macOS:** em Macs com Apple Silicon (M1/M2/M3 e posteriores) ou chip T2, a criptografia já está ativa por padrão, sem necessidade de configuração. Em modelos anteriores, ativar o *FileVault* em Configurações do Sistema → Privacidade e Segurança → FileVault, seguindo as instruções na tela.
- **Linux:** a ativação do LUKS é mais simples quando realizada durante a instalação do sistema operacional. A maioria das distribuições modernas, como Ubuntu, apresenta a opção de criptografar o disco no próprio assistente de instalação, sem necessidade de linha de comando. Em sistemas já instalados, a configuração é mais complexa e recomenda-se apoio técnico especializado.

Esses mecanismos são amplamente disponíveis e podem ser utilizados sem necessidade de infraestrutura adicional. A recomendação geral é utilizar sempre as soluções já integradas ao sistema operacional do equipamento.

Do ponto de vista do padrão exigido:

- **BitLocker** (Windows Pro/Enterprise): configurar em modo XTS-AES 256 para atender ao padrão mínimo do Provimento; verificar a configuração nas políticas de grupo do sistema ou junto ao responsável técnico de TI;
- **Criptografia de Dispositivo** (Windows Home): verifica junto ao fornecedor do sistema registral se a configuração aplicada atende ao padrão AES-256 exigido;
- **FileVault** (macOS): utiliza AES-128 em modo XTS, considerado tecnicamente equivalente para fins de proteção de disco; aceito pelo Provimento como padrão equivalente;
- **LUKS** (Linux): especificar explicitamente AES-256 durante a configuração, pois o padrão pode variar conforme a distribuição e versão utilizada.

13.3 Gestão de chaves criptográficas e revisão periódica

Sistemas criptográficos utilizam chaves para proteger e acessar os dados cifrados. O Provimento nº 213 exige que a gestão de chaves criptográficas observe controles de acesso restritos, segregação de funções e registro de utilização, conforme política interna formalizada (art. 9º, §3º).

No contexto das serventias, recomenda-se priorizar soluções simples e confiáveis. As práticas mínimas obrigatórias são:

- **guardar a chave de recuperação** em local seguro e separado do equipamento criptografado. A perda da chave implica perda irreversível dos dados;
- **não compartilhar** a chave de recuperação com terceiros sem necessidade justificada;
- **registrar** onde a chave está armazenada no dossiê técnico da serventia;
- para *backups* em nuvem: manter a chave de criptografia sob custódia exclusiva da serventia, nunca delegá-la ao provedor de armazenamento.

Revisão periódica dos padrões criptográficos
O Provimento nº 213 exige revisão periódica dos padrões criptográficos adotados, com substituição obrigatória de protocolos ou algoritmos que se tornem obsoletos ou inseguros (Anexo II, item 2, inciso V; Anexo III, item 4.9, inciso IV).
Na prática, isso significa que a serventia deve verificar periodicamente, ao menos uma vez por ano, se as ferramentas e versões de protocolo utilizadas continuam sendo consideradas seguras pela comunidade técnica especializada, e atualizar sua configuração sempre que necessário.
Algoritmos que já foram depreciados e cujo uso é vedado pelo Provimento incluem: MD5, SHA-1, DES, 3DES, RC4, SSL, TLS 1.0 e TLS 1.1.

13.4 Criptografia de *backups* externos

O art. 9º, §1º, inciso III do Provimento nº 213 estabelece que a criptografia deve ser aplicada também às rotinas de *backup*, especialmente quando envolverem armazenamento externo ou em infraestrutura de terceiros.

Essa exigência é distinta da criptografia de disco descrita na subseção anterior. A criptografia de disco protege os dados no equipamento principal. A criptografia de *backup* protege as cópias de segurança quando elas saem do ambiente controlado da serventia.

Por que criptografar o backup separadamente?
A criptografia de disco protege os dados enquanto estão no equipamento da serventia. Mas quando o *backup* é enviado para um serviço de nuvem ou mídia externa, ele sai desse ambiente protegido.
Se o arquivo de *backup* não for criptografado antes do envio, qualquer pessoa com acesso ao ambiente de armazenamento, incluindo funcionários do provedor de nuvem, em caso de falha de segurança, ou terceiros que obtiverem a mídia física, poderá acessar os dados registrais.
A criptografia aplicada antes do envio (*criptografia na origem*) garante que o provedor de armazenamento receba apenas dados cifrados, sem capacidade de acessar o conteúdo.

Como implementar na prática

A criptografia de *backups* externos deve observar os seguintes requisitos:

- **Padrão mínimo:** AES-256 ou equivalente, conforme exige o Anexo II, item 2, inciso II do Provimento;
- **Momento da criptografia:** aplicada antes do envio para o ambiente externo. O arquivo que chega ao provedor já deve estar cifrado;
- **Custódia da chave:** a chave de descriptografia deve ser mantida sob custódia exclusiva da serventia, nunca entregue ou compartilhada com o provedor de armazenamento;
- **Guarda da chave:** a chave deve ser armazenada em local seguro, separado dos arquivos de *backup*, e sua localização deve ser registrada no dossiê técnico da serventia. A perda da chave implica perda irreversível do acervo;
- **Gestão formal:** o Provimento exige, na Etapa 3 do Anexo IV, inventário atualizado de chaves e certificados, segregação de custódia, controle formal de acesso e política documentada de rotação e renovação periódica.

Opções práticas por classe de serventia

- **Classes 1 e 2:** o Provimento admite o uso de serviços de nuvem comerciais amplamente disponíveis (Google Drive, OneDrive, Amazon S3, Dropbox Business e equivalentes), desde que os arquivos sejam criptografados localmente antes do envio e a chave permaneça com a serventia (Anexo IV, item 3.2.1.1). Ferramentas de *backup* que implementam essa criptografia automaticamente são preferíveis, pois reduzem o risco de erro humano;
- **Classe 3:** recomenda-se solução de *backup* com criptografia integrada, gestão formal de chaves e suporte a políticas de WORM, compatível com os requisitos de RPO de 4 horas e as exigências de gestão de chaves do Anexo IV, item 3.1.

Atenção: criptografia pelo provedor não é suficiente

Muitos serviços de nuvem oferecem "criptografia em repouso" onde os dados são cifrados pelo próprio provedor nos servidores dele. Essa proteção não atende ao requisito do Provimento, pois o provedor detém as chaves e pode, em tese, acessar o conteúdo.
O requisito do Provimento é que a chave fique sob custódia exclusiva da serventia. Portanto, a criptografia deve ser aplicada pela própria serventia, antes do envio, com chave que o provedor não conhece.

14 *Backup*, continuidade operacional e recuperação de desastres

Base normativa no Provimento nº 213: Art. 3º, Art. 6º, e Anexos aplicáveis.

Princípio de proteção do acervo registral

Regra prática: se os dados não puderem ser restaurados, o *backup* não cumpre sua função.
A realização de *backups* é uma das medidas mais importantes para proteger os dados registrais e garantir a continuidade das atividades da serventia em caso de falhas tecnológicas, erros operacionais ou incidentes de segurança.
De forma geral, recomenda-se observar três princípios básicos:

- manter cópias automáticas e regulares dos dados e sistemas utilizados pela serventia;
- armazenar ao menos uma cópia de *backup* em local separado do equipamento principal;
- realizar testes periódicos de restauração para verificar se os dados podem ser recuperados corretamente.

A adoção consistente dessas práticas contribui para assegurar a preservação do acervo registral e a continuidade dos serviços prestados à sociedade.

A preservação do acervo registral é uma das responsabilidades centrais das serventias do Registro Civil.

No ambiente digital, essa preservação depende diretamente da existência de cópias de segurança confiáveis e da capacidade de restaurar os dados em caso de falha, incidente ou desastre.

Falhas de hardware, erros humanos, ataques de *software* malicioso ou eventos físicos

podem causar perda ou indisponibilidade de informações.

Por essa razão, a realização de *backups* regulares e a existência de procedimentos de recuperação são medidas essenciais para garantir a continuidade da prestação dos serviços registrais.

14.1 Importância do *backup*

O *backup* consiste na criação de cópias de segurança dos dados armazenados nos sistemas da serventia.

Essas cópias permitem recuperar informações caso ocorra perda, corrupção ou indisponibilidade dos dados originais.

Todos os sistemas e bases de dados utilizados pela serventia devem estar incluídos nas rotinas de *backup*.

Em especial, recomenda-se incluir nos *backups*:

- bancos de dados do sistema registral;
- documentos digitais e imagens registrais;
- arquivos administrativos relevantes;
- configurações essenciais dos sistemas.

Além da realização regular das cópias de segurança, o Provimento nº 213 exige que os *backups* armazenados externamente ou em infraestrutura de terceiros estejam protegidos por criptografia (art. 9º, §1º, inciso III).

Essa exigência significa que os arquivos de *backup* devem ser cifrados antes do envio para qualquer ambiente externo, serviço de nuvem, servidor remoto ou mídia física transportada fora da serventia, com a chave de descriptografia mantida sob custódia exclusiva da serventia, e não do provedor de armazenamento.

Dessa forma, mesmo que o ambiente de armazenamento externo seja comprometido, os dados permanecem inacessíveis a terceiros não autorizados.

14.2 RTO e RPO (tempo e ponto de recuperação)

RTO e RPO: conceitos e valores obrigatórios por classe

O Provimento nº 213 utiliza dois conceitos fundamentais para medir a capacidade de recuperação dos sistemas das serventias após um incidente.

Recovery Point Objective (RPO) - ponto de recuperação

Indica a quantidade máxima de dados que pode ser perdida entre o último *backup* realizado e o momento em que ocorreu o incidente. Na prática, define com que frequência os *backups* devem ser realizados.

Recovery Time Objective (RTO) - tempo de recuperação

Indica o tempo máximo admissível para restaurar o funcionamento dos sistemas após uma falha ou incidente. Na prática, define quanto tempo a serventia pode permanecer sem acesso ao sistema antes de comprometer a continuidade do serviço.

O Provimento nº 213 não apenas define esses conceitos: ele estabelece valores máximos obrigatórios para cada classe de serventia, previstos no Anexo II, itens 2.1 e 2.2. Esses valores devem constar expressamente do Plano de Continuidade de Negócios (PCN) e

do Plano de Recuperação de Desastres (PRD) da serventia, e sua observância deve ser comprovada por meio de testes documentados de restauração.

A Tabela 7 apresenta os valores máximos estabelecidos pelo Provimento.

Tabela 7: Valores máximos de RPO e RTO por classe de serventia (Anexo II, itens 2.1 e 2.2 do Provimento nº 213).

Classe	RPO máximo	RTO máximo
Classe 3	4 horas (perda máxima admissível de dados)	8 horas (tempo máximo para restabelecimento)
Classe 2	12 horas (perda máxima admissível de dados)	24 horas (tempo máximo para restabelecimento)
Classe 1	24 horas (perda máxima admissível de dados)	24 horas (tempo máximo para restabelecimento; admitida solução simplificada documentada no PCN/PRD)

Como interpretar esses valores na prática
Exemplo para Classe 1 (RPO de 24 horas): se o sistema falhar às 15h de uma segunda-feira, a serventia deve conseguir recuperar todos os dados registrados até, no máximo, as 15h do domingo anterior. Isso significa que um *backup* realizado uma vez por dia, no máximo a cada 24 horas, é o mínimo aceitável.
Exemplo para Classe 3 (RPO de 4 horas): se o sistema falhar às 15h, a serventia deve recuperar dados até, no mínimo, as 11h do mesmo dia. Isso exige *backups* incrementais frequentes ao longo do dia, não apenas uma cópia diária.
Exemplo para Classe 3 (RTO de 8 horas): após uma falha grave, os sistemas devem estar plenamente operacionais em no máximo 8 horas. Isso exige procedimentos de restauração previamente testados e documentados.

Os valores de RPO e RTO não são apenas metas internas da serventia: eles devem ser formalmente definidos no PCN e no PRD e comprovados por meio de testes documentados de restauração, cujos resultados integram o dossiê técnico da serventia e são passíveis de verificação correicional.

O Provimento admite ainda como meta técnica de excelência, para ambientes de maior criticidade, a capacidade de recuperação de dados com defasagem inferior a 30 minutos, quando tecnicamente viável e economicamente proporcional (art. 12, §12).

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

O Provimento nº 213 do Conselho Nacional de Justiça estabelece que as serventias devem possuir diretrizes formais destinadas a assegurar a continuidade da prestação dos serviços registrais em situações de incidente, falha técnica ou interrupção operacional.

Para esse fim, devem ser considerados dois instrumentos complementares de planejamento operacional:

Plano de Continuidade de Negócios (PCN) — documento que descreve os procedimentos organizacionais e operacionais necessários para garantir que a serventia continue

prestando seus serviços essenciais mesmo diante de eventos adversos, como falhas de energia, indisponibilidade de sistemas, incidentes de segurança ou desastres naturais.

Plano de Recuperação de Desastres (PRD) — conjunto de procedimentos técnicos destinados à restauração da infraestrutura tecnológica e dos dados da serventia após incidentes graves que comprometam a operação normal dos sistemas.

Na prática, para a maioria das serventias, esses planos podem ser estruturados de forma simples, contemplando pelo menos os seguintes elementos:

- identificação dos sistemas críticos utilizados pela serventia;
- definição de responsáveis pela recuperação dos sistemas;
- localização e forma de acesso aos backups;
- procedimentos básicos de restauração dos dados;
- estimativa de tempo máximo para retomada das operações (RTO);
- estimativa de perda máxima aceitável de dados (RPO).

Para serventias de menor porte, é admissível que essas informações estejam organizadas em um documento simplificado integrado ao dossiê técnico de conformidade.

O objetivo principal desses planos não é criar documentação complexa, mas assegurar que a serventia possua procedimentos claros para restaurar suas operações e preservar a integridade do acervo registral em caso de incidentes.

14.4 *Backup* automático e periodicidades obrigatórias

Backups realizados manualmente dependem da disciplina operacional dos usuários e podem ser esquecidos ou executados de forma irregular. Por esse motivo, o Provimento exige que as rotinas de cópia de segurança sejam automatizadas e monitoradas (art. 12, §2º; Anexo IV, itens 3.2 e 3.3).

O Provimento distingue dois tipos de cópia obrigatórios, que devem ser implementados de forma complementar:

- ***Backup* completo:** cópia integral de todos os dados críticos, realizada com periodicidade máxima definida por classe (Anexo IV, item 3.2, inciso I):
  - Classe 3: intervalo máximo de **24 horas**;
  - Classe 2: intervalo máximo de **48 horas**;
  - Classe 1: intervalo máximo de **72 horas** (admitida solução equivalente que assegure o RPO de 24 h).
- ***Backup* incremental:** cópias das alterações ocorridas desde o último *backup*, realizadas com frequência suficiente para que a perda de dados não exceda o RPO definido para a classe. Para Classe 3 (RPO de 4 h), cópias incrementais várias vezes ao dia são indispensáveis.

Backup completo não é o mesmo que atender ao RPO
O intervalo do *backup* completo define a frequência da cópia integral, mas o RPO é atendido pelos *backups* incrementais. Uma serventia de Classe 3 com *backup* completo diário mas sem incrementais não atende ao RPO de 4 horas.

Além da execução das rotinas, o Provimento exige monitoramento ativo e contínuo (art. 12, §10; Anexo IV, item 3.3): qualquer falha detectada deve gerar imediatamente (i) alerta técnico automático ao responsável e (ii) registro formal do incidente com abertura

de chamado para análise e correção.

Na prática, recomenda-se:

- configurar notificações automáticas de sucesso e falha das rotinas de *backup*;
- verificar periodicamente os registros de execução;
- incluir o monitoramento de *backup* na rotina de checagem operacional da serventia.

14.5 Dois ambientes independentes de armazenamento

Manter os *backups* no mesmo equipamento ou no mesmo ambiente onde estão os dados originais é insuficiente. Incidentes como incêndio, furto, falha grave de *hardware* ou *ransomware* podem comprometer simultaneamente os dados principais e suas cópias.

O Provimento nº 213 exige que os *backups* sejam armazenados em pelo menos dois ambientes tecnicamente independentes, com redundância geográfica ou lógica equivalente (Anexo IV, item 3.2, inciso III).

As arquiteturas admitidas pelo Provimento incluem:

- **Nuvem com redundância geográfica e imutabilidade:** serviço de nuvem que replique os dados automaticamente em regiões distintas e implemente política de WORM ou versionamento bloqueado, impedindo a exclusão ou alteração dos *backups* por período definido;
- **Mídia física off-site:** dispositivo de armazenamento externo mantido em local fisicamente separado das instalações principais da serventia, como HD externo guardado em outro imóvel ou cofre externo;
- **Solução híbrida:** combinação de armazenamento local redundante com replicação para ambiente externo, como um servidor local mais um serviço de nuvem.

Regra simplificada para Classes 1 e 2
O Provimento admite, para serventias das Classes 1 e 2, o uso de serviços de nuvem comerciais amplamente disponíveis como segundo ambiente de armazenamento, desde que os *backups* sejam criptografados antes do envio (*criptografia na origem*), com a chave de descriptografia mantida sob custódia exclusiva da serventia, e não do provedor de nuvem (Anexo IV, item 3.2.1.1).
Na prática: criptografar o arquivo de *backup* localmente antes de enviá-lo para Google Drive, OneDrive, Amazon S3 ou serviço equivalente. O provedor armazena apenas dados cifrados, sem acesso ao conteúdo.

14.6 Proteção dos *backups* contra *ransomware*

Um dos riscos mais sérios para o acervo registral digital é o *ransomware*, um tipo de *software* malicioso que criptografa todos os arquivos acessíveis na rede, tornando-os inutilizáveis e frequentemente alcançando também os *backups* conectados ao mesmo ambiente.

O Provimento nº 213 exige expressamente que ao menos um dos ambientes de *backup* esteja protegido contra criptografia maliciosa, exclusão indevida ou comprometimento sistêmico simultâneo (Anexo IV, item 3.2, inciso III, alínea d).

Na prática, essa proteção pode ser implementada por meio de um ou mais dos seguintes mecanismos:

- **Bloqueio de retenção (WORM - *Write Once, Read Many*):** mecanismo que impede a modificação ou exclusão dos arquivos de *backup* durante um período definido, mesmo por usuários com privilégios administrativos. Disponível em serviços de nuvem como *Amazon S3 Object Lock*, *Azure Immutable Blob Storage* e equivalentes, bem como em algumas soluções de *backup* locais;
- **Versionamento bloqueado:** configuração que mantém versões anteriores dos arquivos mesmo após tentativas de substituição ou exclusão, permitindo recuperar versões íntegras anteriores ao ataque;
- **Isolamento lógico (air gap lógico):** ambiente de *backup* sem conexão permanente com a rede da serventia, acessível apenas por processo controlado e autenticado, impedindo que um ataque de *ransomware* que comprometa a rede alcance automaticamente as cópias de segurança;
- **Controle de acesso reforçado:** credenciais exclusivas e separadas para o ambiente de *backup*, diferentes das credenciais administrativas do sistema principal, com MFA obrigatória, de forma que o comprometimento das credenciais principais não implique automaticamente o acesso aos *backups*.

Atenção: backup conectado não protege contra ransomware

Um *backup* armazenado em HD externo permanentemente conectado ao computador, ou em pasta de rede continuamente acessível, não oferece proteção contra *ransomware*. O *malware* alcança e criptografa todos os arquivos acessíveis no momento do ataque, incluindo os *backups* conectados.
A proteção efetiva exige que ao menos uma cópia esteja em ambiente que o *ransomware* não consiga alcançar ou modificar diretamente, seja por isolamento físico, isolamento lógico ou mecanismo de imutabilidade.

O monitoramento ativo das rotinas de *backup* é igualmente obrigatório: o Provimento exige alertas automáticos e registro formal de falhas nas rotinas de cópia de segurança (Anexo IV, item 3.3). Qualquer falha detectada deve gerar alerta técnico imediato ao responsável e registro formal do incidente.

14.7 Teste de restauração

A existência de *backups* não garante, por si só, que os dados possam ser recuperados.

Arquivos podem estar corrompidos ou o processo de recuperação pode não funcionar corretamente.

Por esse motivo, recomenda-se realizar testes periódicos de restauração.

Na prática, esses testes consistem em:

- selecionar um conjunto de dados ou arquivos de *backup*;
- executar o procedimento de restauração;
- verificar se os dados restaurados estão íntegros e utilizáveis.

Recomenda-se realizar testes de restauração algumas vezes por ano e registrar a realização desses procedimentos.

14.8 Plano simples de continuidade

Mesmo com boas práticas de segurança, incidentes podem ocorrer.

Por esse motivo, é importante que a serventia possua um procedimento básico que descreva como restaurar os sistemas e retomar a operação após um incidente tecnológico.

Esse procedimento pode incluir:

- identificação dos sistemas essenciais para o funcionamento da serventia;
- localização das cópias de *backup*;
- responsáveis técnicos pelo processo de recuperação;
- passos básicos para restaurar os sistemas e retomar as atividades.

Não é necessário um plano complexo de continuidade operacional. O objetivo é garantir que a serventia saiba como agir para restaurar os sistemas e preservar a continuidade dos serviços prestados à população.

15 Registro de eventos e auditoria

Base normativa no Provimento nº 213: Art. 10.

Princípio de rastreabilidade das operações

Regra básica: deve ser possível identificar quem realizou cada operação relevante nos sistemas da serventia.
Os sistemas utilizados pela serventia devem manter registros de eventos relevantes relacionados ao funcionamento dos sistemas e às operações realizadas pelos usuários.
Esses registros, normalmente chamados de *logs*, permitem identificar quando determinadas ações foram realizadas, por qual usuário e em qual sistema.
A manutenção organizada desses registros contribui para a rastreabilidade das atividades, facilita a investigação de incidentes de segurança e apoia eventuais processos de auditoria ou fiscalização.

Os sistemas informatizados utilizados pelas serventias registram automaticamente diversas atividades realizadas pelos usuários. Esses registros, conhecidos como *logs*, são fundamentais para garantir rastreabilidade, transparência e segurança no uso dos sistemas.

Os logs permitem identificar quem acessou um sistema, quais operações foram realizadas e quando essas ações ocorreram. Em caso de erro operacional, incidente de segurança ou questionamento administrativo, esses registros ajudam a reconstruir os acontecimentos e a identificar sua origem.

O Provimento nº 213 prevê a necessidade de manter registros de eventos relevantes relacionados ao funcionamento dos sistemas e ao acesso às informações registrais.

15.1 Importância dos registros de eventos

Os registros de eventos desempenham papel essencial na segurança da informação e na governança dos sistemas utilizados pelas serventias.

Entre seus principais objetivos estão:

- permitir a identificação dos usuários que acessaram os sistemas;
- registrar operações relevantes realizadas nos sistemas registrais;
- detectar comportamentos anormais ou tentativas de acesso indevido;

- apoiar auditorias e verificações administrativas;
- auxiliar na investigação de incidentes tecnológicos.

A existência de logs confiáveis contribui para aumentar a transparência e a responsabilização das ações realizadas no ambiente digital da serventia.

15.2 O que deve ser registrado

Nem todas as atividades realizadas nos sistemas precisam ser registradas em detalhe. Entretanto, algumas operações são especialmente relevantes para fins de segurança e auditoria.

Entre os eventos que normalmente devem ser registrados estão:

- tentativas de login bem-sucedidas ou malsucedidas;
- acessos administrativos aos sistemas;
- inclusão, alteração ou exclusão de registros relevantes;
- mudanças de configurações importantes nos sistemas;
- operações críticas relacionadas ao acervo registral.

Em sistemas que utilizam mecanismos de autenticação federada, como o IdRC, os registros de autenticação também contribuem para identificar de forma confiável os usuários que acessaram os sistemas.

Na maioria dos sistemas registrais modernos, esses registros já são gerados automaticamente.

15.3 Armazenamento e retenção de *logs*

Atenção: prazo mínimo obrigatório de retenção

O Provimento nº 213 estabelece prazo mínimo obrigatório de 5 (cinco) anos para retenção das trilhas de auditoria (Anexo II, item 3, inciso IV). Esse prazo é vinculante para todas as classes de serventias e não pode ser reduzido por política interna.

Os registros de eventos devem ser mantidos pelo prazo mínimo de 5 (cinco) anos, conforme exigido pelo Provimento nº 213 (Anexo II, item 3, inciso IV), sem prejuízo de prazo superior exigido por norma específica ou por determinação da Corregedoria competente.

Além da retenção pelo prazo adequado, o Provimento estabelece requisitos de qualidade e proteção dos registros (art. 10, §1º; Anexo II, item 3):

- **Proteção contra adulteração:** os *logs* devem ser protegidos contra alteração e exclusão não autorizada, mantidos com mecanismos que permitam verificar sua integridade;
- **Identificação precisa:** cada registro deve identificar inequivocamente o usuário, a data, a hora e o tipo de operação realizada;
- **Sincronização de tempo:** os sistemas devem utilizar fonte de tempo confiável (NTP ou equivalente) para garantir que os registros reflitam o horário correto das operações. Registros com horário incorreto comprometem investigações e auditorias (Anexo II, item 3, inciso III);
- **Proteção contra perda acidental:** os registros devem ser incluídos nas rotinas

de *backup* da serventia, assegurando sua preservação em caso de falha de sistema.

15.3.1 Níveis mínimos de auditoria por classe

O art. 10, §§3º a 5º do Provimento define quatro níveis técnicos de trilha de auditoria e estabelece o mínimo exigido por classe:

- **Nível Essencial** (mínimo para Classes 1 e 2): registro de autenticação de usuários, operações principais e eventos de erro relevantes;
- **Nível Intermediário** (mínimo para Classe 3): inclui, adicionalmente, alterações cadastrais, exportações de dados e tentativas de acesso não autorizado;
- **Nível Ampliado** e **Nível Avançado**: podem ser exigidos para a Classe 3 mediante justificativa técnica fundada na criticidade das operações.

Na prática, a maioria dos sistemas registrais modernos já gera automaticamente registros compatíveis com o Nível Essencial. Para verificar se o sistema utilizado atende ao nível exigido para a classe da serventia, recomenda-se consultar o fornecedor do sistema registral.

O objetivo não é armazenar volumes excessivos de informação, mas garantir que eventos relevantes possam ser analisados e preservados pelo prazo mínimo de 5 anos, com integridade verificável.

15.3.2 Imutabilidade, sincronização e integração com backup

Além da retenção pelo prazo adequado e do nível técnico exigido por classe, o Provimento estabelece três requisitos adicionais que são verificados na Etapa 4 por meio de relatório de conformidade (Anexo IV, item 4.1):

- **Imutabilidade:** os registros de *log* devem ser protegidos contra alteração, substituição ou exclusão não autorizada por mecanismos técnicos verificáveis. Não basta que o sistema declare que os *logs* são protegidos: é preciso demonstrar, de forma objetiva, que o conteúdo registrado não pode ser modificado sem geração de evidência auditável;
- **Sincronização de tempo:** todos os sistemas que geram registros de auditoria devem utilizar fonte de tempo confiável (NTP ou equivalente). Registros com horário incorreto comprometem investigações e auditorias, podendo invalidar evidências;
- **Integração com *backup* e recuperação:** as trilhas de auditoria devem estar incluídas nas rotinas de *backup* da serventia, assegurando que possam ser recuperadas em caso de falha de sistema. A recuperação dos *logs* deve ser testada juntamente com a restauração dos demais dados críticos.

O que o relatório de conformidade de auditoria deve atestar

O relatório de conformidade exigido pela Etapa 4 (Anexo IV, item 4.1) deve atestar, cumulativamente:

- que os registros identificam inequivocamente o usuário, a data, a hora e o tipo de operação;
- que o tempo está sincronizado por fonte confiável;
- que os registros são imutáveis e não apenas que "voltam", mas que não podem ser alterados sem rastro;
- que a retenção mínima de 5 anos está assegurada; e
- que os *logs* estão integrados às rotinas de *backup* e podem ser recuperados.

15.4 Análise básica de eventos

Além de manter registros, é recomendável que a serventia realize verificações periódicas simples para identificar eventuais problemas ou comportamentos incomuns nos sistemas.

Essas verificações podem incluir:

- análise de tentativas repetidas de login malsucedidas;
- verificação de acessos administrativos fora do horário habitual;
- revisão de alterações relevantes realizadas nos sistemas.

Na maioria dos casos, essa verificação pode ser realizada com apoio do fornecedor do sistema registral ou do responsável técnico de tecnologia da informação da serventia.

A análise periódica de logs contribui para aumentar a segurança operacional e para detectar precocemente possíveis incidentes.

16 Proteção contra malware e manutenção dos sistemas

Base normativa no Provimento nº 213: Art. 8º e Anexos aplicáveis.

Princípio de manutenção e proteção dos sistemas

Regra prática: sistemas desatualizados ou sem proteção contra malware representam um dos principais riscos de segurança para os dados registrais.
A segurança dos sistemas utilizados pela serventia depende, em grande medida, da manutenção adequada dos equipamentos e dos programas utilizados no ambiente tecnológico.
Para reduzir riscos de incidentes de segurança, recomenda-se manter os sistemas operacionais e aplicativos sempre atualizados, utilizar mecanismos de proteção contra *software* malicioso (*malware*) e restringir a instalação de programas não autorizados nos computadores da unidade.
Essas medidas simples contribuem para prevenir infecções por vírus, *ransomware* e outros tipos de ataques que podem comprometer os dados e o funcionamento dos sistemas registrais.

Os sistemas utilizados pelas serventias do Registro Civil operam em ambiente digital conectado à internet e, portanto, estão expostos a diferentes tipos de ameaças tecnológicas.

Entre essas ameaças estão softwares maliciosos (*malware*), como vírus, trojans, *ransomware* e outros programas que podem comprometer a integridade dos dados ou interromper o funcionamento dos sistemas.

A adoção de medidas básicas de proteção e manutenção dos sistemas contribui significativamente para reduzir esses riscos.

16.1 Proteção contra *software* malicioso

Softwares maliciosos podem ser introduzidos nos computadores por diferentes meios, como anexos de e-mail, downloads de arquivos desconhecidos ou dispositivos externos contaminados.

Para reduzir esse risco, recomenda-se que os computadores da serventia utilizem soluções de proteção contra malware integradas ao sistema operacional ou fornecidas por fabricantes confiáveis.

Entre as práticas recomendadas estão:

- manter ativo o sistema de proteção contra vírus e malware;
- atualizar regularmente as bases de detecção de ameaças;
- evitar a instalação de programas de origem desconhecida;
- restringir o uso de dispositivos externos não confiáveis.

Nos sistemas operacionais modernos, como Windows, macOS e diversas distribuições Linux, já existem mecanismos nativos de proteção que oferecem níveis adequados de segurança quando mantidos atualizados.

16.2 Atualizações de segurança

Uma das formas mais eficazes de reduzir vulnerabilidades tecnológicas é manter os sistemas atualizados.

Fabricantes de sistemas operacionais e aplicativos publicam regularmente atualizações que corrigem falhas de segurança descobertas ao longo do tempo.

Por esse motivo, recomenda-se:

- manter habilitadas as atualizações automáticas do sistema operacional;
- atualizar navegadores e aplicativos utilizados no cartório;
- aplicar atualizações de segurança fornecidas pelo fornecedor do sistema registral;
- substituir softwares que não recebem mais suporte técnico.

A manutenção regular dos sistemas reduz significativamente a exposição a vulnerabilidades conhecidas.

16.3 Boas práticas operacionais

Além das medidas técnicas, algumas práticas operacionais simples contribuem para aumentar a segurança dos computadores utilizados pela serventia.

Entre essas práticas destacam-se:

- evitar abrir anexos de e-mail de origem desconhecida;
- não instalar programas sem necessidade operacional;
- manter os computadores organizados e sob controle da serventia;

- restringir privilégios administrativos apenas a usuários autorizados.

Essas medidas ajudam a prevenir incidentes comuns relacionados ao uso cotidiano dos sistemas.

A combinação de atualizações regulares, proteção contra malware e boas práticas operacionais constitui uma das formas mais eficazes de reduzir riscos tecnológicos no ambiente da serventia.

16.4 Gestão formal de vulnerabilidades

O Provimento nº 213 exige que as serventias mantenham procedimento documentado de gestão de vulnerabilidades, não apenas a aplicação eventual de atualizações (Anexo II, item 5; Anexo IV, item 4.3).

Os requisitos mínimos são:

- **Atualização periódica documentada:** instituir rotina formal de verificação e aplicação de atualizações de sistemas e aplicações, com registro das providências adotadas (Anexo IV, item 4.2);
- **Prazos máximos de tratamento:**
  - vulnerabilidades classificadas como **críticas**: tratamento em prazo máximo de **30 dias**, quando inexistente evidência de exploração ativa;
  - vulnerabilidades com **exploração ativa ou risco iminente**: medidas de contenção imediatas, preferencialmente em até **72 horas**, com registro formal das providências, inclusive das medidas mitigatórias aplicadas durante a janela de correção (Anexo II, item 5, incisos II e III);
- **Registro formal e auditável:** todas as vulnerabilidades identificadas, suas classificações de risco, as providências adotadas e as datas de encerramento devem ser registradas no dossiê técnico da serventia (art. 11, §4º);
- **Integração com a Política de Segurança:** as diretrizes estratégicas de gestão de vulnerabilidades devem constar da Política Interna de Segurança da Informação, sendo vedada qualquer disposição interna que reduza os prazos mínimos estabelecidos no Anexo II (Anexo III, item 4.7).

16.5 Simulação anual de desastre

Além dos testes de restauração de *backup*, o Provimento exige simulações anuais de cenários de desastre para validação do PCN e do PRD (Anexo II, item 6, inciso II; Anexo IV, item 4.4). Essa simulação deve ser realizada por todas as classes de serventias.

O objetivo é verificar, na prática, se os procedimentos documentados no PCN e no PRD funcionam conforme planejado em caso de incidente grave, como falha total de sistema, incêndio ou ataque de *ransomware*.

A simulação deve:

- reproduzir, em ambiente controlado, um cenário de indisponibilidade relevante dos sistemas ou dos dados;
- verificar se o RTO e o RPO definidos para a classe são efetivamente atingíveis;
- identificar falhas, lacunas ou etapas não documentadas nos planos vigentes;
- resultar em relatório formal com os resultados obtidos e, quando necessário, plano de correção.

Os resultados devem integrar o dossiê técnico da serventia e ser utilizados para atualizar o PCN e o PRD.

16.6 Análise de causa raiz e lições aprendidas

O Provimento exige que todos os incidentes de segurança sejam objeto de análise formal de causa raiz e de registro das medidas corretivas adotadas (art. 11, §2º; Anexo IV, item 4.8).

Essa exigência aplica-se a todos os incidentes, independentemente da gravidade, e não apenas aos classificados como críticos.

Na prática, para cada incidente a serventia deve documentar:

- descrição do incidente e data de ocorrência;
- classificação de gravidade (crítico, alto, médio, baixo);
- identificação da causa raiz;
- medidas de contenção adotadas de imediato;
- medidas corretivas implementadas para evitar reincidência;
- lições aprendidas relevantes para aprimoramento dos procedimentos de segurança;
- data de encerramento do tratamento.

O registro dessas informações contribui para o aprimoramento contínuo das práticas de segurança da serventia e é verificado pela Corregedoria nas fiscalizações correicionais.

16.7 Teste de intrusão (*pentest*) - obrigatório para Classe 3

Atenção: requisito obrigatório para Classe 3

O Provimento nº 213 exige que as serventias classificadas como Classe 3 realizem teste de intrusão (*pentest*) ou metodologia técnica equivalente, com periodicidade mínima de a cada 2 (dois) anos (Anexo II, item 6, inciso IV; Anexo IV, item 4.7).
Esse requisito integra a Etapa 4 do Anexo IV, cujo prazo máximo de conclusão para a Classe 3 é de 24 meses a partir da publicação do Provimento.

O teste de intrusão (*pentest*) é uma avaliação técnica de segurança realizada por profissional especializado, que simula tentativas de acesso não autorizado aos sistemas da serventia com o objetivo de identificar vulnerabilidades antes que possam ser exploradas por agentes maliciosos.

16.7.1 Quando o *pentest* é obrigatório

Para as serventias de Classe 3, o teste deve ser realizado:

- **A cada 2 anos**, como periodicidade mínima regular;
- **Adicionalmente**, sempre que houver alteração relevante de infraestrutura, arquitetura, exposição de serviços à internet ou substituição de fornecedor crítico (Anexo II, item 6, inciso IV);
- Com periodicidade reduzida quando a análise de risco do PCN/PRD indicar aumento relevante de superfície de ataque.

16.7.2 Hipóteses de dispensa ou simplificação

O Provimento reconhece situações em que o teste de intrusão individual pode ser substituído ou simplificado (Anexo II, itens 6.1 a 6.3):

- **Solução centralizada ou compartilhada:** quando a serventia utiliza plataforma tecnológica mantida por entidade representativa, operador nacional ou fornecedor único, o requisito pode ser comprovado mediante relatório técnico coletivo que abranja o ambiente efetivamente utilizado, desde que contenha escopo, metodologia, data, resultados e plano de correção (Anexo II, item 6.1);
- **Ambiente integralmente SaaS:** serventias de Classe 3 que operem integralmente em ambiente de solução contratada (SaaS) ou centralizada, sem servidores de aplicação locais, ficam dispensadas da contratação individual de *pentest*, considerando-se o requisito atendido mediante: (i) relatório técnico de segurança fornecido pela empresa desenvolvedora da solução central; e (ii) declaração do titular, sob as penas da lei, de que as estações locais possuem sistema operacional com suporte ativo, antivírus atualizado e firewall habilitado (Anexo II, item 6.3);
- **Ambiente SaaS com componentes locais:** quando houver componentes locais relevantes, exige-se varredura de vulnerabilidades (*scanner*) e validação de configuração de borda, sem necessidade de novo teste completo, salvo se a análise de risco do PCN/PRD indicar superfície de ataque local relevante (Anexo II, item 6.2).

16.7.3 O que o *pentest* deve demonstrar

O resultado do teste deve integrar o dossiê técnico da serventia e conter, minimamente:

- descrição do escopo e da metodologia aplicada;
- data de execução e identificação do responsável técnico;
- resultados obtidos e vulnerabilidades identificadas;
- plano de correção das vulnerabilidades detectadas;
- declaração de aderência assinada pelo responsável técnico, quando realizado coletivamente.

As vulnerabilidades classificadas como críticas identificadas no *pentest* devem ser tratadas em prazo máximo de 30 dias; em caso de exploração ativa ou risco iminente, as medidas de contenção devem ser adotadas preferencialmente em até 72 horas (Anexo II, item 5, incisos II e III).

17 Interoperabilidade, portabilidade e governança evolutiva

Base normativa no Provimento nº 213: Art. 8º e Art. 6º, III.

Etapa 5: requisitos de longo prazo, mas que devem ser planejados desde já

Os requisitos da Etapa 5 possuem os prazos máximos de implementação mais longos (24, 30 ou 36 meses conforme a classe), mas envolvem negociação contratual e planejamento de médio prazo. As cláusulas de reversibilidade e portabilidade devem ser incorporadas já na **Etapa 1**, na revisão dos contratos com fornecedores (Anexo IV, item 1.4).

17.1 Padrões abertos e neutralidade tecnológica

O Provimento nº 213 exige que os sistemas registrais e os documentos produzidos pelas serventias adotem formatos interoperáveis e neutros do ponto de vista tecnológico (art. 14; Anexo IV, item 5.1).

Na prática, isso significa:

- **Documentos registrais digitais:** devem ser produzidos e armazenados em formatos abertos e de longa duração, preferencialmente PDF/A (ISO 19005) para documentos textuais e XML para dados estruturados;
- **Integração com plataformas de fiscalização:** os sistemas devem estar aptos a exportar dados para as plataformas eletrônicas de fiscalização da Corregedoria Nacional e dos Tribunais de Justiça, quando exigido (Anexo IV, item 5.1);
- **Vedação à dependência exclusiva de formatos proprietários:** o acervo registral digital não pode ficar preso a formato que impeça a migração para outro sistema ou a entrega ao sucessor da delegação;
- **APIs e protocolos documentados:** contratos com fornecedores devem especificar os formatos e protocolos de exportação de dados, garantindo que a serventia possa obter seu acervo em formato legível e reutilizável a qualquer tempo.

17.2 Reversibilidade e portabilidade do acervo

Atenção: cláusulas contratuais obrigatórias
O art. 15 do Provimento exige que os contratos com fornecedores de sistemas registrais contenham expressamente cláusulas de reversibilidade e portabilidade. A ausência dessas cláusulas constitui inadimplência contratual e pode configurar descumprimento normativo. Serventias que não possuam essas cláusulas em contratos vigentes devem incluí-las na primeira oportunidade de renovação ou aditamento.

O Provimento estabelece que o acervo registral digital pertence ao serviço público e não ao fornecedor do sistema. Por isso, os contratos com fornecedores devem garantir (art. 15; Anexo III, item 4.5; Anexo IV, item 1.4):

- **Portabilidade integral:** direito de obter uma cópia completa do acervo em formato interoperável a qualquer tempo, sem custos adicionais ou necessidade de autorização prévia do fornecedor;
- **Reversibilidade:** ao término do contrato, o fornecedor deve entregar o acervo em formato legível e reutilizável, cooperar com a transição para o novo sistema e não reter dados como instrumento de pressão comercial;
- **Cooperação em transição:** o fornecedor deve prestar suporte técnico durante o período de migração, incluindo conversão de formatos e validação da integridade

dos dados exportados;
- **Confidencialidade e conformidade com LGPD:** o contrato deve conter cláusula de sigilo, indicação do papel do fornecedor como operador de dados pessoais, e compromisso de notificação em caso de incidente (Lei nº 13.709/2018, art. 48);
- **Gestão de incidentes:** compromisso contratual de notificação imediata à serventia em caso de incidente de segurança que afete os dados registrais.

17.3 Simulação de extração do acervo

O Provimento exige que a serventia realize, periodicamente, uma simulação documentada de extração integral do acervo digital (art. 15, §2º; Anexo IV, item 5.3).

O objetivo é verificar, na prática, se a portabilidade garantida contratualmente é tecnicamente realizável.

As periodicidades obrigatórias são:

- **Classe 3:** simulação a cada **24 meses**;
- **Classe 2:** simulação a cada **30 meses**;
- **Classe 1:** simulação a cada **36 meses**.

A simulação deve:

a) exportar a totalidade do acervo registral digital em formato interoperável, conforme previsto no contrato com o fornecedor;
b) verificar a integridade e a completude dos dados exportados, incluindo metadados e imagens digitalizadas;
c) confirmar que os dados exportados são legíveis e reutilizáveis sem dependência do sistema original;
d) registrar data, escopo, responsável, resultado e eventuais falhas identificadas, com plano de correção quando necessário.

O relatório da simulação deve integrar o dossiê técnico da serventia e ser apresentado em eventuais verificações correicionais.

17.4 Capacitação periódica da equipe

O art. 13 do Provimento exige que as serventias promovam capacitação periódica das pessoas que atuam no ambiente tecnológico registral (Anexo IV, item 5.2).

Os registros de capacitação integram a Etapa 5 e são exigidos no dossiê técnico.

Na prática, a capacitação deve:

- abranger os princípios básicos de segurança da informação, proteção de dados pessoais e uso adequado dos sistemas registrais;
- incluir orientações específicas sobre prevenção de *phishing*, uso seguro de credenciais, procedimentos em caso de incidente e comunicação à Corregedoria;
- ser realizada com periodicidade razoável, compatível com o porte da serventia e a rotatividade da equipe. Recomenda-se ao menos uma vez por ano para toda a equipe e sempre que houver ingresso de novo colaborador em função sensível;
- ser registrada formalmente: lista de presença, data, conteúdo abordado e responsável pela condução.

Formas aceitas de capacitação

O Provimento não exige treinamento formal presencial. São aceitas: capacitações promovidas pela Corregedoria ou por entidades de classe (ARPEN, CNB e similares), cursos *online* com certificado, materiais de orientação interna acompanhados de confirmação de ciência pelos colaboradores, e reuniões internas documentadas com pauta e lista de presença. O critério é que haja **registro formal verificável**.

17.5 Manutenção de registros auditáveis por 5 anos

A obrigação de retenção mínima de 5 anos não se aplica apenas aos *logs* de auditoria dos sistemas: ela alcança toda a documentação de conformidade que comprove a adoção das medidas previstas no Provimento (art. 10, §1º; Anexo II, item 3, inciso IV; Anexo IV, item 5.3).

Isso inclui, entre outros:

- registros de testes de restauração de *backup* e simulações de desastre;
- relatórios de *pentest* e de avaliações técnicas de segurança (Classe 3);
- registros de capacitação da equipe;
- relatórios de análise de causa raiz de incidentes;
- registros de simulações de extração do acervo;
- versões anteriores da Política de Segurança e dos planos PCN/PRD, com as respectivas datas de aprovação e revisão.

Todos esses registros devem estar organizados no dossiê técnico e acessíveis para apresentação em inspeções ou correições. Para Classes 2 e 3, o dossiê deve incluir mecanismo de verificação de integridade (*hash* dos arquivos assinado digitalmente pelo responsável técnico, Anexo IV, item IV).

18 Documentação mínima de conformidade

Base normativa no Provimento nº 213: Art. 4º, Art. 6º e Anexos aplicáveis.

Princípio de documentação mínima

Regra prática: se uma medida de segurança foi implementada, deve existir algum registro simples que permita demonstrar sua adoção.
A implementação das medidas de segurança deve ser acompanhada de registros simples que permitam demonstrar a adoção das práticas recomendadas neste guia.
Essa documentação não precisa ser extensa ou complexa, mas deve ser suficiente para indicar quais controles foram implementados, quais procedimentos são adotados pela serventia e quais evidências podem comprovar essas práticas.
A manutenção organizada dessas informações facilita processos de auditoria, fiscalização ou revisão interna das medidas de segurança.
Além disso, o art. 17 do Provimento nº 213 exige que a conclusão de cada etapa de implementação seja declarada formalmente no Sistema Justiça Aberta, plataforma do Conselho Nacional de Justiça. Essa declaração é renovada anualmente e integra o ciclo de conformidade da serventia.

A implementação de medidas de segurança da informação deve ser acompanhada de

documentação mínima que permita demonstrar a adoção dessas práticas pela serventia.

Essa documentação não precisa ser extensa ou tecnicamente complexa. O objetivo é registrar, de forma simples e organizada, quais medidas foram adotadas para atender aos requisitos do Provimento nº 213.

A existência dessa documentação facilita auditorias, verificações administrativas e a própria gestão interna da infraestrutura tecnológica da serventia.

18.1 Objetivo da documentação

A documentação de conformidade tem como finalidade principal registrar as práticas de segurança adotadas pela serventia e permitir que essas práticas sejam verificáveis.

Entre os principais objetivos da documentação estão:

- demonstrar a adoção das medidas de segurança previstas no Provimento nº 213;
- organizar informações sobre a infraestrutura tecnológica da serventia;
- registrar procedimentos operacionais relacionados à segurança dos sistemas;
- facilitar auditorias e verificações realizadas pelas corregedorias ou por outras autoridades competentes.

Essa documentação também contribui para preservar o conhecimento institucional sobre a organização tecnológica da serventia.

18.2 Elementos mínimos do dossiê técnico

Recomenda-se que cada serventia mantenha um pequeno *dossiê técnico de segurança da informação*, contendo informações básicas sobre sua infraestrutura tecnológica e sobre as práticas adotadas para proteger os sistemas e os dados registrais.

Esse dossiê pode incluir, por exemplo:

- identificação da serventia;
- classe de enquadramento econômico;
- descrição resumida da infraestrutura tecnológica;
- lista de sistemas utilizados na atividade registral;
- relação de usuários autorizados a acessar os sistemas;
- descrição das rotinas de *backup*;
- registro de testes de restauração realizados;
- registro de incidentes tecnológicos relevantes;
- confirmação do nível de auditoria adotado e do prazo de retenção dos *logs* (mínimo de 5 anos);
- identificação do responsável técnico pelo suporte tecnológico da serventia.

Essas informações permitem demonstrar que a serventia mantém controle sobre sua infraestrutura tecnológica e adota práticas básicas de segurança.

18.3 Conformidade com LGPD

As serventias do Registro Civil das Pessoas Naturais realizam, no exercício de suas atividades, operações de tratamento de dados pessoais relacionadas à prática de atos registrais, à gestão administrativa e à prestação de serviços ao público.

O Provimento nº 213 do Conselho Nacional de Justiça determina que os responsáveis pelas serventias assegurem conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), adotando medidas técnicas e organizacionais destinadas à proteção das informações tratadas no âmbito da atividade registral.

Nesse contexto, recomenda-se que a serventia mantenha, no âmbito do dossiê técnico de conformidade, pelo menos os seguintes elementos relacionados à proteção de dados pessoais:

- registro simplificado das operações de tratamento de dados realizadas pela serventia, indicando as principais categorias de dados tratados e suas finalidades institucionais;
- descrição das medidas técnicas e organizacionais adotadas para proteção dos dados pessoais, incluindo controles de acesso, criptografia, backup e registro de eventos;
- definição de procedimentos para tratamento de incidentes de segurança que possam comprometer dados pessoais, incluindo comunicação às autoridades competentes quando aplicável;
- identificação do responsável interno pelo acompanhamento das questões relacionadas à proteção de dados, quando aplicável.

Essas medidas não têm por objetivo criar estruturas administrativas complexas, mas assegurar que a serventia possua procedimentos mínimos de proteção das informações pessoais sob sua responsabilidade, em consonância com a legislação vigente e com as diretrizes estabelecidas pelo Provimento nº 213.

18.4 Organização das evidências

As evidências de implementação das medidas de segurança podem ser organizadas em formato digital ou físico, de acordo com a realidade operacional da serventia.

Entre os exemplos de evidências que podem ser mantidas estão:

- registros ou relatórios de execução de *backups*;
- registros de testes de restauração;
- capturas de tela de configurações de segurança;
- listas de usuários cadastrados nos sistemas;
- registros de atualizações realizadas nos sistemas.

O importante é que essas evidências estejam organizadas de forma que possam ser apresentadas quando necessário.

18.5 Declaração de conformidade no Sistema Justiça Aberta

O art. 17 do Provimento nº 213 estabelece uma obrigação formal que vai além da produção do dossiê técnico: a serventia deve declarar, em campo próprio do Sistema Justiça Aberta, o cumprimento de cada etapa prevista no Anexo IV do Provimento.

Essa declaração:

- deve ser registrada ao final de cada etapa concluída, confirmando o cumprimento integral de todos os seus requisitos;
- deve ser renovada anualmente, acompanhada de síntese do dossiê técnico com evidências mínimas de conformidade;
- deve ser firmada pessoalmente pelo titular da delegação, pelo interino ou pelo interventor responsável pela serventia. A responsabilidade é pessoal e intransferível;

- não pode ser parcial, proporcional ou condicionada: a conclusão de uma etapa pressupõe o cumprimento integral de todos os seus itens e a manutenção efetiva dos requisitos já implementados nas etapas anteriores.

Atenção: declaração falsa

O art. 17, §2º do Provimento estabelece que a declaração falsa, objetivamente verificada em inspeções ou correições, sujeita o responsável às penalidades previstas em lei.
Além disso, o art. 24 prevê que o descumprimento injustificado dos requisitos do Provimento, quando caracterizada negligência, imprudência ou omissão relevante, pode ensejar procedimento administrativo disciplinar, sem prejuízo das responsabilidades civis e penais cabíveis.

A relação entre o dossiê técnico e a declaração no Sistema Justiça Aberta é de complementaridade: o dossiê reúne as evidências técnicas que sustentam a declaração. Sem dossiê organizado e atualizado, a serventia não possui base documental suficiente para sustentar a declaração perante uma fiscalização correicional.

18.6 Atualização e revisão periódica da documentação e da política

A documentação de conformidade e a Política de Segurança da Informação devem ser revisadas periodicamente. O Provimento nº 213 estabelece que a revisão é obrigatória, e não meramente recomendável, sempre que ocorrer ao menos uma das seguintes condições (Anexo III, item 4.9, incisos I a IV; Anexo IV, item 5.4):

- **Alteração normativa relevante:** publicação de novo provimento, resolução ou instrução normativa da Corregedoria Nacional ou dos Tribunais de Justiça que impacte os requisitos de segurança, privacidade ou interoperabilidade das serventias;
- **Evolução tecnológica significativa:** mudança de sistema registral, migração de infraestrutura, adoção de novos ambientes em nuvem ou substituição de fornecedor crítico;
- **Incidente de segurança relevante:** qualquer evento que tenha comprometido ou possa comprometer a integridade, disponibilidade ou confidencialidade do acervo, com análise de causa raiz já concluída;
- **Ciclo anual:** independentemente das condições anteriores, a renovação anual da declaração no Sistema Justiça Aberta deve ser acompanhada de revisão formal da documentação de conformidade e verificação de que a Política de Segurança ainda reflete a realidade operacional da serventia.

Os resultados de cada revisão devem ser registrados no dossiê técnico, com indicação da data, do motivo que a determinou, das alterações realizadas e do responsável pela aprovação.

19 Roteiro prático de início imediato

Roteiro operacional para atendimento das Etapas 1 e 2 do Provimento

O Provimento nº 213 organiza a implementação em cinco **Etapas normativas** definidas no Anexo IV, com prazos obrigatórios por classe de serventia.
Para evitar confusão com essa estrutura oficial, o presente guia utiliza a expressão **passos práticos de execução**.
Os passos apresentados nesta seção organizam as ações iniciais necessárias para o cumprimento das **Etapas 1 e 2 do Provimento**, que possuem os prazos mais curtos.

A Figura 8 apresenta, de forma simplificada, o fluxo completo de implementação previsto no Provimento.

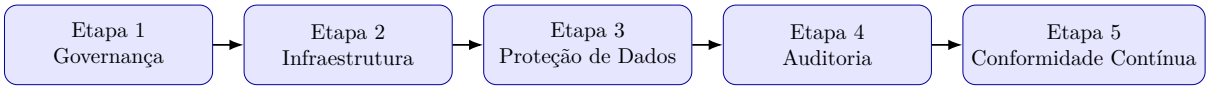


Figura 8: Fluxo simplificado de implementação do Provimento nº 213

A Figura 9 apresenta, de forma didática, a sequência dos passos práticos recomendados para o início imediato da implementação. Esses passos possuem natureza operacional e servem como apoio ao cumprimento das etapas normativas previstas no Provimento nº 213.

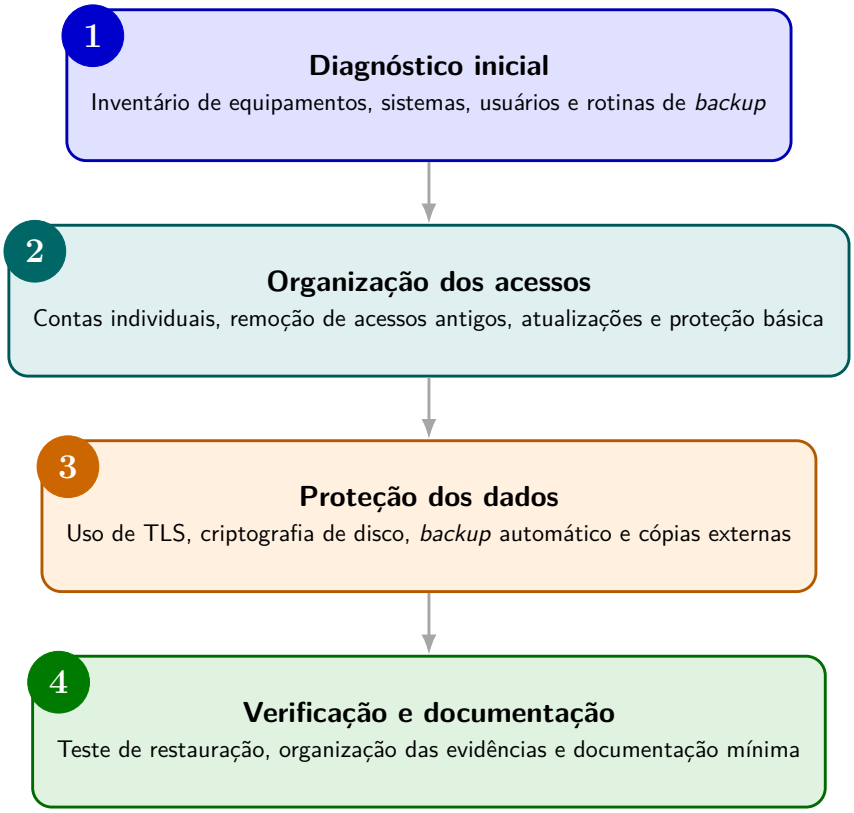


Figura 9: Roteiro prático de início imediato para implementação das medidas prioritárias.

19.1 Passo 1 - Diagnóstico inicial da infraestrutura

O primeiro passo consiste em realizar um levantamento básico da infraestrutura tecnológica da serventia.

a) identificar computadores e servidores utilizados;
b) verificar os sistemas registrais e administrativos em operação;
c) identificar os usuários com acesso aos sistemas;
d) verificar se os sistemas operacionais possuem suporte ativo;
e) identificar a existência de rotinas de *backup*.

Esse diagnóstico inicial permite compreender a situação tecnológica da serventia e preparar a implementação das medidas de segurança.

19.2 Passo 2 - Organização dos acessos e sistemas

Neste passo recomenda-se organizar os mecanismos de acesso aos sistemas e revisar a configuração básica dos equipamentos.

a) garantir contas individuais para cada usuário;
b) remover contas antigas ou não utilizadas;
c) verificar atualização dos sistemas operacionais;
d) ativar mecanismos de proteção contra malware;
e) avaliar a possibilidade de autenticação multifator ou integração com o IdRC.

Essas ações contribuem diretamente para o atendimento dos requisitos da **Etapa 1 do Provimento**.

19.3 Passo 3 - Proteção inicial dos dados

O terceiro passo concentra-se na proteção das informações registrais.

a) verificar o uso de conexões seguras (HTTPS ou TLS);
b) ativar criptografia de disco nos computadores que armazenam dados;
c) configurar rotinas automáticas de *backup*;
d) armazenar cópias de *backup* em ambientes independentes;
e) proteger ao menos um ambiente de *backup* contra *ransomware*.

Essas medidas correspondem aos requisitos iniciais da **Etapa 2 do Provimento**.

19.4 Passo 4 - Verificação e documentação

O último passo consiste em consolidar as medidas adotadas e organizar a documentação mínima de conformidade.

a) realizar teste de restauração de *backup*;
b) revisar registros de eventos dos sistemas;
c) organizar o dossiê técnico de segurança;
d) registrar as medidas de segurança implementadas;
e) definir responsáveis pela manutenção periódica.

Após essas ações, a serventia terá estabelecido uma base mínima de segurança da informação compatível com as etapas iniciais do Provimento.

20 Modelo simplificado de dossiê técnico

Finalidade do dossiê técnico

Ideia central: o dossiê técnico organiza, em um único local, os principais registros que comprovam a adoção das práticas de segurança pela serventia.
O dossiê técnico é um conjunto organizado de informações e registros que documentam as medidas de segurança adotadas pela serventia.
Seu objetivo é reunir, de forma simples e estruturada, as evidências relacionadas à implementação dos controles de tecnologia da informação previstos no Provimento nº 213.
Esse dossiê não precisa ser complexo. Na maioria das serventias, ele pode consistir em um pequeno conjunto de documentos ou registros que permitam demonstrar quais práticas de segurança foram adotadas e como são mantidas pela unidade.

Para facilitar a organização das informações relacionadas à segurança da informação e à infraestrutura tecnológica da serventia, recomenda-se a criação de um *dossiê técnico de segurança da informação*.

Esse dossiê funciona como um repositório organizado de informações e evidências que demonstram a adoção das medidas previstas no Provimento nº 213.

O dossiê não precisa ser um documento complexo. Ele pode ser mantido em formato digital ou físico e deve conter apenas as informações essenciais para compreender como a serventia protege seus sistemas e dados registrais.

20.1 Finalidade do dossiê

O dossiê técnico tem como finalidade registrar de forma simples e organizada as práticas adotadas pela serventia para garantir a segurança de seus sistemas e a proteção do acervo registral.

Entre os principais objetivos do dossiê estão:

- demonstrar a adoção das medidas previstas no Provimento nº 213;
- organizar informações sobre a infraestrutura tecnológica utilizada pela serventia;
- registrar procedimentos operacionais relacionados à segurança da informação;
- facilitar auditorias e verificações realizadas pelas corregedorias ou por outras autoridades competentes.

A existência desse dossiê contribui para a transparência na gestão tecnológica da serventia e facilita a continuidade administrativa em caso de mudança de responsáveis ou de fornecedores técnicos.

20.2 Estrutura mínima recomendada

O dossiê deve ser organizado por etapas do Provimento, de modo que sua estrutura espelhe diretamente os requisitos do Anexo IV e permita verificação correicional eficiente. Os elementos a seguir são obrigatórios ou fortemente recomendados conforme a classe.

1. **Identificação e enquadramento**
   Nome da serventia, município, estado, CNS, identificação do delegatário titular e classe econômica vigente, com referência ao semestre de apuração e data do próximo reenquadramento (Anexo IV, preâmbulo).

2. **Responsáveis formalmente designados**
   Identificação do Responsável de Segurança da Informação (RSI) e, quando aplicável, do Encarregado de Proteção de Dados (DPO/EPD), com data de designação e canal de contato (Anexo IV, item 1.1; art. 7º, §1º).
3. **Política de Segurança da Informação**
   Versão vigente aprovada, data de aprovação, data da última revisão, motivo da revisão e próxima data prevista de revisão. Versões anteriores devem ser retidas por 5 anos (Anexo III; Anexo IV, item 5.4).
4. **Inventário de ativos**
   Relação de equipamentos, sistemas registrais, integrações, contratos com fornecedores, certificados digitais e licenças, com indicação de status e vigência (Anexo IV, item 1.5).
5. **Contratos com fornecedores**
   Confirmação de que os contratos vigentes contêm cláusulas de confidencialidade, conformidade com a LGPD, reversibilidade e portabilidade do acervo, cooperação em transição e gestão de incidentes. Para contratos sem essas cláusulas, registrar data prevista de aditamento (art. 15; Anexo IV, item 1.4).
6. **Documento de arquitetura tecnológica**
   Topologia básica da rede, ambientes utilizados (local, nuvem, híbrido), fluxos de dados críticos, localização dos *backups*, integrações externas relevantes, mecanismos de alta disponibilidade ou redundância (Anexo IV, item 2.7).
7. **Plano de Continuidade de Negócios (PCN) e Plano de Recuperação de Desastres (PRD)**
   Versão vigente com RPO e RTO definidos conforme a classe, identificação de riscos e medidas de mitigação, data da última simulação e resultado. Classe 3: deve incluir mecanismos de alta disponibilidade (Anexo IV, item 2.5).
8. **Gestão de chaves criptográficas**
   Inventário de chaves e certificados com finalidade, algoritmo e datas de criação/expiração; indicação dos responsáveis pela custódia; e registro das últimas operações de rotação ou renovação (Anexo II, item 2, inciso IV; Anexo IV, item 3.1).
9. **Rotinas de *backup***
   Tipo (completo e incremental), periodicidade por tipo, ambientes de armazenamento, mecanismo de proteção anti-*ransomware* adotado e confirmação de criptografia dos *backups* externos com indicação do local de custódia da chave (Anexo IV, item 3.2).
10. **Monitoramento de *backup***
    Confirmação de que alertas automáticos de falha estão configurados e registro dos últimos alertas ou falhas tratadas (Anexo IV, item 3.3).
11. **Testes de restauração de *backup***
    Registro de cada teste com data, escopo, resultado, disponibilidade da chave de descriptografia e responsável. Periodicidade mínima: semestral para Classe 3; anual para Classes 1 e 2 (Anexo IV, item 4.4).
12. **Relatório de conformidade das trilhas de auditoria**
    Atestação de que os *logs* atendem ao nível exigido por classe (Essencial para Classes 1 e 2; Intermediário para Classe 3), são imutáveis, identificam inequivocamente o usuário e a operação, têm tempo sincronizado por fonte confiável (NTP) e estão integrados ao *backup*, com retenção mínima de 5 anos (Anexo IV, item 4.1).
13. **Gestão de vulnerabilidades**

Registro das vulnerabilidades identificadas, classificação de risco, providências adotadas e datas de encerramento. Vulnerabilidades críticas: prazo máximo de 30 dias; exploração ativa: 72 horas (Anexo II, item 5; Anexo IV, item 4.3).

14. **Simulações de desastre**
Registro de cada simulação anual do PCN/PRD: data, cenário simulado, resultado, desvios identificados e plano de correção (Anexo IV, item 4.4).
15. **Registro de incidentes**
Registro de todos os incidentes com: data, descrição, gravidade (crítico/alto/médio/baixo), contenção imediata, análise de causa raiz, medidas corretivas, lições aprendidas e data de encerramento. Para incidentes críticos: registro de comunicação à Corregedoria com data e protocolo (art. 11; Anexo IV, item 4.8).
16. **Teste de intrusão (*pentest*)** - *Classe 3 apenas*
Relatório do último *pentest* com escopo, metodologia, data, responsável, vulnerabilidades encontradas e plano de correção. Periodicidade máxima: 2 anos (Anexo II, item 6; Anexo IV, item 4.7). Hipóteses de dispensa documentadas conforme Seção 16.7.
17. **Capacitação da equipe**
Registros das capacitações realizadas: data, conteúdo, participantes e responsável pela condução. Periodicidade mínima recomendada: anual (Anexo IV, item 5.2).
18. **Padrões abertos e interoperabilidade**
Confirmação dos formatos adotados para armazenamento e exportação do acervo (PDF/A, XML ou equivalente) e integração com plataformas de fiscalização (Anexo IV, item 5.1).
19. **Simulação de extração do acervo**
Registro de cada simulação com data, escopo, resultado, responsável e eventuais falhas: a cada 24 meses (Classe 3), 30 meses (Classe 2) ou 36 meses (Classe 1) (Anexo IV, item 5.3).
20. **Declarações no Sistema Justiça Aberta**
Registro das declarações de conclusão de etapas realizadas, com data, etapa declarada e nome do responsável. Renovação anual obrigatória (art. 17).

Requisito de integridade do dossiê para Classes 2 e 3
Para serventias de Classes 2 e 3, o Anexo IV, item IV exige que o dossiê técnico inclua mecanismo de verificação de integridade: geração de *hash* (preferencialmente SHA-256 ou superior) dos arquivos que compõem o dossiê, assinado digitalmente pelo responsável técnico, guardado em repositório com controle de acesso e registro auditável de alterações. Para Classe 1, admite-se dossiê em formato simplificado sem esse mecanismo, desde que os documentos estejam organizados e acessíveis.

20.3 Atualização, retenção e guarda do dossiê

O dossiê deve ser atualizado sempre que ocorrer qualquer dos seguintes eventos:

- conclusão de etapa do Anexo IV declarada no Sistema Justiça Aberta;
- substituição de equipamentos, sistemas ou fornecedores críticos;
- alteração nas rotinas de *backup*, nos responsáveis designados ou na Política de Segurança;
- ocorrência de incidente de segurança classificado como alto ou crítico;
- realização de teste de restauração, simulação de desastre ou simulação de extração

do acervo;
- renovação anual da declaração no Sistema Justiça Aberta.

Retenção mínima: todos os documentos e registros que integram o dossiê devem ser retidos por prazo mínimo de 5 anos (Anexo II, item 3, inciso IV; Anexo IV, item 5.3). Versões anteriores da Política de Segurança, dos PCN/PRD e dos relatórios de testes devem ser preservadas com indicação da data de vigência.

Guarda: o dossiê deve ser armazenado em repositório com acesso restrito e controlado, distinto do ambiente de produção dos sistemas registrais, e incluído nas rotinas de *backup* da serventia. Para Classes 2 e 3, aplicam-se os requisitos de integridade com *hash* assinado descritos na subseção anterior.

21 *Checklist* final de verificação periódica

Recomendação prática

Utilize este checklist ao menos uma vez por ano.
A verificação periódica dos controles de segurança ajuda a garantir que as medidas adotadas pela serventia permaneçam adequadas ao longo do tempo, especialmente após mudanças na infraestrutura tecnológica, atualizações de sistemas ou alterações na equipe. Essa revisão anual também facilita processos de auditoria e demonstra a manutenção contínua das práticas previstas no Provimento nº 213.

A manutenção das práticas de segurança da informação requer verificações periódicas para garantir que as medidas adotadas continuem sendo aplicadas corretamente.

Mudanças na infraestrutura tecnológica, substituição de equipamentos, atualizações de sistemas ou alterações na equipe podem afetar a configuração de segurança da serventia.

Por esse motivo, recomenda-se que a serventia realize revisões periódicas de seus controles de segurança, utilizando um checklist simples que permita verificar a continuidade das medidas adotadas.

21.1 *Checklist* consolidado dos controles

As tabelas 8, 9, 10, 11 e 12 reúnem os controles de todas as cinco etapas e pode ser utilizada como instrumento de verificação periódica. As colunas indicam a quais classes cada controle se aplica.

21.2 Calendário normativo de obrigações periódicas

A Tabela 13 sintetiza as principais obrigações periódicas decorrentes do Provimento nº 213, com indicação de periodicidade e aplicabilidade por classe.

Além dessas obrigações programadas, lembrar que qualquer incidente de segurança classificado como crítico ou alto dispara imediatamente: (i) comunicação à Corregedoria (máx. 72 h); (ii) abertura de registro formal no dossiê; e (iii) quando envolver dados pessoais, notificação à ANPD (art. 7º, §3º).

Tabela 8: *Checklist* da Etapa 1 - Governança e conformidade legal

Controle verificado	Cl. 1	Cl. 2	Cl. 3	OK
Responsável de Segurança da Informação (RSI) formalmente designado.	Sim	Sim	Sim	☐
Política de Segurança da Informação aprovada, publicada internamente e vigente.	Sim	Sim	Sim	☐
Contas individualizadas implantadas; credenciais compartilhadas eliminadas.	Sim	Sim	Sim	☐
MFA obrigatória para acessos administrativos e sistemas críticos; justificativa técnica para perfis de menor risco no dossiê.	Sim	Sim	Sim	☐
Inventário de ativos, integrações, certificados e contratos atualizado.	Sim	Sim	Sim	☐
Contratos com fornecedores contêm cláusulas de confidencialidade, LGPD, reversibilidade, portabilidade e cooperação em transição.	Sim	Sim	Sim	☐
Procedimento de comunicação de incidentes críticos à Corregedoria (máx. 72 h; meta: 24 h) documentado.	Sim	Sim	Sim	☐
Conclusão da Etapa 1 declarada no Sistema Justiça Aberta.	Sim	Sim	Sim	☐

Tabela 9: *Checklist* da Etapa 2 - Infraestrutura e continuidade operacional.

Controle verificado	Cl. 1	Cl. 2	Cl. 3	OK
Nobreak (UPS) com autonomia mín. 30 min instalado nos equipamentos críticos.	Sim	Sim	Sim	☐
Plano de contingência energética documentado.	Sim	Sim	Sim	☐
Ambiente físico com controle de acesso e proteção contra incêndio/inundação/variação térmica.	Sim	Sim	Sim	☐
Conectividade compatível com a classe: $\geq$2 Mbps (Cl. 1), $\geq$10 Mbps (Cl. 2), $\geq$50 Mbps (Cl. 3).	Sim	Sim	Sim	☐
PCN e PRD formalizados com RPO e RTO da classe.	Sim	Sim	Sim	☐
Proteção de *endpoint* (antivírus/antimalware) ativa em todas as estações e servidores.	Sim	Sim	Sim	☐
Documento de arquitetura tecnológica formalizado (topologia, ambientes, fluxos, *backups*, integrações).	Sim	Sim	Sim	☐
Conclusão das Etapas 1–2 declarada no Sistema Justiça Aberta.	Sim	Sim	Sim	☐

Tabela 10: *Checklist* da Etapa 3 - Proteção do acervo digital.

Controle verificado	Cl. 1	Cl. 2	Cl. 3	OK
Criptografia em repouso AES-256 ativa nos equipamentos com dados registrais.	Sim	Sim	Sim	☐
TLS 1.2+ em todas as comunicações; versões depreciadas desabilitadas.	Sim	Sim	Sim	☐
Firewall stateful com IPS/IDS implantado (não apenas roteador doméstico).	Sim	Sim	Sim	☐
Segmentação de rede: VLANs (Cl. 2 e 3); medida idônea (Cl. 1).	Sim	Sim	Sim	☐
Gestão formal de chaves com inventário, custódia segregada, rotação e registro.	-	Sim	Sim	☐
Backup completo com periodicidade max. 72/48/24 h (Cl. 1/2/3) + incremental compatível com RPO.	Sim	Sim	Sim	☐
Backup em 2 ambientes independentes; ao menos um com proteção WORM/versionamento/*air gap*.	Sim	Sim	Sim	☐
Backups externos criptografados; chave sob custódia exclusiva da serventia.	Sim	Sim	Sim	☐
Monitoramento automático de *backup* com alertas configurados.	Sim	Sim	Sim	☐
Trilhas de auditoria imutáveis implantadas: nível Essencial (Cl. 1/2); Intermediário (Cl. 3).	Sim	Sim	Sim	☐

Tabela 11: *Checklist* da Etapa 4 - Monitoramento, auditoria e validação.

Controle verificado	Cl. 1	Cl. 2	Cl. 3	OK
Relatório de conformidade das trilhas de auditoria emitido (imutabilidade, NTP, retenção 5 anos, integração com *backup*).	Sim	Sim	Sim	☐
Rotina documentada de atualização periódica de sistemas e aplicações.	Sim	Sim	Sim	☐
Gestão formal de vulnerabilidades: críticas ≤30 dias; exploração ativa ≤72 h.	Sim	Sim	Sim	☐
Simulação anual de desastre realizada e documentada.	Sim	Sim	Sim	☐
Testes de restauração de *backup* documentados: semestral (Cl. 3); anual (Cl. 1/2).	Sim	Sim	Sim	☐
Análise de causa raiz e lições aprendidas documentadas para todos os incidentes.	Sim	Sim	Sim	☐
Pentest ou equivalente realizado a cada 2 anos. Ver dispensa SaaS (Seção 16.7).	-	-	Sim	☐

Tabela 12: *Checklist* da Etapa 5 - Interoperabilidade e governança evolutiva.

Controle verificado	Cl. 1	Cl. 2	Cl. 3	OK
Sistemas integrados a plataformas de fiscalização; formatos abertos (PDF/A, XML) adotados.	Sim	Sim	Sim	☐
Capacitação periódica da equipe realizada com registro formal.	Sim	Sim	Sim	☐
Registros do dossiê retidos por mínimo de 5 anos.	Sim	Sim	Sim	☐
Plano de reversibilidade/portabilidade formalizado; simulação de extração do acervo realizada: a cada 36/30/24 meses (Cl. 1/2/3).	Sim	Sim	Sim	☐
Política de Segurança revisada após alteração normativa, incidente relevante ou ciclo anual.	Sim	Sim	Sim	☐
Declaração de conclusão integral registrada no Sistema Justiça Aberta; dossiê atualizado.	Sim	Sim	Sim	☐

Tabela 13: Calendário de obrigações periódicas por classe (Provimento nº 213).

Obrigação	Base normativa	Cl. 1	Cl. 2	Cl. 3
Declaração no Sistema Justiça Aberta	art. 17	Anual	Anual	Anual
Renovação do enquadramento econômico	art. 16, §1º	Anual	Anual	Anual
Revisão da Política de Segurança (ciclo mínimo)	Anexo III; Anexo IV, item 5.4	Anual	Anual	Anual
Revisão da lista de usuários autorizados	Anexo II, item 1	Anual	Anual	Anual
Capacitação da equipe	Anexo IV, item 5.2	Anual	Anual	Anual
Atualização do inventário de ativos e contratos	Anexo IV, item 1.5	Anual	Anual	Anual
Simulação anual de desastre (PCN/PRD)	Anexo II, item 6, inc. II	Anual	Anual	Anual
Teste de restauração de *backup*	Anexo IV, item 4.4	Anual	Anual	Semestral
Rotação de chaves criptográficas (conforme política)	Anexo II, item 2, inc. IV	-	Anual	Anual
Pentest ou metodologia equivalente	Anexo II, item 6, inc. IV	-	-	Bienal
Simulação de extração integral do acervo	Anexo IV, item 5.3	36 meses	30 meses	24 meses
Reenquadramento: correção dos limites pelo IPCA	art. 16, §2º	Anual	Anual	Anual

22 Considerações finais

Mensagem final

A adoção das medidas apresentadas neste guia contribui para fortalecer a segurança dos sistemas utilizados pelas serventias e para proteger o acervo registral sob sua responsabilidade.
A implementação dessas práticas não exige soluções tecnológicas complexas, mas sim organização, atenção aos controles essenciais e manutenção periódica das medidas adotadas.
Com a aplicação gradual dessas recomendações, as serventias podem alcançar níveis adequados de segurança da informação e demonstrar conformidade com os princípios estabelecidos no Provimento nº 213.

A transformação digital do Registro Civil ampliou significativamente a importância da segurança da informação e da proteção dos dados registrais.

Os sistemas informatizados passaram a desempenhar papel essencial na prestação dos serviços pelas serventias, exigindo cuidados mínimos para garantir a integridade, a disponibilidade e a confidencialidade das informações mantidas sob responsabilidade dos oficiais de registro civil.

O Provimento nº 213 estabelece um conjunto de diretrizes destinadas a fortalecer a proteção do acervo registral e a reduzir riscos tecnológicos associados ao uso de sistemas digitais.

Este guia foi elaborado com o objetivo de traduzir essas diretrizes em orientações práticas, acessíveis e compatíveis com a realidade operacional das serventias brasileiras.

A implementação das medidas apresentadas não exige, na maioria dos casos, a adoção de tecnologias complexas ou de alto custo. A utilização consistente de boas práticas básicas de segurança da informação já é suficiente para reduzir significativamente os riscos operacionais associados ao ambiente digital.

A adoção progressiva dessas medidas contribui para:

- proteger o acervo registral contra perda ou acesso indevido;
- aumentar a confiabilidade dos sistemas utilizados pelas serventias;
- garantir maior continuidade na prestação dos serviços registrais;
- fortalecer a confiança institucional no sistema de Registro Civil brasileiro.

A segurança da informação deve ser compreendida como um processo contínuo de melhoria e adaptação às mudanças tecnológicas.

Com organização, atenção aos controles essenciais e revisão periódica das práticas adotadas, as serventias podem alcançar níveis adequados de segurança e conformidade com os princípios estabelecidos pelo Provimento nº 213.

23 Lista de Acrônimos

A Tabela 14 apresenta os acrônimos e siglas utilizados ao longo deste guia, com suas respectivas definições.

Tabela 14: Acrônimos e siglas utilizados neste guia.

Acrônimo	Significado	Descrição resumida
3DES	*Triple Data Encryption Standard*	Algoritmo de criptografia depreciado; uso vedado pelo Provimento.
AES	*Advanced Encryption Standard*	Padrão de criptografia simétrica; o Provimento exige AES-256 como robustez mínima para dados em repouso e *backups* externos.
ANPD	Autoridade Nacional de Proteção de Dados	Órgão fiscalizador da LGPD; deve ser notificada em incidentes com risco a titulares de dados pessoais.
CNJ	Conselho Nacional de Justiça	Órgão do Poder Judiciário responsável pela edição do Provimento nº 213.
CNS	Código Nacional de Serventia	Identificador único de cada serventia extrajudicial no cadastro do CNJ.
DES	*Data Encryption Standard*	Algoritmo de criptografia depreciado; uso vedado pelo Provimento.
DMZ	*Demilitarized Zone*	Zona de rede intermediária entre a internet e a rede interna, para filtragem e controle de tráfego.
DPO/EPD	*Data Protection Officer* / Encarregado de Proteção de Dados	Pessoa designada como canal de comunicação sobre proteção de dados pessoais.
EOL	*End of Life*	Encerramento do suporte oficial de um *software* ou sistema pelo fabricante.
HA	*High Availability*	Mecanismos que asseguram continuidade dos sistemas mesmo em caso de falha de componentes.
HD	*Hard Disk*	Disco rígido; dispositivo de armazenamento de dados.
HTTP	*Hypertext Transfer Protocol*	Protocolo de comunicação utilizado na *web*; versão sem criptografia.
HTTPS	*Hypertext Transfer Protocol Secure*	Versão segura do HTTP, protegida por TLS; obrigatória para comunicações da serventia.
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira	Cadeia de certificação digital oficial do Brasil.
IdRC	Sistema de Autenticação Eletrônica do Registro Civil	Plataforma de autenticação baseada em OpenID Connect/OAuth 2.0, disponibilizada pelo ON-RCPN.
IDS	*Intrusion Detection System*	Sistema que monitora e registra tentativas de intrusão na rede.
IPCA	Índice Nacional de Preços ao Consumidor Amplo	Índice oficial para correção anual dos limites de arrecadação das classes.
IPS	*Intrusion Prevention System*	Sistema que detecta e bloqueia ativamente tráfego malicioso na rede.
ISP	*Internet Service Provider*	Provedor de acesso à internet.
LGPD	Lei Geral de Proteção de Dados Pessoais	Lei nº 13.709/2018; regulamenta o tratamento de dados pessoais no Brasil.
LUKS	*Linux Unified Key Setup*	Sistema de criptografia de disco utilizado em distribuições Linux.
MD5	*Message Digest Algorithm 5*	Algoritmo de *hash* depreciado; uso vedado pelo Provimento.
MFA	*Multi-Factor Authentication*	Autenticação multifator; obrigatória para acessos administrativos e críticos.
NTP	*Network Time Protocol*	Protocolo de sincronização de relógio; exigido para precisão temporal nos *logs*.
ON-RCPN	Operador Nacional do Registro Civil das Pessoas Naturais	Entidade responsável pela operação nacional dos serviços eletrônicos do Registro Civil.
PCN	Plano de Continuidade de Negócios	Documento com procedimentos para manter a prestação de serviços em situações adversas.

Continua na próxima página

Continuação da Tabela 14

Acrônimo	Significado	Descrição resumida
PDF/A	*Portable Document Format for Archiving*	Formato padronizado (ISO 19005) para preservação de documentos digitais de longa duração.
PRD	Plano de Recuperação de Desastres	Procedimentos técnicos para restauração da infraestrutura após incidentes graves.
RC4	*Rivest Cipher 4*	Algoritmo de criptografia de fluxo depreciado; uso vedado pelo Provimento.
RCPN	Registro Civil das Pessoas Naturais	Serviço extrajudicial responsável pelo registro de nascimentos, casamentos e óbitos.
RPO	*Recovery Point Objective*	Perda máxima admissível de dados entre o último *backup* e um incidente.
RSI	Responsável de Segurança da Informação	Pessoa formalmente designada para coordenar as ações de segurança da informação na serventia.
RTO	*Recovery Time Objective*	Tempo máximo admissível para restaurar os sistemas após falha ou incidente.
SaaS	*Software as a Service*	Modelo em que o sistema é executado e mantido integralmente pelo fornecedor em ambiente remoto.
SAI	Sistema de Alimentação Ininterrupta	Designação técnica para nobreak/UPS.
SGBD	Sistema de Gerenciamento de Banco de Dados	*Software* para armazenamento, organização e gestão dos dados registrais.
SHA-1	*Secure Hash Algorithm 1*	Algoritmo de *hash* depreciado; uso vedado pelo Provimento.
SHA-256	*Secure Hash Algorithm 256*	Algoritmo de *hash* seguro recomendado para verificação de integridade de documentos e dossiês.
SSL	*Secure Sockets Layer*	Protocolo de segurança depreciado, predecessor do TLS; uso vedado pelo Provimento.
SSID	*Service Set Identifier*	Identificador de rede Wi-Fi; utilizado na configuração de redes isoladas.
TI	Tecnologia da Informação	Área responsável pela gestão da infraestrutura tecnológica da serventia.
TLS	*Transport Layer Security*	Protocolo de segurança para comunicações em rede; mínimo exigido: TLS 1.2; recomendado: TLS 1.3.
TPM	*Trusted Platform Module*	Chip de segurança para armazenamento seguro de chaves criptográficas.
UPS	*Uninterruptible Power Supply*	Nobreak; autonomia mínima de 30 min exigida pelo Provimento.
VLAN	*Virtual Local Area Network*	Segmentação lógica de rede; obrigatória para Classes 2 e 3.
WORM	*Write Once, Read Many*	Armazenamento imutável; utilizado para proteção de *backups* contra *ransomware*.
XML	*Extensible Markup Language*	Formato aberto para dados estruturados; exigido para interoperabilidade.
XTS	*XEX-based Tweaked-codebook mode with ciphertext Stealing*	Modo de operação de criptografia de disco usado pelo BitLocker e FileVault.

24 Glossário de termos técnicos

Esta seção apresenta definições simplificadas de alguns termos técnicos utilizados ao longo deste guia.

O objetivo do glossário é facilitar a compreensão dos principais conceitos relacionados à segurança da informação e à infraestrutura tecnológica das serventias do Registro Civil.

Algumas definições apresentadas neste glossário foram adaptadas das definições estabelecidas no Provimento nº 213, com objetivo de facilitar sua compreensão prática no contexto das serventias do Registro Civil.

AES-256 (*Advanced Encryption Standard*)

Padrão de criptografia simétrica amplamente reconhecido pela comunidade técnica internacional, que utiliza chaves de 256 bits para cifrar dados. É considerado altamente seguro e é adotado por governos, instituições financeiras e infraestruturas críticas em todo o mundo.

O Provimento nº 213 estabelece o AES-256 como padrão mínimo de robustez para a criptografia de dados em repouso (Anexo II, item 2, inciso II). As ferramentas nativas dos sistemas operacionais modernos, BitLocker, FileVault e LUKS, implementam este padrão quando configuradas corretamente.

Arquitetura compartilhada

Modelo de infraestrutura tecnológica em que duas ou mais serventias utilizam recursos computacionais comuns, como servidores, redes ou serviços em nuvem, mantendo segregação lógica de dados e controles de acesso independentes.

Autenticação

Processo utilizado para verificar a identidade de um usuário que tenta acessar um sistema. Normalmente é realizado por meio de senha, certificado digital, token ou outros mecanismos de verificação.

Autenticação multifator (MFA)

Mecanismo de autenticação que exige dois ou mais fatores de verificação para confirmar a identidade do usuário. Por exemplo: senha combinada com um código temporário gerado por aplicativo autenticador.

Backup

Cópia de segurança dos dados armazenados em sistemas informatizados. O *backup* permite recuperar informações em caso de falha de sistema, erro humano ou incidente tecnológico.

BitLocker / Criptografia de Dispositivo

Mecanismos de criptografia de disco integrados ao sistema operacional Windows. A Criptografia de Dispositivo está disponível em todas as edições do Windows (incluindo Home) e pode ser ativada em Configurações → Privacidade e Segurança. O *BitLocker* é a versão avançada, disponível nas edições Pro, Enterprise e Education, com opções adicionais de gestão. Ambos protegem os dados armazenados no computador, impedindo o

acesso às informações caso o equipamento seja perdido, furtado ou acessado sem autorização.

Criptografia

Técnica utilizada para proteger dados por meio de codificação matemática, de forma que apenas pessoas ou sistemas autorizados possam acessar as informações.

Dados em trânsito

Informações que estão sendo transmitidas entre sistemas ou computadores por meio de redes de comunicação, como a internet.

Dados em repouso

Informações armazenadas em computadores, servidores ou dispositivos de armazenamento.

FileVault

Tecnologia de criptografia de disco integrada ao sistema operacional macOS. O *FileVault* protege os dados armazenados no computador por meio de criptografia, impedindo o acesso às informações caso o equipamento seja perdido ou acessado sem autorização.

Firewall / *Firewall stateful*

Equipamento ou *software* responsável por controlar o tráfego de dados entre redes, permitindo ou bloqueando conexões conforme regras de segurança previamente definidas.

O *firewall stateful* inspeciona cada pacote de dados no contexto da conexão à qual pertence, mantendo tabela de estado das sessões ativas e bloqueando pacotes que não correspondam a conexões legítimas. Difere do filtro de pacotes simples (presente em roteadores domésticos), que avalia cada pacote de forma isolada sem considerar o contexto da conexão.

O Provimento nº 213 exige a implantação de *firewall stateful* com IPS/IDS (*Intrusion Prevention/Detection System*) em todas as classes de serventias, como parte da infraestrutura de segurança perimetral básica (Anexo II, item 4, inciso II; Anexo IV, item 3.4). Um simples roteador doméstico sem inspeção de estado não atende a esse requisito.

Hypertext Transfer Protocol Secure (HTTPS)

Versão segura do protocolo HTTP utilizada na navegação na internet. O HTTPS utiliza criptografia baseada em TLS para proteger os dados transmitidos entre o navegador do usuário e o servidor.

IdRC

Sistema de Autenticação Eletrônica do Registro Civil, utilizado para autenticação segura de usuários em plataformas e sistemas institucionais. Baseia-se em padrões modernos de autenticação digital.

Incidente crítico

Evento de segurança da informação que comprometa ou possa comprometer de forma relevante a disponibilidade, a integridade, a autenticidade, a confidencialidade ou a rastreabilidade do acervo, dos sistemas ou da continuidade do serviço (art. 2º, inciso VII do Provimento nº 213). Incidentes críticos devem ser comunicados à Corregedoria competente em até 72 horas da ciência do evento (art. 11, §1º; Anexo II, item 4, inciso III), e à ANPD quando houver risco ou dano relevante a titulares de dados pessoais (art. 7º, §3º). Como meta de diligência reforçada, recomenda-se comunicar em até 24 horas quando possível (Anexo IV, item 1.6).

IPS/IDS

Sistemas de detecção e prevenção de intrusão que monitoram o tráfego de rede em busca de padrões anômalos ou ataques conhecidos. O *Intrusion Detection System*(IDS) identifica e registra tentativas de intrusão; o *Intrusion Prevention System*(IPS) vai além e bloqueia ativamente o tráfego malicioso. O Provimento nº 213 exige a implantação de *firewall stateful* com IPS/IDS em todas as classes de serventias (Anexo II, item 4, inciso II; Anexo IV, item 3.4).

Log

Registro automático de eventos realizados em um sistema informatizado, como acessos de usuários, operações executadas e alterações de configuração. O Provimento nº 213 exige que as trilhas de auditoria (*logs*) sejam retidas por prazo mínimo de 5 (cinco) anos, protegidas contra alteração ou exclusão não autorizada, e que cada registro identifique inequivocamente o usuário, a data e a hora da operação (Anexo II, item 3, incisos II e IV).

LUKS

Sistema de criptografia de disco amplamente utilizado em sistemas Linux. O LUKS permite proteger dados armazenados em dispositivos de armazenamento por meio de criptografia, evitando acesso não autorizado às informações.

Malware

Termo genérico utilizado para designar softwares maliciosos, como vírus, *trojans* ou *ransomware*, desenvolvidos para comprometer sistemas ou dados.

Nobreak (UPS)

Equipamento utilizado para proteger computadores e servidores contra quedas ou variações de energia elétrica, permitindo o funcionamento temporário dos equipamentos em caso de interrupção de energia.

Protocolo

Conjunto de regras técnicas que define como sistemas informatizados se comunicam em uma rede.

Pentest (teste de intrusão)

Avaliação técnica de segurança realizada por profissional especializado, que simula tentativas de acesso não autorizado aos sistemas com o objetivo de identificar vulnerabilidades antes que possam ser exploradas por agentes maliciosos. Para serventias de Classe 3, o Provimento nº 213 exige a realização de *pentest* ou metodologia equivalente com periodicidade mínima de a cada 2 anos, ou sempre que houver alteração relevante de infraestrutura (Anexo II, item 6, inciso IV; Anexo IV, item 4.7). Existem hipóteses de dispensa para serventias que operam em ambiente integralmente SaaS (Anexo II, item 6.3).

Portabilidade de dados

Capacidade de extrair, transferir e reutilizar os dados da serventia em formato estruturado e interoperável, preservando sua integridade, autenticidade e rastreabilidade, de modo a permitir migração para outro sistema ou fornecedor.

Ransomware

Tipo de *software* malicioso que bloqueia o acesso aos dados de um sistema ou criptografa arquivos, exigindo pagamento para restaurar o acesso às informações.

Recovery Point Objective (RPO)

Quantidade máxima de dados que pode ser perdida entre o último *backup* e a ocorrência de um incidente. Define, na prática, a frequência mínima necessária das rotinas de *backup*.

O Provimento nº 213 estabelece os seguintes valores máximos de RPO por classe (Anexo II, item 2.1): Classe 3: 4 horas; Classe 2: 12 horas; Classe 1: 24 horas. Esses valores devem constar do PCN e do PRD da serventia.

Recovery Time Objective (RTO)

Tempo máximo admissível para restaurar os sistemas e retomar as operações após uma falha ou incidente tecnológico. Define, na prática, o quanto a serventia pode permanecer sem acesso aos sistemas antes de comprometer a continuidade do serviço.

O Provimento nº 213 estabelece os seguintes valores máximos de RTO por classe (Anexo II, item 2.2): Classe 3: 8 horas; Classe 2: 24 horas; Classe 1: 24 horas (admitida solução simplificada documentada no PCN/PRD). Esses valores devem ser comprovados por testes documentados de restauração.

Reversibilidade

Garantia técnica e contratual de restituição integral e utilizável do acervo digital da serventia, incluindo dados, configurações e registros operacionais, em caso de substituição de sistema, mudança de fornecedor ou transição de gestão.

Servidor

Computador ou sistema responsável por fornecer serviços, dados ou aplicações a outros computadores conectados em rede.

Sistema Justiça Aberta

Plataforma eletrônica mantida pelo Conselho Nacional de Justiça na qual os responsáveis pelas serventias extrajudiciais devem declarar o cumprimento das etapas previstas no Provimento nº 213.

Nos termos do art. 17 do Provimento, cada declaração deve ser renovada anualmente e acompanhada de síntese do dossiê técnico com evidências mínimas de conformidade. A declaração falsa, objetivamente verificada em inspeções ou correições, sujeita o responsável às penalidades previstas em lei (art. 17, §2º).

Sistema registral

Software utilizado pelas serventias para realizar o registro, armazenamento e gestão dos atos registrais e dos dados associados.

Solução contratada

Modelo tecnológico em que a serventia depende estruturalmente de fornecedor externo para hospedagem, manutenção ou atualização de seus sistemas, não detendo controle técnico pleno sobre a infraestrutura crítica ou sobre os mecanismos essenciais de segurança.

Solução própria Modelo tecnológico em que a serventia mantém controle direto sobre sua infraestrutura e seus sistemas críticos, incluindo armazenamento de dados, mecanismos de segurança e capacidade de manutenção ou evolução tecnológica, ainda que possa contar com suporte técnico terceirizado.

Subclasse

Subdivisão interna de cada uma das três classes econômicas previstas no art. 16 do Provimento nº 213. A Classe 1 se subdivide em Subclasses A, B e C (cada uma equivalente

a um terço do teto de R$ 100.000 semestrais); a Classe 2, em Subclasses D, E e F (proporcionais ao teto de R$ 500.000); e a Classe 3, em Subclasses G, H, I e J (definidas por múltiplos do teto da Classe 2: até 3×, de 3× a 6×, de 6× a 12×, e acima de 12×, respectivamente). O enquadramento em subclasse é reavaliado anualmente com base na arrecadação do semestre anterior, e os limites são corrigidos pelo IPCA. Variações de até 10% do limite superior da faixa anterior exigem confirmação por dois ciclos consecutivos para produzir efeitos (art. 16, §§1º a 3º). Para fins de implementação das medidas deste guia, o determinante imediato é a classe (1, 2 ou 3).

VLAN (*Virtual Local Area Network*)

Tecnologia de segmentação lógica de rede que permite criar domínios de *broadcast* separados sobre a mesma infraestrutura física, isolando o tráfego de diferentes segmentos como se fossem redes físicas distintas. Para as serventias de Classes 2 e 3, o Provimento nº 213 exige a implementação obrigatória de VLANs ou solução tecnicamente equivalente para separar o ambiente administrativo/servidores do ambiente de atendimento ao público ou de dispositivos externos (art. 7º, inciso VII, alínea a). Para a Classe 1, admite-se solução simplificada idônea que produza o mesmo efeito de isolamento funcional (alínea b). O controle do tráfego entre VLANs deve ser realizado pelo *firewall stateful*.

Transport Layer Security (TLS)

Protocolo de segurança utilizado para proteger a comunicação entre sistemas em redes de computadores. O TLS garante a confidencialidade e a integridade dos dados transmitidos, sendo a base do protocolo HTTPS utilizado na navegação segura na internet.

O Provimento nº 213 exige a versão TLS 1.2 ou superior para dados em trânsito (Anexo II, item 2, inciso I), sendo o TLS 1.3 a versão recomendada por ser a mais atual e segura. O uso de versões anteriores, SSL, TLS 1.0 e TLS 1.1, é vedado pelo Provimento, por possuírem vulnerabilidades conhecidas e serem consideradas depreciadas pela comunidade técnica especializada.

Usuário

Pessoa autorizada a acessar sistemas informatizados da serventia por meio de conta individual de acesso.

Write Once, Read Many (WORM)

Mecanismo de armazenamento que permite gravar dados uma única vez, impedindo sua modificação ou exclusão posterior durante um período definido, mesmo por usuários com privilégios administrativos.

No contexto de *backups*, o WORM é utilizado para proteger as cópias de segurança contra *ransomware* e exclusão indevida, garantindo que os arquivos permaneçam íntegros e recuperáveis mesmo em caso de comprometimento do ambiente principal. Está disponível em serviços de nuvem como Amazon S3 Object Lock, Azure Immutable Blob Storage e equivalentes, bem como em soluções de *backup* locais compatíveis.

A Modelo de Política Básica de Segurança da Informação

Finalidade e abrangência deste modelo

Este apêndice apresenta um modelo de Política de Segurança da Informação que pode ser adotado e adaptado pelas serventias do Registro Civil das Pessoas Naturais.
O modelo foi estruturado para contemplar integralmente os dez elementos mínimos obrigatórios definidos no Anexo III do Provimento nº 213/2026 (itens 4.1 a 4.10), permitindo que a serventia formalize sua política em conformidade com os requisitos normativos desde a Etapa 1 do processo de implementação.
A política pode e deve ser adaptada à realidade operacional de cada serventia. Para unidades de menor porte (Classe 1), é admissível uma versão mais concisa, desde que contemple todos os elementos mínimos. Para serventias de Classes 2 e 3, recomenda-se maior detalhamento, especialmente nos itens relativos à gestão de fornecedores, criptografia e integração com o PCN/PRD.

O Anexo III do Provimento nº 213 estabelece o conteúdo mínimo obrigatório da Política Interna de Segurança da Informação das serventias. A política deve conter, no mínimo, os elementos indicados nos itens 4.1 a 4.10 daquele Anexo, podendo ser ampliada ou estruturada segundo metodologias reconhecidas de governança e *compliance*, desde que preservados os requisitos funcionais ali estabelecidos.

O modelo a seguir está organizado em seções que correspondem diretamente a cada um desses elementos obrigatórios. A tabela abaixo indica a correspondência entre as seções do modelo e os itens do Anexo III.

Tabela 15: Correspondência entre as seções do modelo de política e o Anexo III do Provimento nº 213.

Item do Anexo III	Elemento obrigatório	Seção correspondente neste modelo
4.1	Governança e responsabilidades	Seção 1 (Finalidade) e Seção 6 (Governança e responsabilidades)
4.2	Regras de controle e revogação de acesso	Seção 7 (Controle de acesso e revogação)
4.3	Diretrizes de uso aceitável	Seção 8 (Diretrizes de uso aceitável)
4.4	Integração com PCN e PRD, com RTO e RPO	Seção 9 (Continuidade operacional – PCN e PRD)
4.5	Proteção física de ativos	Seção 10 (Proteção física de ativos)
4.6	Procedimentos de gestão de incidentes	Seção 11 (Gestão de incidentes de segurança)
4.7	Gestão de vulnerabilidades	Seção 12 (Gestão de vulnerabilidades)
4.8	Proteção de dados pessoais (LGPD)	Seção 13 (Proteção de dados pessoais – LGPD)
4.9	Criptografia	Seção 14 (Criptografia e gestão de chaves)
4.10	Gestão de fornecedores	Seção 15 (Gestão de fornecedores)

Como utilizar este modelo

Passo 1: copie o modelo abaixo e substitua os campos indicados entre colchetes (por exemplo, [nome da serventia]) pelas informações da sua unidade.
Passo 2: revise cada seção e adapte as diretrizes à realidade operacional da serventia, eliminando itens inaplicáveis ou acrescentando controles adicionais conforme necessário.
Passo 3: submeta o documento à aprovação do delegatário, interino ou interventor, registrando a data de aprovação e a forma de divulgação interna.
Passo 4: divulgue a política a todos os colaboradores, estagiários e terceiros que utilizem os sistemas da serventia.
Passo 5: registre a existência da política no dossiê técnico e mantenha-a atualizada conforme os critérios de revisão estabelecidos na Seção 16 deste modelo.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

[Nome da Serventia]

CNS: [número] Classe: [1/2/3]

A.1 Seção 1 – Finalidade

Correspondência: Anexo III, itens 1 e 4.1 do Provimento nº 213.

Esta Política de Segurança da Informação tem como finalidade estabelecer princípios, diretrizes e responsabilidades para a proteção dos sistemas informatizados, dos dados registrais e das informações tratadas pela serventia [nome da serventia], assegurando confidencialidade (quando aplicável, nos termos da legislação), integridade, disponibilidade, rastreabilidade e conformidade legal (*compliance*).

A.2 Seção 2 – Abrangência

Correspondência: Anexo III, item 2 do Provimento nº 213.

Esta política aplica-se ao delegatário, interino ou interventor responsável pela serventia, a todos os colaboradores (escreventes, auxiliares, estagiários), bem como a terceiros e fornecedores que tenham acesso aos sistemas, aos dados ou às instalações da serventia.

Todos os destinatários desta política devem tomar ciência formal de seu conteúdo. O registro de ciência deve ser mantido no dossiê técnico da serventia pelo prazo mínimo de 5 (cinco) anos.

A.3 Seção 3 – Princípios

Correspondência: Anexo III, item 3 do Provimento nº 213.

A gestão da segurança da informação na serventia observa os seguintes princípios fundamentais:

- **Confidencialidade:** garantir que as informações sejam acessadas apenas por pessoas autorizadas, observadas as hipóteses legais de publicidade;
- **Integridade:** assegurar que dados e registros sejam mantidos íntegros, completos e protegidos contra alterações não autorizadas;
- **Disponibilidade:** manter os sistemas e as informações acessíveis e operacionais quando necessário;
- **Rastreabilidade:** registrar as operações realizadas nos sistemas de forma que seja possível identificar quem realizou cada ação, quando e de que forma;
- **Conformidade legal:** assegurar que as práticas de segurança da informação estejam em conformidade com a legislação vigente, especialmente a Lei nº 6.015/1973, a Lei nº 8.935/1994, a Lei nº 13.709/2018 (LGPD) e o Provimento nº 213/2026 do CNJ.

A.4 Seção 4 – Definições

Para os fins desta política, aplicam-se as definições estabelecidas no art. 2º do Provimento nº 213/2026, bem como os termos técnicos apresentados no glossário do Guia Rápido de Implementação (Seção 24).

A.5 Seção 5 – Referências normativas

Esta política fundamenta-se nos seguintes instrumentos normativos:

- Provimento nº 213/2026 do Conselho Nacional de Justiça;
- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);
- Lei nº 6.015/1973 – Lei de Registros Públicos;
- Lei nº 8.935/1994 – Lei dos Notários e Registradores;
- normas complementares editadas pela Corregedoria Nacional de Justiça e pela Corregedoria do Tribunal de Justiça do Estado de [UF].

A.6 Seção 6 – Governança e responsabilidades

Correspondência: Anexo III, item 4.1 do Provimento nº 213.

6.1. O **delegatário** (ou interino/interventor) é o responsável final pela segurança da informação e pelo cumprimento desta política, nos termos do art. 5º, §1º do Provimento nº 213. A responsabilidade é pessoal e indelegável, ainda que haja contratação de terceiros.

6.2. O **Responsável de Segurança da Informação (RSI)** é a pessoa formalmente designada para coordenar a implementação, o monitoramento e a atualização das medidas de segurança previstas nesta política. O RSI da serventia é: [nome / cargo / data de designação].

6.3. O **Encarregado de Proteção de Dados (DPO/EPD)**, quando aplicável, é a pessoa designada como canal de comunicação sobre proteção de dados pessoais perante os titulares e a ANPD. O encarregado desta serventia é: [nome / cargo / data de designação / ou indicação de não aplicabilidade com justificativa].

6.4. Todos os **colaboradores e terceiros** são responsáveis por:

- observar as diretrizes estabelecidas nesta política;

- utilizar os sistemas da serventia de forma responsável e em conformidade com suas atribuições;
- manter sigilo sobre suas credenciais de acesso;
- comunicar imediatamente ao RSI qualquer incidente, suspeita de incidente ou vulnerabilidade identificada nos sistemas.

A.7 Seção 7 – Controle de acesso e revogação

Correspondência: Anexo III, item 4.2 do Provimento nº 213.

7.1. Autenticação individualizada. Cada pessoa que utiliza os sistemas da serventia deve possuir conta de acesso individual, com credencial pessoal e intransferível. É vedado, em qualquer hipótese, o uso de contas compartilhadas, genéricas (por exemplo, "atendimento", "cartorio") ou que impeçam a responsabilização individual (art. 5º, §2º do Provimento).

7.2. Autenticação multifator (MFA). A MFA é obrigatória para:

- acessos administrativos aos sistemas registrais e de gestão;
- acessos remotos à infraestrutura da serventia;
- acesso a bancos de dados e painéis de configuração de sistemas;
- funcionalidades críticas que envolvam dados registrais sensíveis ou operações irreversíveis.

A autenticação por fator único é admitida apenas para perfis de menor risco, desde que tecnicamente justificada e documentada no dossiê técnico. Sempre que possível, recomenda-se a integração com o IdRC.

7.3. Princípio da necessidade. Os perfis de acesso devem ser segregados conforme as funções efetivamente exercidas, concedendo-se apenas as permissões estritamente necessárias para a realização das atividades atribuídas a cada usuário.

7.4. Contas técnicas. É admitido o uso de contas técnicas automatizadas exclusivamente para integração entre sistemas ou execução de rotinas sistêmicas, desde que haja segregação de privilégios, registro auditável de todas as operações, identificação inequívoca da conta e do sistema responsável, e vedação de uso para prática direta de atos notariais ou registrais (art. 5º, §3º).

7.5. Revogação e revisão de acessos. Os acessos devem ser revogados ou ajustados nos seguintes casos:

- **desligamento:** a conta deve ser desativada imediatamente após o encerramento do vínculo do colaborador, estagiário ou terceiro com a serventia;
- **mudança de função:** as permissões devem ser ajustadas para refletir as novas atribuições, removendo-se acessos que deixaram de ser necessários;
- **afastamento prolongado:** contas de usuários em licença, férias ou afastamento superior a 30 dias devem ser temporariamente suspensas;
- **revisão periódica:** a lista de usuários autorizados e seus respectivos perfis de acesso devem ser revisados pelo RSI ao menos uma vez por ano, com registro no dossiê técnico.

O registro de usuários autorizados deve ser mantido atualizado conforme o modelo apresentado no Apêndice D deste guia.

A.8 Seção 8 – Diretrizes de uso aceitável

Correspondência: Anexo III, item 4.3 do Provimento nº 213.

Os recursos tecnológicos da serventia — computadores, servidores, equipamentos de rede, sistemas registrais, acesso à internet e dispositivos periféricos — são ferramentas de trabalho destinadas exclusivamente ao exercício das atividades registrais e administrativas da unidade.

8.1. São condutas obrigatórias:

- utilizar os sistemas exclusivamente para fins institucionais e compatíveis com as atribuições funcionais;
- bloquear a sessão do computador ao se ausentar da estação de trabalho;
- manter sigilo sobre senhas e credenciais de acesso;
- comunicar imediatamente ao RSI qualquer anomalia, tentativa de acesso indevido ou comportamento inesperado dos sistemas.

8.2. São condutas vedadas:

- instalar softwares não autorizados nos equipamentos da serventia;
- utilizar dispositivos de armazenamento externo (pen drives, HDs) sem autorização do RSI;
- compartilhar credenciais de acesso com outros usuários;
- acessar conteúdos ou serviços não relacionados à atividade registral em equipamentos da serventia;
- desativar ou contornar mecanismos de proteção, como antivírus, firewall ou criptografia de disco;
- armazenar dados registrais em dispositivos pessoais ou serviços de nuvem não autorizados pela serventia.

8.3. O descumprimento das diretrizes de uso aceitável sujeitará o responsável às medidas administrativas cabíveis, sem prejuízo das responsabilidades civis e penais.

A.9 Seção 9 – Continuidade operacional – PCN e PRD

Correspondência: Anexo III, item 4.4 do Provimento nº 213.

A serventia mantém Plano de Continuidade de Negócios (PCN) e Plano de Recuperação de Desastres (PRD) formalizados e atualizados, em conformidade com o item 2.5 do Anexo IV do Provimento, contendo:

- identificação e avaliação estruturada dos riscos que possam comprometer a continuidade das operações registrais;
- definição objetiva das medidas de mitigação para cada risco identificado;
- parâmetros expressos de **RTO** (*Recovery Time Objective*) e **RPO** (*Recovery Point Objective*) compatíveis com a classe da serventia:
  - Classe 1: RPO máximo de 24 horas / RTO máximo de 24 horas;
  - Classe 2: RPO máximo de 12 horas / RTO máximo de 24 horas;
  - Classe 3: RPO máximo de 4 horas / RTO máximo de 8 horas;
- previsão de medidas de curto prazo (até 30 dias) e de médio prazo (até 90 dias) para resposta a incidentes e restauração da normalidade operacional;
- procedimentos específicos para restauração dos sistemas, bancos de dados e acervo

registral a partir das cópias de segurança;
- identificação dos responsáveis por cada etapa do processo de recuperação;
- localização e forma de acesso aos *backups* e às chaves de descriptografia necessárias à restauração.

O PCN e o PRD devem ser testados por meio de simulação anual de desastre e atualizados sempre que houver alteração relevante na infraestrutura tecnológica, nos sistemas utilizados ou após a ocorrência de incidente grave. Os resultados das simulações e das atualizações devem ser registrados no dossiê técnico.

Os parâmetros de RTO e RPO estabelecidos acima são os definidos para a classe [1/2/3] desta serventia, conforme Anexo II, itens 2.1 e 2.2 do Provimento nº 213.

A.10 Seção 10 – Proteção física de ativos

Correspondência: Anexo III, item 4.5 do Provimento nº 213.

Os equipamentos críticos de tecnologia da informação — servidores, *switches*, roteadores, *firewalls* e nobreaks — devem estar instalados em ambiente com as seguintes condições mínimas:

- **controle de acesso restrito:** o acesso ao local onde os equipamentos estão instalados deve ser limitado a pessoas formalmente autorizadas. Em serventias de menor porte, um armário com chave ou uma sala de uso exclusivo do responsável técnico já atende ao requisito;
- **proteção contra incêndio:** o ambiente deve dispor de extintor de incêndio adequado a equipamentos elétricos (CO_2 ou pó químico seco classe C);
- **proteção contra inundação:** os equipamentos devem ser instalados em local sem risco de infiltração ou inundação;
- **proteção contra variações térmicas:** o ambiente deve possuir ventilação adequada para evitar superaquecimento;
- **estabilidade elétrica:** os equipamentos críticos devem estar protegidos por nobreak (SAI/UPS) com autonomia mínima de 30 minutos, e a infraestrutura elétrica deve possuir aterramento funcional e tecnicamente aferido, mantido laudo atualizado com ART (art. 12, §8º);
- **organização física:** cabeamento organizado e identificado, equipamentos fixados adequadamente, ausência de materiais inflamáveis próximos aos ativos de TI.

Para serventias que operam integralmente em nuvem ou em arquitetura SaaS, sem infraestrutura local significativa, a proteção física é suprida pela documentação contratual que comprove ou ao menos indicie a adoção, pelo fornecedor, de controles equivalentes de segurança física e ambiental (Anexo I, item 3, inciso I).

A.11 Seção 11 – Gestão de incidentes de segurança

Correspondência: Anexo III, item 4.6 do Provimento nº 213; art. 11.

A serventia mantém procedimento documentado para gestão de incidentes de segurança da informação, contemplando as seguintes fases:

a) **identificação:** detecção do evento por qualquer colaborador, sistema de monitoramento ou fornecedor;

b) **classificação por gravidade:** todo incidente deve ser classificado como **crítico**, **alto**, **médio** ou **baixo**, conforme o impacto sobre a disponibilidade, integridade, confidencialidade ou rastreabilidade do acervo e dos sistemas;
c) **contenção:** adoção imediata de medidas para limitar o impacto do incidente e evitar sua propagação;
d) **erradicação:** eliminação da causa raiz do incidente;
e) **recuperação:** restauração dos sistemas e dados afetados;
f) **registro e documentação:** todos os incidentes devem ser registrados formalmente, com indicação de data, descrição, gravidade, medidas adotadas, análise de causa raiz, medidas corretivas e lições aprendidas (art. 11, §2º).

11.1. Comunicação obrigatória. Incidentes classificados como **críticos** devem ser comunicados à Corregedoria competente no prazo máximo de **72 horas** da ciência do evento (Anexo II, item 4, inciso III), sem prejuízo das comunicações exigidas pela legislação específica.

Como meta de diligência reforçada, a comunicação deve ocorrer em até **24 horas** sempre que possível, especialmente quando houver risco relevante de indisponibilidade prolongada, comprometimento de dados pessoais ou potencial impacto sistêmico (Anexo IV, item 1.6).

11.2. Incidentes envolvendo dados pessoais. Quando o incidente puder acarretar risco ou dano relevante aos titulares de dados pessoais, deverá ser comunicado também à Autoridade Nacional de Proteção de Dados (ANPD), nos termos e prazos definidos pela legislação e regulamentação vigentes (art. 7º, §3º).

O modelo de registro de incidentes consta do Apêndice E deste guia.

A.12 Seção 12 – Gestão de vulnerabilidades

Correspondência: Anexo III, item 4.7 do Provimento nº 213; Anexo II, item 5.

A serventia mantém procedimento documentado de gestão de vulnerabilidades tecnológicas, observando integralmente os prazos e critérios técnicos definidos no Anexo II, item 5, vedada qualquer disposição interna que flexibilize ou reduza esses parâmetros mínimos.

12.1. Atualização periódica. Sistemas operacionais, aplicações, *firmwares* de equipamentos de rede e demais componentes tecnológicos devem ser mantidos atualizados. Não é admitida a utilização de componentes cujo suporte oficial pelo fabricante tenha sido encerrado (*End of Life* – EOL), devendo a serventia manter evidência documental atualizada da vigência do suporte técnico (art. 4º, §3º).

12.2. Prazos máximos de tratamento:

- vulnerabilidades classificadas como **críticas**: tratamento em prazo máximo de **30 dias**, quando inexistente evidência de exploração ativa;
- vulnerabilidades com **exploração ativa, risco iminente ou comprometimento relevante**: adoção de medidas imediatas de contenção e correção emergencial, preferencialmente em até **72 horas**, com registro formal das providências adotadas, inclusive das medidas mitigatórias aplicadas durante a janela de correção.

12.3. Registro formal. Todas as vulnerabilidades identificadas devem ser registradas no dossiê técnico com indicação de: data de identificação, classificação de risco, providências

implementadas, responsável e data de encerramento (art. 11, §4º).

A.13 Seção 13 – Proteção de dados pessoais (LGPD)

Correspondência: Anexo III, item 4.8 do Provimento nº 213; art. 7º.

A serventia observa integralmente a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) no exercício de suas atividades registrais e administrativas.

13.1. Controlador de dados. O delegatário (ou interino/ interventor) responsável pela serventia é o **controlador** de dados pessoais no âmbito da unidade, nos termos do art. 7º do Provimento nº 213.

13.2. Registro de operações de tratamento. A serventia mantém registro das operações de tratamento de dados pessoais realizadas, conforme exigido pelo art. 7º, §1º do Provimento e pela LGPD.

13.3. Direitos dos titulares. A serventia mantém procedimentos para atendimento aos direitos dos titulares de dados pessoais previstos na LGPD, observados os limites e as condições estabelecidos na legislação registral.

13.4. Encarregado (DPO). A serventia designou encarregado pelo tratamento de dados pessoais, quando aplicável, com atribuições compatíveis com a legislação e com os riscos inerentes às atividades desempenhadas (art. 7º, §2º). Identificação: [nome / cargo / ou indicação de não aplicabilidade].

13.5. Comunicação de incidentes à ANPD. Incidentes de segurança que possam acarretar risco ou dano relevante aos titulares de dados pessoais devem ser comunicados à Autoridade Nacional de Proteção de Dados (ANPD) e à Corregedoria competente, nos termos e prazos definidos pela legislação e regulamentação vigentes (art. 7º, §3º).

13.6. Medidas técnicas e organizacionais. As medidas de segurança previstas nesta política — incluindo controle de acesso, criptografia, *backup*, registro de eventos e gestão de incidentes — constituem medidas técnicas e organizacionais adotadas pela serventia para proteção dos dados pessoais sob sua responsabilidade.

A.14 Seção 14 – Criptografia e gestão de chaves

Correspondência: Anexo III, item 4.9 do Provimento nº 213; art. 9º; Anexo II, item 2.

14.1. Dados em trânsito. Toda comunicação entre os sistemas da serventia e serviços externos deve utilizar protocolo **TLS 1.2 ou superior** (TLS 1.3 recomendado). É vedado o uso de versões depreciadas: SSL, TLS 1.0 e TLS 1.1.

14.2. Dados em repouso. Equipamentos que armazenam dados registrais devem utilizar criptografia de disco com robustez equivalente, no mínimo, a **AES-256** ou padrão tecnicamente equivalente ou superior (Anexo II, item 2, inciso II).

14.3. *Backups* externos. Toda cópia de segurança destinada a armazenamento externo ou em infraestrutura de terceiros deve ser criptografada **antes do envio** (*criptografia na origem*), com padrão mínimo AES-256, mantida a chave de descriptografia sob **custódia exclusiva da serventia** e não do provedor de armazenamento.

14.4. Algoritmos vedados. É proibido o uso dos seguintes algoritmos e protocolos, considerados depreciados ou vulneráveis: MD5, SHA-1, DES, 3DES, RC4, SSL, TLS 1.0

e TLS 1.1.

14.5. Gestão de chaves criptográficas. A serventia mantém gestão formal das chaves criptográficas utilizadas, contemplando:

- inventário atualizado de chaves e certificados digitais, com indicação de finalidade, algoritmo, data de emissão e data de expiração;
- segregação de custódia: as chaves não devem estar sob controle exclusivo de um único usuário nem armazenadas no mesmo ambiente que os dados protegidos;
- controle formal de acesso: apenas responsáveis formalmente designados podem acessar as chaves;
- política de rotação e renovação periódica, com procedimento documentado;
- registro auditável das operações de geração, renovação e revogação de chaves.

14.6. Revisão periódica dos padrões criptográficos. Os padrões adotados pela serventia devem ser revisados ao menos uma vez por ano, com substituição obrigatória de algoritmos ou protocolos que se tornem obsoletos ou inseguros, assegurada a adoção de padrões reconhecidos como adequados pela comunidade técnica especializada (Anexo II, item 2, inciso V; Anexo III, item 4.9, inciso IV). O resultado da revisão deve ser registrado no dossiê técnico.

A.15 Seção 15 – Gestão de fornecedores

Correspondência: Anexo III, item 4.10 do Provimento nº 213; arts. 13 e 15.

A serventia adota os seguintes controles para a gestão da relação com fornecedores de sistemas e serviços de tecnologia da informação:

15.1. Avaliação prévia de segurança. Antes da contratação ou renovação de serviços de tecnologia, a serventia deve avaliar se o fornecedor possui condições técnicas de atender aos requisitos de segurança da informação previstos no Provimento nº 213, incluindo capacidade de criptografia, *backup*, disponibilidade e proteção de dados pessoais.

15.2. Cláusulas contratuais obrigatórias. Os contratos com fornecedores que envolvam tratamento, armazenamento ou processamento de dados da serventia devem conter, no mínimo, cláusulas expressas e exequíveis de (art. 13, §6º; Anexo IV, item 1.8):

i) confidencialidade;
ii) reversibilidade integral do acervo;
iii) portabilidade integral do acervo em formato interoperável e não proprietário;
iv) disponibilização de documentação técnica necessária à migração;
v) cooperação em caso de transição de fornecedor;
vi) gestão de incidentes, com compromisso de notificação imediata à serventia em caso de incidente que afete os dados registrais;
vii) conformidade integral com a Lei nº 13.709/2018 (LGPD).

15.3. Responsabilidades em caso de incidentes. Os contratos devem definir claramente as responsabilidades do fornecedor em caso de incidentes de segurança, incluindo prazos de comunicação, apoio técnico para contenção e recuperação, e preservação de evidências para análise de causa raiz.

15.4. Monitoramento contínuo. A serventia deve acompanhar continuamente o cumprimento das obrigações contratuais pelo fornecedor, especialmente no que se refere a atualizações de segurança, manutenção de suporte técnico vigente e observância dos pa-

drões de proteção de dados.

15.5. Mitigação de dependência estrutural. Considera-se mitigada a dependência em relação a fornecedor quando houver, cumulativamente (art. 15):

i) cláusula contratual expressa de reversibilidade e portabilidade em formato interoperável;
ii) comprovação de teste de extração integral do acervo;
iii) inexistência de restrição técnica ou contratual que impeça a migração sem anuência discricionária do fornecedor.

A.16 Seção 16 – Revisão, auditoria e vigência

Correspondência: Anexo III, item 5 do Provimento nº 213.

16.1. Revisão periódica. Esta política deve ser revisada e, quando necessário, atualizada nas seguintes situações:

- ao menos uma vez por ano, independentemente de outras condições;
- sempre que houver alteração legislativa ou regulatória relevante, especialmente em matéria de proteção de dados pessoais;
- sempre que houver alteração significativa na infraestrutura tecnológica, nos sistemas utilizados ou nos fornecedores da serventia;
- após incidente de segurança classificado como crítico ou alto, com análise de causa raiz já concluída.

16.2. Registros auditáveis. As versões anteriores desta política, bem como os registros de revisão (data, motivo, alterações realizadas e responsável), devem ser mantidos por prazo mínimo de **5 (cinco) anos**, em formato acessível para fiscalização correicional.

16.3. Fiscalização. Esta política e seus registros estão sujeitos à fiscalização pela Corregedoria competente, nos termos do Provimento nº 213 e das demais normas aplicáveis.

16.4. Vigência. Esta política entra em vigor na data de sua aprovação pelo delegatário (ou interino/interventor) e permanece vigente até sua substituição por versão atualizada.

Aprovação:

Data de aprovação: _____

Versão: _____

_____	_____
Delegatário / Interino / Interventor	Responsável de Segurança da Informação

Forma de divulgação interna: _____

Data da divulgação: _____

Próxima revisão programada: _____

B Registro de Rotinas de *Backup*

Registro das rotinas de *backup*

A realização de *backups* periódicos é essencial para proteger os dados registrais contra perdas acidentais ou falhas tecnológicas.
Além de manter as cópias de segurança, recomenda-se registrar de forma simples a execução das rotinas de *backup*, indicando quando elas foram realizadas e quais sistemas ou dados foram incluídos.
Esse registro ajuda a demonstrar que a serventia mantém práticas regulares de proteção dos dados e facilita eventuais processos de auditoria ou verificação de conformidade.

A realização regular de *backups* é uma das medidas mais importantes para garantir a preservação do acervo registral e a continuidade das atividades da serventia em caso de falhas tecnológicas ou incidentes.

Para demonstrar que essas rotinas estão sendo executadas, recomenda-se manter um registro simples das operações de *backup* realizadas.

Esse registro permite acompanhar a execução das cópias de segurança, identificar eventuais falhas e demonstrar a adoção das práticas previstas no Provimento nº 213.

B.1 Finalidade do registro

O registro das rotinas de *backup* tem como objetivo documentar a realização das cópias de segurança dos dados e sistemas utilizados pela serventia.

Esse registro também contribui para:

- verificar a regularidade da execução dos *backups*;
- identificar eventuais falhas no processo de cópia de segurança;
- registrar testes de restauração realizados;
- facilitar auditorias ou verificações administrativas relacionadas à segurança da informação.

A manutenção desse registro ajuda a garantir que as rotinas de *backup* estejam sendo executadas de forma consistente.

B.2 Informações recomendadas

O registro das rotinas de *backup* pode conter apenas informações essenciais sobre a execução das cópias de segurança.

Entre os dados que devem ser registrados estão:

- data e horário da execução do *backup*;
- sistema ou base de dados incluída no *backup*;
- ambientes de armazenamento utilizados (indicar os dois ambientes independentes exigidos pelo Provimento, com identificação de cada um);
- confirmação de que ao menos um ambiente possui proteção contra *ransomware* (WORM, versionamento bloqueado ou equivalente);
- confirmação de criptografia aplicada antes do envio para armazenamento externo;
- responsável pela verificação do *backup*;

- resultado da verificação de integridade;
- observações sobre eventuais falhas ou ocorrências.

Essas informações permitem acompanhar a execução das rotinas de *backup* e identificar rapidamente possíveis problemas.

B.3 Modelo simplificado de registro

A serventia pode manter um registro simples das rotinas de *backup* em formato de tabela.

A Tabela 16 apresenta um exemplo de estrutura que pode ser utilizada para organizar essas informações.

Tabela 16: Modelo simplificado de registro das rotinas de *backup*.

Data	Sistema ou dados	Local do *backup*	Responsável	Observações

Esse registro pode ser mantido em formato digital ou impresso, conforme a organização administrativa da serventia.

O importante é que as informações estejam disponíveis para consulta e permitam verificar a execução regular das rotinas de *backup*, conforme ilustrado na Tabela 16.

C Registro de Teste de Restauração de *Backup*

Verificação da capacidade de recuperação dos dados

A realização de testes de restauração é essencial para verificar se os dados armazenados nos *backups* podem ser recuperados corretamente em caso de necessidade.
Recomenda-se que a serventia realize periodicamente testes de restauração e registre os resultados dessa verificação, indicando a data do teste e os sistemas ou dados avaliados.
Esse procedimento contribui para assegurar que os mecanismos de *backup* estejam funcionando de forma adequada e que o acervo registral possa ser recuperado em situações de falha ou incidente.

A existência de cópias de segurança não garante, por si só, que os dados poderão ser recuperados em caso de falha ou incidente tecnológico.

Arquivos de *backup* podem estar corrompidos, incompletos ou incompatíveis com o ambiente de recuperação.

Por esse motivo, recomenda-se que as serventias realizem testes periódicos de restauração de *backup* para verificar se os dados armazenados podem ser efetivamente recuperados.

C.1 Finalidade do teste

O teste de restauração tem como objetivo confirmar que as cópias de segurança produzidas pela serventia podem ser utilizadas para recuperar os dados em caso de incidente.

Esses testes permitem:

- verificar a integridade dos arquivos de *backup*;
- confirmar que o processo de restauração funciona corretamente;
- identificar eventuais problemas nas rotinas de *backup*;
- demonstrar que a serventia possui capacidade de recuperar seus dados em caso de falha.

A realização desses testes fortalece a confiabilidade das rotinas de *backup* e contribui para a continuidade das atividades da serventia.

C.2 Procedimento recomendado

O teste de restauração pode ser realizado de forma simples, utilizando uma cópia recente do *backup*.

De forma geral, recomenda-se:

a) selecionar uma cópia de *backup* recente armazenada no ambiente externo;
b) verificar a disponibilidade da chave de descriptografia - confirmar que a chave necessária para decifrar o *backup* está acessível e funcional antes de iniciar a restauração;
c) descriptografar e restaurar os dados em ambiente controlado ou em computador de teste;
d) verificar se os arquivos ou bases de dados restaurados estão íntegros e acessíveis;
e) registrar a realização do teste, incluindo confirmação de que a criptografia foi corretamente aplicada e que a chave estava disponível e funcional.

Por que testar a descriptografia?

Um *backup* criptografado cuja chave foi perdida, corrompida ou armazenada incorretamente é irrecuperável. O teste de restauração deve sempre incluir a verificação de que a chave de descriptografia está disponível e funcional e não apenas que o arquivo de *backup* existe.
Por isso, a localização e o procedimento de acesso à chave devem estar registrados no dossiê técnico da serventia e verificados a cada teste.

Não é necessário restaurar todo o sistema a cada teste. A verificação de uma amostra representativa de dados já permite confirmar o funcionamento do processo de recuperação.

C.3 Modelo simplificado de registro

Recomenda-se manter um registro simples dos testes de restauração de *backup* realizados pela serventia.

A Tabela 17 apresenta um exemplo de estrutura que pode ser utilizada para documentar esses testes.

Esse registro permite demonstrar que a serventia verifica periodicamente a capacidade de recuperação dos dados armazenados em suas cópias de segurança, conforme ilustrado

Tabela 17: Modelo simplificado de registro de testes de restauração de *backup*.

Data	*Backup* testado	Chave disponível	Resultado	Responsável	Observações

na Tabela 17.

Recomenda-se realizar testes de restauração ao menos uma ou duas vezes por ano.

C.4 Registro de revisão do Plano de Continuidade e Recuperação

Este registro tem por objetivo documentar a revisão periódica do Plano de Continuidade de Negócios (PCN) e do Plano de Recuperação de Desastres (PRD) da serventia, permitindo demonstrar a atualização das medidas de continuidade operacional e recuperação dos sistemas.

Tabela 18: Registro de revisão do PCN e do PRD

Data	Plano revisado	Ajustes realizados	Responsável	Próxima revisão
	PCN / PRD			
	PCN / PRD			
	PCN / PRD			

D Registro de Usuários Autorizados

Controle de usuários autorizados

A serventia deve manter um registro atualizado das pessoas autorizadas a acessar os sistemas utilizados na atividade registral.
Esse registro permite identificar quais usuários possuem acesso aos sistemas, quais funções exercem e quais permissões lhes foram atribuídas.
A manutenção organizada dessas informações facilita a revisão periódica dos acessos, contribui para a segurança dos sistemas e apoia eventuais processos de auditoria ou fiscalização.

O controle adequado de acesso aos sistemas utilizados pela serventia depende da identificação clara das pessoas que possuem autorização para utilizar esses sistemas.

Para garantir rastreabilidade das operações realizadas e evitar acessos indevidos às informações registrais, recomenda-se manter um registro atualizado dos usuários autorizados a acessar os sistemas da serventia.

Esse registro também contribui para demonstrar a adoção de práticas adequadas de controle de acesso, conforme as diretrizes estabelecidas pelo Provimento nº 213.

D.1 Finalidade do registro

O registro de usuários autorizados tem como objetivo documentar quais pessoas possuem acesso aos sistemas informatizados da serventia e quais funções exercem.

Entre os principais objetivos desse registro estão:

- identificar os usuários autorizados a acessar os sistemas da serventia;
- registrar as funções exercidas por cada usuário;
- facilitar a revisão periódica das permissões de acesso;
- demonstrar a adoção de práticas de controle de acesso aos sistemas.

A manutenção desse registro contribui para aumentar a transparência na gestão dos acessos aos sistemas.

D.2 Controle de acesso aos sistemas

Cada usuário da serventia deve possuir uma conta individual de acesso aos sistemas utilizados na atividade registral.

Contas compartilhadas devem ser evitadas, pois dificultam a identificação das operações realizadas nos sistemas.

Sempre que possível, recomenda-se:

- conceder apenas as permissões necessárias para cada função;
- revisar periodicamente a lista de usuários autorizados;
- remover ou desativar contas de usuários que deixarem a serventia;
- habilitar MFA obrigatoriamente para acessos administrativos e funcionalidades críticas; para demais perfis de menor risco, documentar tecnicamente a justificativa no dossiê da serventia;
- considerar a integração com o IdRC, que suporta MFA de forma centralizada.

Essas medidas ajudam a garantir maior segurança no acesso aos sistemas e às informações registrais.

D.3 Modelo simplificado de registro

A serventia pode manter um registro simples dos usuários autorizados em formato de tabela.

A Tabela 19 apresenta um exemplo de estrutura que pode ser utilizada para organizar essas informações.

Esse registro deve ser atualizado sempre que houver alteração na equipe da serventia ou mudança nas permissões de acesso aos sistemas.

A manutenção da lista apresentada na Tabela 19 contribui para garantir que apenas usuários autorizados possuam acesso aos sistemas da serventia.

Recomenda-se revisar periodicamente essa lista para assegurar que os acessos permaneçam adequados às funções exercidas por cada usuário.

Tabela 19: Modelo simplificado de registro de usuários autorizados.

Nome do usuário	Função	Sistema ou acesso	Data de autorização

E Registro de Incidentes de Segurança

Registro de incidentes de segurança

Sempre que ocorrer um evento relevante que possa afetar a segurança dos sistemas ou a disponibilidade dos serviços da serventia, recomenda-se registrar o incidente de forma simples e objetiva.
Esse registro permite documentar o ocorrido, identificar as medidas adotadas para resolução do problema e facilitar análises posteriores.
Atenção: incidentes classificados como críticos devem ser comunicados à Corregedoria competente no prazo máximo de 72 horas (art. 11, §1º; Anexo II, item 4, inciso III). Esse prazo é obrigatório e vinculante.

Mesmo com a adoção de boas práticas de segurança da informação, incidentes tecnológicos podem ocorrer.

Falhas de sistemas, tentativas de acesso indevido, problemas de infraestrutura ou eventos relacionados à segurança dos sistemas podem afetar o funcionamento dos serviços da serventia.

O Provimento nº 213 (art. 11) exige que a serventia mantenha procedimentos documentados para gestão de incidentes, contemplando identificação, classificação por gravidade, medidas de contenção, erradicação, recuperação e registro das ocorrências.

E.1 Classificação por gravidade e obrigações de comunicação

Atenção: prazo obrigatório de comunicação

O Provimento nº 213 estabelece que incidentes críticos devem ser comunicados à Corregedoria competente em até 72 horas (Anexo II, item 4, inciso III), sem prejuízo das comunicações exigidas pela legislação específica, em particular a LGPD.
Como meta de diligência reforçada, o Provimento recomenda que a comunicação ocorra em até 24 horas sempre que possível, especialmente quando houver risco relevante de indisponibilidade prolongada, comprometimento de dados pessoais ou potencial impacto sistêmico (Anexo IV, item 1.6).

O Provimento adota quatro níveis de gravidade para classificação de incidentes (Anexo II, item 4, inciso II): crítico, alto, médio e baixo.

A classificação orienta a urgência da resposta e determina as obrigações de comunicação:

- **Incidente crítico:** evento que comprometa ou possa comprometer de forma re-

levante a disponibilidade, a integridade, a autenticidade, a confidencialidade ou a rastreabilidade do acervo, dos sistemas ou da continuidade do serviço (art. 2º, inciso VII). Exige comunicação à Corregedoria competente em até 72 horas da ciência do incidente, e à ANPD quando houver risco ou dano relevante a titulares de dados pessoais (art. 7º, §3º);

- **Incidente alto:** evento com impacto significativo sobre os sistemas ou o acervo, sem atingir o limiar de criticidade. Requer resposta prioritária e registro formal;
- **Incidente médio** e **baixo:** ocorrências de menor impacto, tratadas conforme procedimento interno, com registro obrigatório.

Todos os incidentes, independentemente da gravidade, devem ser objeto de análise de causa raiz e de registro formal das medidas corretivas adotadas (art. 11, §2º).

E.2 Exemplos de incidentes de segurança

Entre os tipos de eventos que podem ser registrados como incidentes de segurança estão:

- tentativas repetidas de acesso não autorizado aos sistemas;
- falhas graves em sistemas informatizados;
- indisponibilidade prolongada de sistemas ou serviços tecnológicos;
- detecção de *software* malicioso (*ransomware*, vírus, *trojan*) em computadores da serventia;
- perda, furto ou dano de equipamentos que armazenam dados registrais;
- vazamento ou exposição indevida de dados pessoais ou registrais.

Os três primeiros e o último da lista são candidatos a classificação como críticos, dependendo da extensão do impacto, e podem ativar o prazo de 72 horas para comunicação à Corregedoria.

Nem todo evento tecnológico precisa ser registrado como incidente de segurança. Recomenda-se registrar apenas ocorrências relevantes que possam impactar a segurança ou o funcionamento dos sistemas.

E.3 Modelo simplificado de registro

A serventia pode manter um registro simples dos incidentes de segurança em formato de tabela.

A Tabela 20 apresenta um exemplo de estrutura que pode ser utilizada para documentar esses eventos. A coluna de gravidade e a de comunicação à Corregedoria são essenciais para demonstrar conformidade com o art. 11 do Provimento.

Tabela 20: Modelo simplificado de registro de incidentes de segurança.

Data	Descrição	Gravidade	Medidas adotadas	Impacto em Dados Pessoais (LGPD)	Comunicação à Corregedoria	Responsável
		Crítico/Alto/ Médio/Baixo			Sim/Não Data:	

Esse registro deve ser mantido de forma organizada e atualizado sempre que ocorrer um incidente relevante relacionado à segurança da informação.

A manutenção do histórico apresentado na Tabela 20 contribui para melhorar a gestão da segurança e permite identificar oportunidades de aprimoramento nas práticas adotadas pela serventia.

F Arquitetura mínima recomendada para serventias

Organização básica da infraestrutura tecnológica

A organização adequada da infraestrutura tecnológica contribui para aumentar a segurança e a confiabilidade dos sistemas utilizados pela serventia.
Na maioria das unidades, uma arquitetura simples, composta por equipamentos de rede adequados, computadores atualizados e rotinas consistentes de *backup*, já é suficiente para reduzir riscos operacionais relevantes.
O objetivo desta seção é apresentar uma estrutura mínima recomendada, que pode servir como referência para a organização segura do ambiente tecnológico da serventia.

A organização adequada da infraestrutura tecnológica contribui significativamente para a segurança dos sistemas utilizados pelas serventias do Registro Civil.

Uma arquitetura tecnológica simples e bem estruturada permite reduzir riscos operacionais, facilitar a manutenção dos sistemas e garantir maior continuidade na prestação dos serviços registrais.

A arquitetura apresentada a seguir representa um modelo mínimo recomendado para a maioria das serventias, considerando soluções amplamente disponíveis e de fácil implementação.

F.1 Princípios da arquitetura

A infraestrutura tecnológica da serventia deve ser organizada de forma a atender alguns princípios básicos de segurança e confiabilidade.

Entre os principais princípios recomendados estão:

- separação clara entre equipamentos de rede e computadores utilizados pelos usuários;
- utilização de sistemas operacionais com suporte e atualizações de segurança;
- proteção dos dados registrais por meio de *backup* e criptografia;
- controle de acesso aos sistemas por meio de contas individualizadas;
- utilização de comunicação segura entre sistemas e serviços.

A adoção desses princípios contribui para reduzir riscos tecnológicos e facilitar a gestão da infraestrutura.

F.2 Componentes principais

Uma arquitetura mínima para a infraestrutura tecnológica da serventia normalmente inclui os seguintes componentes:

- conexão de internet fornecida por provedor de acesso;
- modem ou equipamento de acesso à rede;
- roteador ou *firewall* responsável pela distribuição da rede local;
- computadores utilizados pelos usuários da serventia;
- servidor local ou sistema registral fornecido por empresa especializada;
- solução de *backup* local ou em nuvem.

Dependendo da solução tecnológica adotada pela serventia, alguns desses componentes podem estar integrados em um único sistema ou serviço.

F.3 Organização da rede local, *firewall* e segmentação por classe

O Provimento nº 213 estabelece dois requisitos distintos e cumulativos para a infraestrutura de rede das serventias: a implantação de *firewall stateful* com IPS/IDS e a adoção de segmentação lógica de rede, ambos obrigatórios para todas as classes, com nível de exigência proporcional ao porte da unidade (Anexo II, item 4; art. 7º, inciso VII; Anexo IV, item 3.4).

F.3.1 *Firewall stateful* com IPS/IDS

Atenção: *firewall stateful* é requisito obrigatório para todas as classes

O Anexo II, item 4, inciso II, e o Anexo IV, item 3.4, exigem a implantação de *firewall stateful* ou solução equivalente com IPS/IDS em todas as classes. Um simples roteador doméstico, sem inspeção de estado, não atende a esse requisito.

Um *firewall stateful* difere de um roteador comum por manter registro do estado de cada conexão ativa, bloqueando pacotes que não correspondam a conexões legítimas. O IPS (*Intrusion Prevention System*) detecta e bloqueia ativamente padrões de ataque; o IDS (*Intrusion Detection System*) identifica e registra tentativas de intrusão.

Na prática, para a maioria das serventias, esse requisito pode ser atendido por:

- **Appliance de rede** com *firmware* que implemente inspeção de estado e IPS/IDS integrado (ex.: equipamentos de linha profissional de fabricantes como Fortinet, Cisco, Ubiquiti, Sophos e similares);
- **Software** instalado em servidor dedicado (ex.: pfSense, OPNsense, ou soluções comerciais equivalentes) com módulos de IPS/IDS habilitados;
- **Solução gerenciada pelo fornecedor** do sistema registral, quando este assumir contratualmente a responsabilidade pelo perímetro de rede da serventia, desde que documentada a conformidade com os requisitos do Anexo II.

Em qualquer hipótese, o *firewall* deve ser configurado com política restritiva (*default deny*), permitindo apenas os fluxos estritamente necessários para a operação dos serviços registrais.

F.3.2 Segmentação lógica de rede por classe

O art. 7º, inciso VII do Provimento, exige separação funcional entre, no mínimo: ambiente administrativo ou de servidores e ambiente de atendimento ao público ou de dispositivos externos. A forma de implementar essa separação varia por classe:

- **Classes 2 e 3 (obrigatório):** implantação de mecanismos formais de segmentação, como *Virtual Local Area Networks* (VLANs) ou soluções tecnicamente equivalentes ou superiores (art. 7º, inciso VII, alínea a). As VLANs criam domínios de *broadcast* separados sobre a mesma infraestrutura física, isolando o tráfego do ambiente administrativo/servidores do tráfego de equipamentos de uso público ou externo. O controle de fluxo entre VLANs deve ser feito pelo *firewall*;
- **Classe 1 (obrigatório, solução simplificada admitida):** adoção de medida técnica idônea que impeça a comunicação irrestrita entre dispositivos administrativos e dispositivos de uso público (art. 7º, inciso VII, alínea b). Exemplos de soluções admitidas: rede Wi-Fi de convidados separada da rede interna por configuração do roteador; segmento físico distinto; configuração de SSID isolado sem acesso à rede administrativa. O requisito é a separação funcional demonstrável, não necessariamente via VLAN.

Exemplo prático de segmentação para Classe 1

Uma serventia de Classe 1 atende ao público em um computador conectado à internet via rede Wi-Fi. Os servidores e computadores administrativos estão em rede cabeada separada. O roteador é configurado para isolar a rede Wi-Fi de atendimento da rede administrativa interna (função "guest network" ou SSID isolado). Essa configuração, documentada no dossiê técnico, é suficiente para atender à alínea b do art. 7º, inciso VII.

F.3.3 Boas práticas complementares de rede

Independentemente da classe, recomenda-se adicionalmente:

- proteger o acesso administrativo ao *firewall*/roteador com senha forte e MFA, quando suportado;
- desabilitar protocolos e serviços desnecessários no equipamento de rede;
- manter o *firmware* do *firewall* e do roteador atualizado;
- registrar e revisar periodicamente as regras de *firewall* ativas, documentando as alterações no dossiê técnico;
- manter os equipamentos de rede em local físico seguro e com acesso restrito.

A configuração da infraestrutura de rede deve ser documentada no dossiê técnico, incluindo diagrama simplificado, descrição das VLANs ou segmentos adotados e regras de *firewall* vigentes.

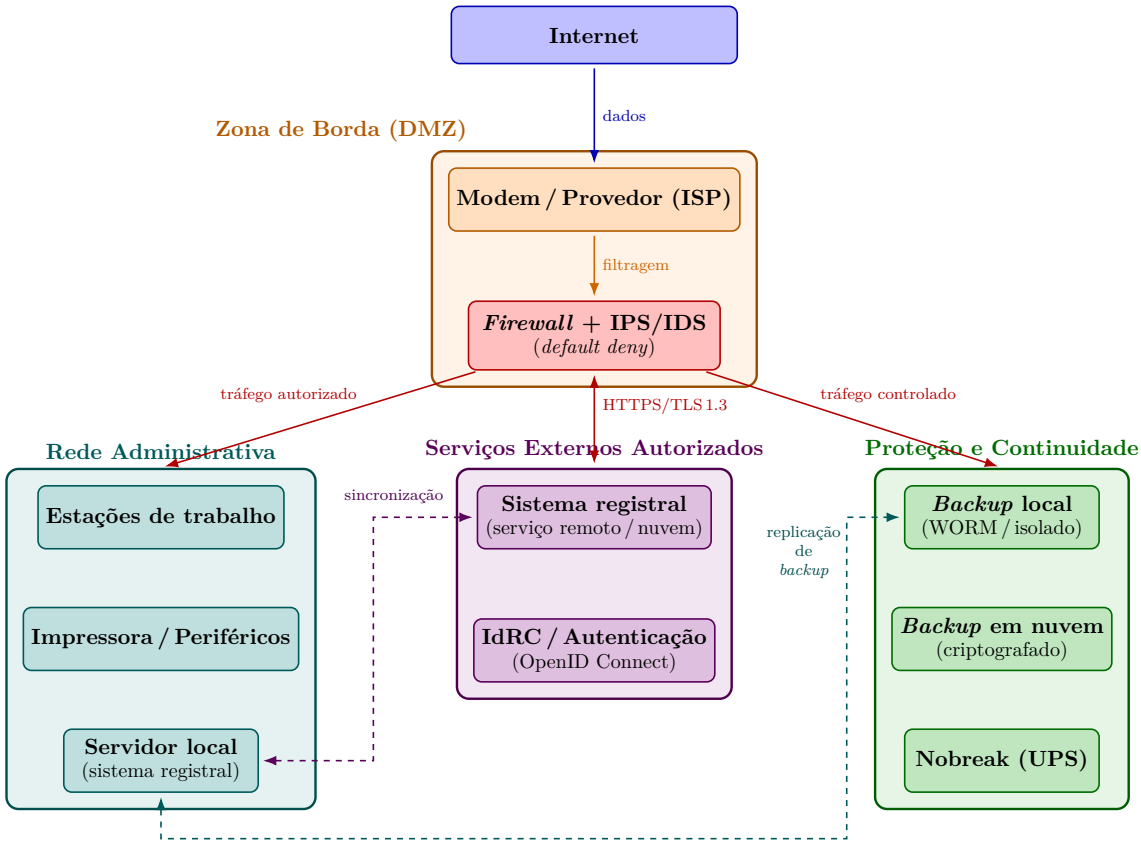
F.4 Exemplo simplificado de arquitetura

A Figura 10 apresenta um exemplo de arquitetura tecnológica mínima recomendada para serventias do Registro Civil.

A arquitetura ilustrada organiza a infraestrutura tecnológica da serventia em quatro zonas funcionais principais:

- **Zona de Borda**, responsável pela conexão com a internet e pela filtragem do tráfego de rede;
- **Rede Administrativa**, que reúne os computadores, servidores e demais equipamentos utilizados nas atividades internas da serventia;
- **Serviços Externos Autorizados**, acessados de forma segura pela internet, como

Figura 10: Exemplo de arquitetura de segurança mínima para serventias do Registro Civil, com segregação de zonas de rede, proteção de borda e mecanismos de *backup* redundante.



sistemas registrais em nuvem ou serviços de autenticação digital;

- **Zona de Proteção e Continuidade**, dedicada às rotinas de *backup*, armazenamento seguro de cópias de dados e proteção elétrica dos equipamentos.

A separação da infraestrutura em zonas é um princípio fundamental de segurança da informação. Essa organização reduz o risco de que uma falha, erro de configuração ou comprometimento de um sistema se propague livremente para os demais componentes da rede.

Nesse modelo, o *firewall*, posicionado entre a internet e a rede interna, exerce papel central na proteção da infraestrutura. É ele que controla o tráfego de rede, autoriza ou bloqueia conexões e registra eventos relevantes de segurança. Dependendo da solução utilizada, o equipamento pode ainda incorporar mecanismos de detecção e prevenção de intrusões (IPS/IDS).

O modelo apresentado deve ser entendido como uma referência mínima de organização tecnológica. Serventias de maior porte ou com maior volume de operações podem adotar arquiteturas mais elaboradas, incluindo:

- segmentação adicional de redes por meio de VLANs;
- servidores dedicados para funções específicas;
- redundância de enlaces de internet;
- sistemas avançados de monitoramento e auditoria.

Independentemente do nível de sofisticação adotado, é essencial que a arquitetura respeite os princípios de segregação de rede, controle de acesso e continuidade operacional

previstos no Provimento nº 213.

A Tabela 21 apresenta exemplos de tecnologias amplamente utilizadas que podem apoiar a implementação dos controles de segurança descritos neste guia. As soluções indicadas têm caráter meramente orientativo: outras tecnologias tecnicamente equivalentes podem ser adotadas, desde que atendam aos requisitos estabelecidos pelo Provimento.

A utilização consistente das tecnologias indicadas na Tabela 21 contribui para aumentar a segurança da infraestrutura tecnológica da serventia e facilitar o cumprimento das práticas recomendadas neste guia.

Tabela 21: Exemplos de tecnologias utilizadas na implementação dos controles de segurança.

Categoria	**Tecnologia recomendada**	**Observações**
Comunicação segura	HTTPS com TLS 1.2 ou superior (TLS 1.3 recomendado)	Padrão mínimo exigido pelo Provimento (Anexo II, item 2, inciso I). Versões anteriores, SSL, TLS 1.0 e TLS 1.1, são vedadas. Verificar a versão utilizada junto ao fornecedor do sistema registral.
Criptografia de disco	Criptografia de Dispositivo ou *BitLocker* (Windows) em modo XTS-AES 256 *FileVault* (macOS) LUKS com AES-256 (Linux)	Padrão mínimo exigido: AES-256 ou equivalente (Anexo II, item 2, inciso II). Verificar a configuração aplicada junto ao responsável técnico. Algoritmos depreciados (DES, 3DES, RC4) são vedados.
Autenticação de usuários	Contas individuais de acesso MFA	MFA é obrigatória para acessos administrativos e funcionalidades críticas (art. 5º, §2º do Provimento). Para perfis de menor risco, fator único é admitido apenas com justificativa técnica documentada. Recomenda-se integração com o IdRC.
Autenticação eletrrônica	IdRC (Registro Civil)	Sistema de autenticação baseado em OpenID Connect e OAuth, permitindo autenticação segura e federada entre sistemas.
Proteção contra malware	Ferramentas de proteção integradas ao sistema operacional	Sistemas operacionais modernos incluem mecanismos de proteção que devem ser mantidos atualizados.
Backup de dados	*Backup* automático local *Backup* em nuvem com redundância geográfica Solução híbrida (local + nuvem)	O Provimento exige dois ambientes tecnicamente independentes. Ao menos um deve estar protegido contra *ransomware* por WORM, versionamento bloqueado ou isolamento lógico. *Backups* em nuvem devem ser criptografados antes do envio, com chave sob custódia exclusiva da serventia.
Registro de eventos	Logs do sistema operacional Logs do sistema registral	Permitem rastrear operações e apoiar auditorias ou investigações de incidentes.
Infraestrutura de rede = *firewall*	*Firewall stateful* com IPS/IDS (appliance profissional ou software como pfSense/OPNsense)	Obrigatório para todas as classes (Anexo II, item 4, inciso II). Roteador doméstico simples não atende. O *firewall* deve operar com política restritiva (*default deny*) e com módulo IPS/IDS habilitado.
Infraestrutura de rede - segmentação	VLANs (Classes 2 e 3); isolamento de rede pública/admin (Classe 1)	Classes 2 e 3: VLANs ou equivalente obrigatório (art. 7º, inciso VII, alínea a). Classe 1: medida idônea que impeça comunicação irrestrita entre rede administrativa e dispositivos de uso público (alínea b). Configuração deve ser documentada no dossiê técnico.
Proteção elétrica	Nobreak	Evita perda de dados ou danos aos equipamentos em caso de queda de energia.