Corregedoria

PROVIMENTO N. 213, DE 20 DE FEVEREIRO DE 2026.

Dispõe sobre os padrões mínimos de tecnologia da informação e comunicação para garantir a segurança, a integridade, a disponibilidade, a autenticidade e a rastreabilidade, assegurando a continuidade das atividades dos serviços notariais e de registro do Brasil; revoga o Provimento n. 74, de 31 de julho de 2018; e dá outras providências.

O CORREGEDOR NACIONAL DE JUSTIÇA, no uso de suas atribuições constitucionais, legais e regimentais e

CONSIDERANDO o poder de fiscalização e o poder normativo do Poder Judiciário sobre os atos praticados por seus órgãos (art. 103-B, §4º, I, II e III, da Constituição Federal);

CONSIDERANDO a competência do Poder Judiciário para fiscalizar os serviços notariais e de registro (artigos 103-B, §4º, I e III, e 236, §1º, da Constituição Federal);

CONSIDERANDO a competência do Corregedor Nacional de Justiça para expedir provimentos e outros atos normativos destinados ao aperfeiçoamento das atividades dos serviços notariais e de registro (art. 8º, X, do Regimento Interno do Conselho Nacional de Justiça);

CONSIDERANDO a obrigação dos notários e registradores de cumprir as normas técnicas estabelecidas pelo Poder Judiciário (artigos 37 e 38 da Lei n. 8.935/1994);

CONSIDERANDO que os serviços notariais e de registro constituem atividade de organização técnica e administrativa destinada a assegurar a publicidade, a autenticidade, a segurança e a eficácia dos atos jurídicos, impondo-se que os meios operacionais empregados sejam compatíveis com tais finalidades institucionais;

CONSIDERANDO o contínuo avanço tecnológico, a crescente informatização das rotinas extrajudiciais e a implementação de sistemas eletrônicos, inclusive plataformas de registro eletrônico compartilhado, que viabilizam a prática de atos notariais e registrais mediante o emprego de tecnologias da informação e comunicação, com impacto direto sobre a forma de organização, armazenamento e circulação de dados;

CONSIDERANDO a necessidade de uniformizar critérios para a manutenção, guarda e conservação de livros, documentos, arquivos eletrônicos e mídias digitais de segurança que integram o acervo das serventias extrajudiciais, de modo a assegurar padronização procedimental, integridade informacional e eficiência administrativa;

CONSIDERANDO a imperiosa necessidade de adequação contínua do serviço notarial e de registro no Brasil, composto por mais de 12.000 (doze mil) serventias extrajudiciais marcadas por expressivas assimetrias estruturais, econômicas e tecnológicas, aos padrões contemporâneos de segurança da informação, bem como a urgência na adoção de mecanismos estruturados de defesa cibernética aptos a resguardar as bases de dados e os sistemas informatizados, garantindo a confidencialidade, a integridade, a disponibilidade e a rastreabilidade do acervo digital;

CONSIDERANDO que a implementação de padrões modernos de tecnologia da informação e de planos de continuidade de negócios deve observar diretriz de progressividade e proporcionalidade regulatória, com vistas a compatibilizar o incremento dos níveis de maturidade tecnológica com a diversidade de capacidades operacionais e econômicas das serventias extrajudiciais;

CONSIDERANDO as críticas, contribuições técnicas e sugestões apresentadas nos autos do Processo nº 09274/2024, em trâmite no Conselho Nacional de Justiça, as quais evidenciam a necessidade de aperfeiçoamento normativo e de consolidação de parâmetros objetivos de conformidade,

RESOLVE:

Art. 1º Este Provimento estabelece os padrões mínimos de tecnologia da informação e comunicação (TIC) a serem observados no exercício das atividades notariais e de registro no Brasil, com vistas a assegurar o adequado planejamento, a segurança, a integridade, a disponibilidade e a continuidade dos serviços.

Art. 2º Para os fins deste Provimento, consideram-se:

I - alta disponibilidade: arquitetura tecnológica destinada a assegurar continuidade operacional mediante redundância de componentes, mecanismos automáticos de *failover* e redução significativa de indisponibilidade não planejada;

II - arquitetura compartilhada: arranjo sistêmico de infraestrutura tecnológica utilizado por duas ou mais serventias, mediante compartilhamento de recursos de hardware, rede, serviços ou governança, seja sob forma cooperativa entre unidades, seja mediante utilização de infraestrutura comum mantida por entidade representativa e/ou por Operador Nacional, podendo dar suporte a uma ou mais soluções tecnológicas;

III - classe da serventia: categoria de enquadramento econômico definida com base na arrecadação bruta semestral, utilizada como critério de proporcionalidade regulatória para gradação de prazos, exigências técnicas e níveis mínimos de controle;

IV - contratação individual de soluções tecnológicas: modelo bilateral de aquisição, licenciamento ou prestação de serviços tecnológicos destinados exclusivamente à serventia contratante, sem compartilhamento estrutural com outras unidades;

V - dados críticos: informações cuja perda, alteração, indisponibilidade ou divulgação indevida possa comprometer a validade jurídica dos atos, a continuidade do serviço ou a proteção de dados pessoais, compreendendo, no mínimo, livros e atos eletrônicos, bases registrais, trilhas de auditoria, backups, integrações sistêmicas e dados sensíveis;

VI - dossiê técnico: conjunto organizado, íntegro e verificável de evidências documentais, técnicas e operacionais destinadas a demonstrar o cumprimento de etapa ou requisito específico, apto à fiscalização pela Corregedoria competente;

VII - 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, exigindo comunicação imediata à Corregedoria competente;

VIII - interoperabilidade: capacidade técnica de sistemas distintos de trocar, interpretar e utilizar informações de forma segura, padronizada e funcionalmente integrada, assegurada a preservação da integridade e da rastreabilidade dos dados;

IX - modelos de fornecimento como serviço (*as a service*): regime contratual em que a infraestrutura, a plataforma ou a aplicação tecnológica é disponibilizada por fornecedor externo sob forma de serviço continuado, incluindo, entre outros modelos, *Software as a Service* (SaaS), *Platform as a Service* (PaaS) e *Infrastructure as a Service* (IaaS);

X - Plano de Continuidade de Negócios (PCN): conjunto estruturado de procedimentos destinados a assegurar a continuidade da prestação do serviço em situações de indisponibilidade;

XI - Plano de Recuperação de Desastres (PRD): conjunto de medidas técnicas e operacionais voltadas à restauração de sistemas e dados após incidente grave;

XII - portabilidade de dados: possibilidade de extração, transferência e reutilização estruturada dos dados da serventia, em formato interoperável e tecnicamente acessível, sem perda de integridade, rastreabilidade ou autenticidade;

XIII - reversibilidade: garantia contratual e técnica de restituição integral e utilizável dos dados, configurações e registros da serventia ao seu titular, em caso de encerramento contratual, substituição de fornecedor ou transição de gestão;

XIV - RPO (*Recovery Point Objective*): ponto máximo de perda de dados aceitável em caso de incidente;

XV - RTO (*Recovery Time Objective*): tempo máximo admissível para restabelecimento das operações;

XVI - solução compartilhada: modelo de uso de software ou plataforma em que duas ou mais serventias operam em ambiente computacional unificado, sob segregação lógica de dados e controles;

XVII - solução coletiva: modelo de contratação ou de governança conjunta por duas ou mais serventias para implementação ou utilização de solução tecnológica comum, com compartilhamento de decisões estratégicas, de custos ou de gestão contratual, independentemente da arquitetura técnica adotada;

XVIII - solução contratada: modelo caracterizado pela dependência estrutural da serventia em relação a terceiros para a manutenção, atualização, evolução ou hospedagem de sistemas, independentemente do modelo de negócio (licenciamento, prestação continuada ou *as a service*), configurada sempre que o delegatário não detiver controle técnico pleno ou autonomia sobre:

a) a manutenção corretiva e as atualizações vitais à operação;

b) a infraestrutura crítica de processamento ou armazenamento (hospedagem);

c) os mecanismos de segurança e a custódia de chaves criptográficas; ou

d) a extração integral, autônoma e documentada do acervo em formato interoperável, sem necessidade de anuência ou intervenção do fornecedor;

XIX - solução própria: modelo em que a serventia detém autonomia estrutural quanto à organização, custódia, administração e operação de sua infraestrutura tecnológica e de seus ativos críticos, mantendo sob sua gestão integral os controles de segurança, a governança técnica e a capacidade de manutenção e evolução do sistema, ainda que conte com apoio técnico terceirizado;

XX - autonomia estrutural: quando a serventia detenha controle técnico suficiente sobre a continuidade operacional, os mecanismos essenciais de segurança e a extração integral e migrável do acervo, inexistindo dependência estrutural de fornecedor para a continuidade, atualização ou administração essencial da solução;

XXI - tolerância a falhas: capacidade técnica de sistemas ou infraestruturas de continuar operando, ainda que com desempenho reduzido, diante da ocorrência de falha parcial de componentes;

XXII - vulnerabilidade crítica: falha técnica ou fragilidade de configuração cuja exploração efetiva ou potencial apresente risco relevante de comprometimento da integridade, da disponibilidade, da autenticidade, da confidencialidade ou da rastreabilidade do acervo, dos sistemas ou da continuidade do serviço;

XXIII - Corregedoria competente: Corregedoria do Tribunal de Justiça do Estado ou do Distrito Federal que detenha competência de fiscalização e controle sobre o foro extrajudicial.

§1º Para os fins deste Provimento, distingue-se tolerância a falhas, caracterizada pela continuidade operacional diante de falha parcial de componente, de alta disponibilidade, entendida como arquitetura estruturada com redundância e mecanismos automáticos de *failover* destinados à minimização de indisponibilidade não planejada, admitindo-se a adoção de qualquer das soluções, isolada ou combinadamente, desde que atendidos os parâmetros de RTO e RPO aplicáveis à respectiva classe.

§2º Sempre que este Provimento fizer referência à manutenção ou ampliação dos níveis de proteção, considerar-se-ão compreendidos os requisitos de segurança, integridade, disponibilidade, autenticidade, rastreabilidade e continuidade do serviço, bem como o objetivo de assegurar a autenticidade, segurança e eficácia dos atos jurídicos, observada a legislação pertinente à proteção de dados pessoais, no que tange à publicidade.

Art. 3º Magistrados, delegatários, interinos e interventores deverão adotar e manter políticas de gestão, fiscalização e controle que assegurem, no tratamento de dados e informações, confidencialidade (quando aplicável, nos termos da legislação), integridade, disponibilidade, autenticidade e rastreabilidade dos atos praticados.

§1º Os serviços notariais e de registro deverão instituir, desde a entrada em vigor deste Provimento, diretrizes formais de continuidade operacional e preservação de dados, incorporadas à Política Interna de Segurança da Informação, devendo a formalização técnica completa do Plano de Continuidade de Negócios (PCN) e do Plano de Recuperação de Desastres (PRD) observar a implementação progressiva prevista no Anexo IV.

§2º Os planos referidos no §1º deverão contemplar a identificação e a avaliação de riscos, as medidas de mitigação correspondentes e as providências de curto prazo (até 30 dias), e de médio prazo (até 90 dias), destinadas ao tratamento de incidentes e à restauração da normalidade operacional.

Art. 4º Os serviços notariais e de registro deverão observar os padrões mínimos de tecnologia da informação e comunicação estabelecidos nos Anexos deste Provimento, de acordo com as classes nele definidas.

§1º Os Anexos deste Provimento integram-no para todos os fins, possuindo natureza normativa e caráter vinculante, devendo ser observados integralmente, sem prejuízo das disposições constantes do corpo principal deste ato.

§2º Todos os softwares utilizados pelas serventias deverão possuir licenciamento regular para uso comercial, admitindo-se aqueles de código aberto ou de livre distribuição, desde que compatíveis com as normas de segurança da informação e demais disposições deste Provimento.

§3º Não será admitida, para fins de cumprimento dos requisitos deste Provimento, a utilização de sistemas operacionais, sistemas gerenciadores de banco de dados, aplicações críticas ou quaisquer componentes tecnológicos cujo ciclo de suporte oficial pelo fabricante tenha sido encerrado (*End of Life* - EOL), devendo a serventia manter evidência documental atualizada da vigência do suporte técnico e das atualizações de segurança.

§4º Os requisitos técnicos detalhados nos Anexos constituem desdobramento operacional das normas gerais estabelecidas no corpo principal deste Provimento e deverão ser interpretados de forma integrada e proporcional à classe da serventia, prevalecendo, em caso de aparente sobreposição dentro da mesma classe normativa, a disposição que estabelecer o padrão funcionalmente mais protetivo.

§5º A implementação dos requisitos previstos neste Provimento e em seus Anexos observará, além da proporcionalidade por classe, a matriz necessidade/utilidade e a matriz custo/benefício, reputando-se atendido o dever de conformidade quando a serventia demonstrar, em dossiê técnico ou relatório simplificado, firmado por profissional qualificado e produzido sob responsabilidade do delegatário, interino ou interventor, que adotou solução tecnicamente equivalente ou superior ao requisito funcional estabelecido.

§6º Para as serventias enquadradas na Classe 1, o relatório simplificado de implementação previsto no Anexo IV será considerado forma adequada e suficiente de comprovação, dispensada a estrutura ampliada de dossiê técnico, sem prejuízo da responsabilidade do delegatário quanto à veracidade e à manutenção das evidências.

Art. 5º Os responsáveis pelas serventias extrajudiciais e seus colaboradores, inclusive prepostos e fornecedores, deverão utilizar mecanismos de autenticação individualizados e compatíveis com seus perfis de acesso, com as funções efetivamente exercidas e com o grau de risco associado às atividades desempenhadas, de modo a assegurar a identificação do usuário, a rastreabilidade das ações praticadas e a responsabilização individual por ações ou por omissões.

§1º As obrigações previstas neste artigo são cumpridas sob a responsabilidade pessoal do titular da delegação, ainda que executadas por colaboradores, prepostos, terceiros ou fornecedores contratados.

§2º Ressalvado o previsto em normas específicas, para o atendimento do disposto no caput, deverão ser empregados mecanismos seguros de autenticação, observando-se, como regra, a autenticação multifator nos acessos a sistemas, bases de dados ou funcionalidades críticas, admitida a autenticação por fator único apenas para perfis de menor risco, desde que tecnicamente justificada, vedado, em qualquer hipótese, o uso de credenciais compartilhadas, genéricas ou que impeçam a responsabilização individual.

§3º Admitir-se-á a utilização de contas técnicas automatizadas destinadas exclusivamente à integração entre sistemas ou à execução de rotinas sistêmicas, desde que haja segregação de privilégios, registro auditável de todas as operações, identificação inequívoca daquelas contas, do sistema responsável e vedação de sua utilização para prática direta de atos notariais e/ou de registro.

Art. 6º Os responsáveis pelas serventias extrajudiciais deverão adotar, formalizar e manter políticas de gestão que:

I - estejam alinhadas à Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e à legislação correlata;

II - assegurem a legitimidade, a autenticidade e a regularidade dos atos notariais e de registro, em conformidade com a Lei nº 6.015/1973 (artigos 23 a 26) e com a Lei nº 8.935/1994 (art. 46);

III - garantam a transferência organizada dos acervos da serventia aos eventuais sucessores, incluindo, no mínimo, bancos de dados, softwares, manuais, políticas internas, controle de acessos, inventário de ativos tecnológicos e histórico de atualizações;

IV - promovam a continuidade da prestação do serviço de forma adequada, ininterrupta, segura, eficaz e eficiente, em conformidade com planos de contingência e de continuidade de negócios, periodicamente revisados.

Parágrafo único. As políticas de gestão previstas neste artigo deverão ser implementadas e aperfeiçoadas de forma progressiva, em conformidade com as etapas estruturadas no Anexo IV, observada a ordem sequencial ali estabelecida, sem prejuízo da responsabilidade do delegatário, interino ou interventor quanto à adoção das medidas mínimas de conformidade e mitigação de riscos desde a entrada em vigor deste Provimento.

Art. 7º O delegatário, interino ou interventor, na qualidade de responsável pelo tratamento de dados pessoais no âmbito da serventia extrajudicial, deverá assegurar conformidade com a Lei nº 13.709/2018, adotando medidas técnicas e organizacionais adequadas à proteção de dados.

§1º A serventia deverá manter registro das operações de tratamento de dados, conforme exigido pela legislação vigente.

§2º Quando aplicável, deverá ser designado encarregado pelo tratamento de dados pessoais, com atribuições compatíveis com a legislação e com os riscos inerentes às atividades desempenhadas.

§3º Incidentes de segurança que possam acarretar risco ou dano relevante aos titulares deverão ser comunicados à Autoridade Nacional de Proteção de Dados e à Corregedoria competente.

Art. 8º As soluções tecnológicas utilizadas pelos serviços notariais e de registro deverão:

I - basear-se em princípios e normas técnicas reconhecidas na área de Tecnologia da Informação e Comunicação, compatíveis com os valores previstos neste Provimento e com o estímulo à inovação;

II - possibilitar integração com diferentes plataformas, assegurando a interoperabilidade;

III - evitar, sempre que possível, a dependência de fornecedores exclusivos;

IV - ser compostas por componentes devidamente licenciados, admitindo-se o uso de software livre ou de código aberto, desde que observadas as normas de segurança da informação e de conformidade aplicáveis;

V - assegurar, sempre que envolverem infraestrutura física ou virtual compartilhada entre múltiplas serventias ou entre a serventia e outros clientes do fornecedor, a segregação lógica inequívoca de dados, bases, trilhas de auditoria, backups e controles de acesso, mediante mecanismos técnicos aptos a impedir acesso, visualização, alteração ou extração indevida por terceiros, preservada a autonomia jurídica e operacional da unidade;

VI - assegurar flexibilidade arquitetural e redundância compatível com a classe da serventia, independentemente de a solução operar em ambiente local, em nuvem ou em arquitetura híbrida, desde que observados os padrões de segurança da informação e de proteção de dados pessoais;

VII - assegurar segmentação lógica de redes internas, com separação funcional entre, no mínimo, ambientes administrativos ou de servidores e ambientes destinados a atendimento ao público ou a dispositivos externos, observada a proporcionalidade segundo a classe da serventia, nos seguintes termos:

a) para as Classes 2 e 3, mediante implementação obrigatória de mecanismos formais de segmentação, tais como VLANs ou soluções tecnicamente equivalentes ou superiores;

b) para a Classe 1, mediante adoção de medida técnica idônea que impeça a comunicação irrestrita entre dispositivos administrativos e dispositivos de uso público, admitida solução simplificada equivalente ou superior, no mínimo, compatível com a infraestrutura.

§1º A caracterização da solução tecnológica adotada pela serventia (própria, contratada, compartilhada ou coletiva) deverá observar critérios materiais de governança técnica, controle efetivo dos dados, autonomia de continuidade operacional e inexistência de dependência estrutural não mitigada, prevalecendo a realidade técnica e contratual sobre a nomenclatura atribuída pelas partes.

§2º A adoção das soluções tecnológicas referidas neste artigo poderá ocorrer por meio de arquiteturas, metodologias ou combinações técnicas diversas, inclusive inovadoras, desde que assegurem, de forma objetivamente demonstrável e documentada, grau equivalente ou superior de conformidade com os padrões mínimos de segurança, integridade, disponibilidade, autenticidade, rastreabilidade e continuidade estabelecidos neste ato normativo.

§3º Todas as serventias deverão adotar mecanismos de proteção perimetral aptos a controlar o tráfego de entrada e saída de dados, impedir acessos não autorizados e registrar eventos relevantes de segurança, compatíveis com sua classe e com a criticidade de suas operações.

§4º Para as serventias enquadradas nas Classes 2 e 3, os mecanismos referidos no §3º deverão contemplar, cumulativamente:

I - inspeção ativa de tráfego em nível de rede;

II - geração e retenção de registros auditáveis de eventos de segurança;

III - capacidade de detecção e bloqueio de ameaças avançadas, inclusive por análise comportamental ou por inteligência de ameaças, admitida a adoção de soluções integradas ou dedicadas, desde que tecnicamente demonstrada a equivalência funcional.

§5º Para as serventias enquadradas na Classe 1, os mecanismos de proteção perimetral deverão, no mínimo:

I - realizar filtragem de conexões externas;

II - registrar eventos críticos de acesso e bloqueio; e

III - manter configuração formalmente documentada, passível de verificação pela Corregedoria competente.

Art. 9º Os dados sensíveis, informações pessoais, registros eletrônicos e demais informações armazenadas ou transmitidas no âmbito das serventias deverão ser protegidos por mecanismos de criptografia adequados ao estado da técnica, observadas as boas práticas reconhecidas e os padrões mínimos definidos neste Provimento.

§1º A criptografia deverá ser aplicada:

I - aos dados em trânsito, mediante protocolos seguros atualizados;

II - aos dados em repouso, especialmente quando armazenados em servidores, estações de trabalho, dispositivos móveis ou ambientes em nuvem;

III - às rotinas de backup, quando envolverem armazenamento externo ou em infraestrutura de terceiros.

§2º Os algoritmos e protocolos utilizados deverão possuir reconhecimento público, atualização ativa e suporte vigente, vedada a utilização de padrões considerados obsoletos ou vulneráveis.

§3º A gestão de chaves criptográficas deverá observar controles de acesso restritos, segregação de funções e registro de utilização, conforme definido em política interna formalizada.

Art. 10. As serventias deverão manter trilhas de auditoria (*logs*) que permitam a rastreabilidade das operações realizadas nos sistemas utilizados para prática de atos notariais e registrais, assegurando a identificação de usuários, data, hora, minuto e segundo das operações, natureza da ação executada e resultado obtido.

§1º Os registros de *log* deverão ser protegidos, no mínimo, contra alteração, exclusão não autorizada e perda acidental, devendo ser armazenados por prazo mínimo definido neste Provimento.

§2º O nível de detalhamento das trilhas de auditoria observará a classe da serventia, o volume anual de atos praticados e a criticidade da atividade desempenhada, devendo atender, no mínimo, aos níveis técnico-operacionais definidos no §3º deste artigo.

§3º Para fins deste Provimento, as trilhas de auditoria classificam-se nos seguintes níveis:

I - Nível Essencial: registro de autenticação de usuários, operações principais e eventos de erro relevantes;

II - Nível Intermediário: registro adicional de alterações cadastrais, exportações de dados e tentativas de acesso não autorizado;

III - Nível Ampliado: registro detalhado de operações administrativas, alterações de configuração e integrações sistêmicas;

IV - Nível Avançado: registro granular de eventos de sistema, correlação automatizada e monitoramento contínuo.

§4º As serventias classificadas nas Classes 1 e 2 deverão observar, no mínimo, o Nível Essencial, facultada a adoção de níveis superiores conforme avaliação de risco e disponibilidade de recursos.

§5º As serventias de Classe 3 deverão observar, no mínimo, o Nível Intermediário, podendo ser exigido nível superior mediante justificativa técnica fundada na criticidade das operações realizadas.

§6º O prazo mínimo de retenção das trilhas de auditoria será definido no Anexo II, observado o princípio da proporcionalidade por classe, sem prejuízo de prazo superior exigido por norma específica ou por determinação correcional fundamentada.

Art. 11. As serventias extrajudiciais deverão manter procedimentos documentados para gestão de incidentes de segurança da informação, contemplando, no mínimo, identificação, classificação por gravidade, medidas de contenção, erradicação, recuperação e registro das ocorrências.

§1º Incidentes classificados como críticos deverão ser comunicados à Corregedoria competente no prazo máximo definido no Anexo II, sem prejuízo das comunicações exigidas pela legislação específica.

§2º Todos os incidentes deverão ser objeto de análise de causa raiz e de registro formal das medidas corretivas adotadas.

§3º A gestão de vulnerabilidades observará os requisitos técnicos, prazos de tratamento, critérios de priorização e deveres de registro estabelecidos no Anexo II, devendo as diretrizes estratégicas correspondentes constar da Política Interna de Segurança da Informação prevista no Anexo III. Os prazos máximos e os critérios técnicos de tratamento constam exclusivamente do Anexo II, vedada interpretação autônoma de dispositivos da Política Interna que implique redução do padrão mínimo ali estabelecido.

§4º As medidas adotadas no âmbito da gestão de vulnerabilidades deverão ser registradas formalmente no dossiê técnico da serventia, com indicação da data de identificação, classificação de risco, providências implementadas e data de encerramento.

Art. 12. Os atos e livros eletrônicos deverão ser produzidos, armazenados, preservados e geridos de modo a assegurar, de forma permanente, a autenticidade, a integridade material e lógica, a imutabilidade do conteúdo jurídico originalmente praticado, a rastreabilidade das operações e, quando exigido por lei, a confidencialidade, observadas as normas de segurança da informação e de proteção de dados pessoais, inclusive quando utilizados ambientes tecnológicos externos ou em nuvem.

§1º A integridade e a imutabilidade referidas no *caput* deverão ser garantidas por mecanismos técnicos que:

I - preservem histórico verificável de versões;

II - mantenham registro comprovável de integridade;

III - impeçam modificação, substituição ou sobrescrita sem geração automática de trilha de auditoria imutável e identificável;

IV - permitam auditoria técnica independente, quando necessária.

§2º A serventia deverá manter política formal de cópias de segurança (backup), automatizada e monitorada, apta a assegurar a continuidade operacional e a recuperação íntegra do acervo eletrônico.

§3º As cópias de segurança deverão compreender:

I - cópias completas realizadas em periodicidade compatível com a classe da serventia; e

II - mecanismos adicionais de preservação contínua ou incremental de dados, aptos a assegurar a recuperação dos atos até o limite do objetivo de ponto de recuperação (RPO) aplicável.

§4º O atendimento ao RPO poderá ocorrer por meio de cópias incrementais, replicação contínua, recuperação em ponto específico no tempo (*point-in-time recovery*) ou tecnologia equivalente, não se confundindo com a periodicidade das cópias completas.

§5º Os parâmetros objetivos de RPO por classe, as periodicidades mínimas de backup e as arquiteturas técnicas aptas ao seu atendimento constam nos Anexos I e II deste Provimento.

§6º As cópias de segurança deverão ser mantidas em ambiente tecnicamente independente daquele utilizado para o processamento primário dos dados, assegurada segregação física ou lógica apta a prevenir comprometimento simultâneo, admitidas soluções em nuvem ou arquiteturas híbridas que demonstrem equivalência ou superioridade de segurança, integridade, disponibilidade e resiliência.

§7º A arquitetura de armazenamento deverá dispor de mecanismos de tolerância a falhas ou de alta disponibilidade compatíveis com a classe da serventia e com a criticidade do acervo.

§8º A infraestrutura elétrica que suporte ativos críticos de tecnologia da informação deverá possuir aterramento funcional e tecnicamente aferido, mantido laudo atualizado subscrito por profissional habilitado, com anotação de responsabilidade técnica.

§9º As rotinas de backup deverão ser submetidas a testes formais e documentados de restauração, em periodicidade compatível com a classe da serventia, nos termos definidos nos Anexos, devendo os resultados integrar o dossiê técnico.

§10. As rotinas de backup devem ser continuamente monitoradas quanto à sua execução bem-sucedida e à integridade dos dados restauráveis. Qualquer falha detectada deverá gerar, de forma imediata:

I – alerta técnico automático ao responsável;

II – registro formal do incidente, com abertura de chamado para análise e correção.

§11. A política de retenção de backups não exime o cumprimento da obrigatoriedade de guarda das trilhas de auditoria previstas no art. 10 e no Anexo II desta norma, nem autoriza a eliminação de registros cuja conservação seja exigida por legislação específica ou por determinação de autoridade competente.

§12. Constitui meta técnica de excelência, para ambientes de maior criticidade, a capacidade de recuperação de dados com defasagem inferior a 30 (trinta) minutos, quando tecnicamente viável e economicamente proporcional, nos termos definidos nos Anexos.

Art. 13. O cumprimento dos requisitos técnicos previstos neste Provimento poderá ocorrer por meio de:

I - solução própria;

II - solução contratada, inclusive sob modelos de fornecimento como serviço (SaaS, PaaS, IaaS ou equivalentes);

III - solução compartilhada;

IV - solução coletiva.

§1º Os modelos previstos neste artigo poderão ser adotados de forma isolada ou combinada, desde que, considerados em conjunto, assegurem o atendimento integral dos requisitos estabelecidos neste Provimento e em seus Anexos.

§2º A contratação de terceiros poderá ser realizada de forma individual ou coletiva, inclusive por intermédio de Operador Nacional e/ou de entidade representativa de notários e/ou registradores regularmente constituída e gerida por delegatários.

§3º A responsabilidade pelo cumprimento integral dos requisitos normativos permanece pessoal e indelegável do delegatário, interino ou interventor responsável pela serventia, ainda que haja contratação de terceiros ou participação em solução coletiva e/ou compartilhada.

§4º Quando o cumprimento dos requisitos técnicos previstos neste Provimento ocorrer por meio de plataforma nacional estruturada, solução coletiva ou ambiente tecnológico mantido por entidade representativa de notários e/ou registradores e/ou por operador nacional regularmente instituído, admitir-se-á a centralização material da implementação dos controles técnicos, desde que:

I - a entidade mantenedora demonstre, por meio de documentação técnica formal e auditável, a conformidade integral ou equivalente com os requisitos estabelecidos neste Provimento e em seus Anexos;

II - a serventia mantenha, em seu dossiê técnico, evidência atualizada da adesão à plataforma, da abrangência dos controles implementados centralmente e da compatibilidade destes com sua classe;

III - permaneça assegurada a responsabilidade pessoal e funcional do delegatário quanto à governança local, ao controle de acessos internos, à gestão de incidentes, à integração com seus planos de continuidade e à observância da legislação de proteção de dados pessoais.

§5º A implementação centralizada referida no §4º não implica dispensa normativa das serventias quanto ao dever de conformidade, mas autoriza que a comprovação de requisitos estruturais seja realizada por meio de certificação ou documentação coletiva emitida pela entidade mantenedora, sem prejuízo da fiscalização correicional individual.

§6º As contratações deverão conter, no mínimo, cláusulas que assegurem confidencialidade, reversibilidade, portabilidade de dados, gestão de incidentes e observância integral da Lei nº 13.709/2018.

§7º Quando a solução tecnológica estrutural for mantida por entidade representativa de notários e/ou de registradores, Operador Nacional ou por outro fornecedor que atenda a múltiplas serventias, a validação técnica estrutural realizada uma única vez, mediante relatório técnico abrangente e auditável, produzirá efeito para todas as serventias usuárias quanto aos requisitos estruturais, cabendo à fiscalização individual restringir-se aos controles locais de governança, gestão de acessos e integração operacional.

Art. 14. A adoção de solução própria, contratada, compartilhada ou coletiva não afasta nem mitiga a autonomia jurídica da serventia extrajudicial, permanecendo íntegra a responsabilidade pessoal do delegatário, interino ou interventor quanto aos atos praticados e ao cumprimento das obrigações legais, regulamentares e correicionais.

Parágrafo único. A centralização material de controles técnicos, quando admitida nos termos deste Provimento, não implica transferência de responsabilidade funcional nem exoneração do dever de governança local, fiscalização interna e conformidade normativa.

Art. 15. Considera-se mitigada a dependência estrutural em relação a fornecedor ou entidade mantenedora quando houver, cumulativamente:

I – cláusula contratual expressa que assegure reversibilidade integral e portabilidade de dados em formato interoperável, estruturado e não proprietário;

II – comprovação documental de realização de teste de extração integral do acervo, nos termos do Anexo IV;

III – inexistência de restrição técnica ou contratual que impeça a migração do acervo para outra solução sem necessidade de anuência discricionária do fornecedor.

§1º A mitigação da dependência estrutural não afasta o dever de supervisão contínua da solução tecnológica adotada nem dispensa a manutenção de evidências atualizadas no dossiê técnico ou relatório simplificado, conforme a classe da serventia.

§2º A caracterização da mitigação será aferida à luz da realidade técnica e contratual efetivamente existente, prevalecendo o conteúdo material da relação sobre a nomenclatura adotada pelas partes.

Art. 16. Para os fins deste Provimento e dos demais atos normativos correlatos, as serventias extrajudiciais serão enquadradas conforme a arrecadação bruta semestral, apurada na forma das diretrizes expedidas pela Corregedoria Nacional de Justiça, adotando-se como referência o valor máximo fixado para cada classe e as escalas internas a ele associadas:

I - A Classe 1 abrange as unidades cuja receita semestral não ultrapasse R$ 100.000,00 (cem mil reais), organizando-se em três faixas equivalentes, calculadas sobre esse montante: Subclasse A, até um terço do teto; Subclasse B, acima de um terço e até dois terços; Subclasse C, acima de dois terços e até o valor integral estabelecido para a classe;

II - A Classe 2 compreende as unidades cuja receita supere o marco da Classe 1 e não exceda R$ 500.000,00 (quinhentos mil reais), distribuindo-se igualmente em três segmentos proporcionais ao respectivo teto: Subclasse D, até um terço do limite da classe; Subclasse E, acima de um terço e até dois terços; Subclasse F, acima de dois terços e até o valor integral estabelecido para a classe;

III - A Classe 3 alcança as unidades cuja receita ultrapasse o limite da Classe 2, sendo suas subdivisões definidas por múltiplos daquele valor: Subclasse G, até três vezes esse valor; Subclasse H, acima de três e até seis vezes; Subclasse I, acima de seis e até doze vezes esse valor; e Subclasse J, acima de doze vezes o mesmo referencial.

§1º O enquadramento da serventia deverá ser reavaliado anualmente, com base na arrecadação do semestre imediatamente anterior, produzindo efeitos para o período subsequente, observados os prazos de adaptação previstos neste Provimento.

§2º Os limites de arrecadação definidos neste artigo serão automaticamente atualizados a cada ano de vigência deste Provimento, pelo IPCA ou por outro índice oficial que venha a substituí-lo.

§3º A migração de classe ou subclasse não produzirá efeitos imediatos quando a variação da arrecadação não ultrapassar dez por cento do limite superior da faixa anterior, hipótese em que será exigida consolidação por dois ciclos consecutivos.

Art. 17. Em campo próprio do banco de dados público nominado Sistema Justiça Aberta, os responsáveis pelas serventias extrajudiciais (exercentes de função dotada de fé pública) deverão declarar o cumprimento das diversas fases previstas para as sucessivas etapas, consideradas necessárias à integral execução deste ato normativo, prestando os esclarecimentos que venham a ser requisitados pelas Corregedorias, bem como apresentando a documentação pertinente.

§1º A declaração referida no *caput* deverá ser renovada anualmente e acompanhada de síntese do dossiê técnico, contendo evidências mínimas de conformidade com os requisitos estruturais e operacionais previstos neste Provimento e em seus Anexos.

§2º A declaração falsa, objetivamente verificada em inspeções ou em correições, sujeitará o responsável às penalidades previstas em lei.

Art. 18. Os atos normativos da Corregedoria Nacional de Justiça que disponham sobre tecnologia da informação e segurança da informação deverão ser interpretados de forma sistemática, integrada e orientada à máxima efetividade da proteção do acervo, da continuidade do serviço, da autenticidade, da segurança e da eficácia dos atos jurídicos.

Parágrafo único. É vedada interpretação isolada de dispositivos que conduza à exclusão de deveres técnicos, à redução dos níveis mínimos de proteção normativa ou à fragmentação dos regimes de segurança, auditoria e continuidade dos serviços extrajudiciais.

Art. 19. As soluções tecnológicas adotadas pelas serventias extrajudiciais deverão ser tecnicamente aptas à integração com plataformas eletrônicas de fiscalização e controle, observados padrões mínimos nacionais de interoperabilidade que assegurem, cumulativamente:

I - a capacidade de intercâmbio estruturado de dados em formato aberto ou tecnicamente equivalente, apto à leitura automatizada e à preservação da integridade e da consistência das informações;

II - a identificação inequívoca da serventia emissora e do sistema solicitante, com mecanismos idôneos de verificação de autenticidade e integridade das informações transmitidas;

III - a utilização de canal seguro de comunicação, compatível com o estado da técnica, apto a resguardar a confidencialidade, a integridade e a rastreabilidade das operações realizadas;

IV - a manutenção de registros auditáveis das integrações efetuadas.

§1º A integração referida no *caput* poderá ocorrer por meio de interfaces técnicas, serviços eletrônicos ou mecanismos estruturados de disponibilização, envio ou acesso autenticado a dados, inclusive em ambientes tecnológicos compartilhados ou em nuvem, desde que preservados a segregação lógica por serventia, os limites legais de sigilo e a finalidade fiscalizatória.

§2º A implementação observará critérios de proporcionalidade conforme a classe da serventia e respeitará as normas de proteção de dados pessoais, vedada a imposição de solução tecnológica específica quando demonstrada equivalência funcional aos padrões estabelecidos neste artigo.

Art. 20. A implementação inicial obrigatória dos requisitos previstos neste Provimento, correspondente à conclusão das Etapas 1 e 2 do Anexo IV, relativas à governança, à conformidade legal, à infraestrutura e à continuidade operacional, deverá ocorrer nos seguintes prazos, contados da data de entrada em vigor deste Provimento:

I – 90 (noventa) dias, para as serventias enquadradas na Classe 3;

II – 150 (cento e cinquenta) dias, para as serventias enquadradas na Classe 2;

III – 210 (duzentos e dez) dias, para as serventias enquadradas na Classe 1.

§1º A exigibilidade plena dos requisitos técnicos e organizacionais previstos neste Provimento deverá ser interpretada de forma sistemática e integrada com o Anexo IV.

§2º Os prazos estabelecidos no *caput* não autorizam:

I – a declaração formal de conclusão de etapa posterior sem o cumprimento integral e comprovado dos requisitos da etapa imediatamente anterior, não se vedando, contudo, a implementação técnica voluntária e antecipada de controles mais avançados, desde que preservada a ordem sequencial para fins de certificação formal;

II – a postergação dos requisitos estruturais mínimos das Etapas 1 e 2;

III – o afastamento das medidas mínimas de mitigação de risco expressamente previstas neste ato normativo.

Art. 21. As Corregedorias dos Tribunais de Justiça poderão, de forma excepcional e mediante decisão fundamentada, prorrogar, uma única vez, os prazos previstos no art. 20 por até 90 (noventa) dias, quando demonstrada inviabilidade temporária de adequação de natureza técnica ou financeira, desde que a serventia:

I – apresente plano formal de adequação com cronograma definido e indicação de responsáveis; e

II – implemente imediatamente medidas compensatórias mínimas de redução de risco, conforme orientação técnica da Corregedoria competente.

§1º Para as serventias da Classe 1, o requerimento de prorrogação será submetido a análise simplificada pela Corregedoria competente.

§2º As serventias das Classes 2 e 3 deverão apresentar requerimento formal à respectiva Corregedoria, indicando de forma objetiva as razões do pedido, os elementos probatórios pertinentes, inclusive orçamentos, e as providências que serão adotadas ao longo da prorrogação para a ultimação do cumprimento das normas técnicas eventualmente inadimplidas, inclusive aquelas pertinentes ao Provimento nº 74/2018, bem como das normas integrantes deste Provimento.

Art. 22. As serventias poderão implementar os requisitos técnicos previstos nas Etapas 3 a 5 do Anexo IV em regime progressivo de maturidade, observada a proporcionalidade por classe e os prazos máximos estabelecidos no art. 23.

§1º As serventias enquadradas na Classe 3 poderão apresentar plano estruturado de evolução de maturidade em segurança da informação, com horizonte máximo de 24 (vinte e quatro) meses, observado o prazo global previsto no art. 23, desde que:

I – cumpram integralmente, desde o primeiro ciclo, os requisitos mínimos relativos à criptografia, à autenticação multifator para acessos administrativos, à gestão de incidentes e à conformidade com a Lei nº 13.709/2018;

II – apresentem cronograma formal de aprimoramento progressivo dos controles avançados de monitoramento, gestão de vulnerabilidades e automação de auditoria;

III – submetam-se à primeira avaliação técnica no prazo máximo de 12 (doze) meses.

§2º As serventias das Classes 1 e 2 poderão implementar os requisitos de monitoramento avançado e automação de auditoria em regime progressivo de maturidade, desde que observem imediatamente os requisitos mínimos relativos à criptografia, à gestão de incidentes, à conformidade com a Lei nº 13.709/2018 e à proteção de backups.

§3º As Etapas 3 a 5 do Anexo IV permanecem submetidas aos regimes de progressividade, maturidade e proporcionalidade estabelecidos neste artigo e nos Anexos.

Art. 23. A implementação cumulativa e integral de todas as etapas previstas no Anexo IV deverá estar concluída nos seguintes prazos máximos, contados da data de entrada em vigor deste Provimento, observada a implementação inicial obrigatória prevista no art. 20 como fase integrante e indissociável do cronograma global:

I - até 24 (vinte e quatro) meses, para as serventias enquadradas na Classe 3;

II - até 30 (trinta) meses, para as serventias enquadradas na Classe 2;

III - até 36 (trinta e seis) meses, para as serventias enquadradas na Classe 1.

Parágrafo único. Os prazos máximos estabelecidos neste artigo englobam os prazos de implementação inicial previstos no art. 20, os quais constituem fase obrigatória e preliminar do cronograma global de adequação, devendo a execução das etapas subsequentes observar a ordem sequencial e cumulativa definida no Anexo IV.

Art. 24. O descumprimento injustificado dos requisitos técnicos e organizacionais previstos neste Provimento, quando caracterizada negligência, imprudência ou omissão relevante do titular da delegação, poderá ensejar a instauração de procedimento administrativo disciplinar, sem prejuízo das responsabilidades civis e penais cabíveis.

Art. 25. O acompanhamento e a fiscalização do cumprimento deste ato normativo observará metodologia orientada por risco, com priorização de serventias cuja situação revele maior probabilidade ou maior potencial de impacto decorrente de eventual não conformidade.

§1º Para os fins deste artigo, consideram-se, entre outros elementos indicativos de risco:

I – indícios objetivamente verificáveis de não conformidade, compreendidos como inconsistências entre informações declaradas e dados disponíveis, evidências externas de falhas não reportadas, ausência de documentação mínima exigida ou padrões reiterados de comportamento incompatíveis com as obrigações previstas neste ato;

II – informações desatualizadas ou ausência de atualização periódica dos dados e documentos exigidos;

III – inconsistências detectadas por cruzamento de bases ou por análise técnica de coerência entre dados econômicos, operacionais e estruturais;

IV – reincidência de falhas não sanadas ou fatores de criticidade operacional que elevem o potencial impacto sistêmico de eventual interrupção, indisponibilidade ou comprometimento da integridade do serviço.

§2º Consideram-se fatores de criticidade operacional, para os fins do inciso IV do §1º, elementos relacionados ao volume de atos praticados, à posição estratégica na rede de prestação de serviço extrajudicial, ao grau de interconexão tecnológica, à dependência de infraestrutura compartilhada ou a outras circunstâncias que ampliem o alcance social, econômico ou jurídico de eventual falha.

Art. 26. Fica revogado o Provimento nº 74, de 31 de julho de 2018.

Ministro **MAURO CAMPBELL MARQUES**

ANEXO I

INFRAESTRUTURA TECNOLÓGICA MÍNIMA

Disposição geral:

Este Anexo estabelece os requisitos estruturais mínimos de infraestrutura tecnológica necessários à continuidade operacional dos serviços notariais e de registro, compreendendo elementos físicos, energéticos, de conectividade e de suporte técnico, sem prejuízo dos controles de segurança previstos nos Anexos II e III. Os requisitos técnicos nele previstos constituem parâmetros mínimos compatíveis com o estado da técnica vigente à época da edição deste Provimento. Sempre que houver evolução tecnológica ou substituição de padrões, admitir-se-á a adoção de soluções tecnicamente equivalentes ou superiores, desde que assegurada, de forma demonstrável, a manutenção ou ampliação dos níveis de segurança, disponibilidade, integridade, rastreabilidade e continuidade exigidos neste ato normativo.

1. Infraestrutura de energia

I - utilização de fonte de energia estável e confiável;

II - sistema de aterramento adequado às normas técnicas vigentes;

III - utilização de Sistema de Alimentação Ininterrupta (SAI/UPS) ou solução tecnicamente equivalente, com autonomia suficiente para assegurar o salvamento de dados em memória, o encerramento seguro das transações ativas e o desligamento ordenado dos equipamentos (*safe shutdown*), recomendando-se, preferencialmente, autonomia estendida de 30 (trinta) minutos;

IV - previsão de plano de contingência energética compatível com a classe da serventia.

2. Conectividade e rede

I - conexão à internet com capacidade compatível com o pleno funcionamento dos sistemas informatizados e integrações obrigatórias;

II - as velocidades nominais mínimas indicadas constituem referência compatível com o cenário tecnológico atual e poderão ser substituídas por métricas técnicas mais adequadas à evolução dos serviços digitais, desde que assegurado desempenho efetivo compatível com a classe da serventia, com as integrações obrigatórias e com o cumprimento dos parâmetros de RTO e RPO definidos neste Provimento.

III - as atuais velocidades mínimas de referência são:

a) Classe 1: 2 Mbps;

b) Classe 2: 10 Mbps;

c) Classe 3: 50 Mbps;

IV - As velocidades nominais previstas neste item possuem caráter referencial. Considera-se atendido o requisito de conectividade quando a serventia demonstrar, por meio de 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 contratada;

V - Para fins de atendimento ao critério de desempenho efetivo referido neste inciso, admite-se a adoção de soluções complementares ou alternativas de continuidade e restauração, tais como armazenamento local redundante, replicação híbrida, cópia de segurança local sincronizada com nuvem, procedimentos de "*seed*" inicial, ou outros meios tecnicamente equivalentes, desde que documentados no PCN/PRD e aptos a demonstrar, de modo verificável, a aderência ao RTO e ao RPO estabelecidos;

VI - utilização de roteador para gerenciamento das conexões internas e externas;

VII - utilização de comutador (*switch*) para conexão dos dispositivos internos;

VIII - possibilidade de múltiplos links ou tecnologia equivalente que assegure desempenho efetivo compatível com a classe da serventia.

2.1. Para a Classe 1, a adoção de arquitetura de alta disponibilidade, redundância simultânea de links ou duplicação integral de infraestrutura não constitui requisito obrigatório quando o RTO e o RPO definidos para a respectiva classe forem comprovadamente atendidos por meio de backup periódico testado e procedimento documentado de restauração, observado o prazo máximo de 24 (vinte e quatro) horas.

3. Ambiente físico e proteção estrutural

I - existência de espaço físico isolado para equipamentos críticos, com controle de acesso restrito, quando houver infraestrutura local; nas hipóteses de utilização integral de infraestrutura em nuvem, deverá ser mantida documentação contratual que comprove ou ao menos indicie a adoção, pelo fornecedor, de controles equivalentes de segurança física e ambiental;

II - proteção contra incêndios, inundações, variações térmicas e acesso indevido;

III - organização física adequada à preservação da integridade dos ativos tecnológicos.

4. Infraestrutura de segurança perimetral básica

I - utilização de solução de proteção de endpoint (antivírus/antimalware);

II - implantação de firewall stateful ou solução equivalente com IPS/IDS;

III - segmentação lógica mínima de rede compatível com a criticidade da serventia.

5. Armazenamento estrutural e disponibilidade

I - utilização de SGBD com integridade transacional e rastreabilidade (*logs*);

II - para as Classes 1 e 2, considera-se atendido o requisito de tolerância a falhas ou alta disponibilidade mediante adoção de arquitetura que, sem exigir duplicação plena de todos os componentes, assegure, de modo verificável, o cumprimento do RTO e do RPO definidos no PCN/PRD, admitindo-se, entre outras soluções equivalentes: (a) virtualização com restauração automatizada; (b) '*warm standby*' ou imagem pronta para recuperação; (c) serviços gerenciados em nuvem com redundância regional; ou (d) redundância local simples com reposição rápida, desde que documentadas as premissas e os testes de restauração;

III - Para a Classe 3, mecanismos de tolerância a falhas (*Fault Tolerance*) ou alta disponibilidade (HA), compatíveis com a classe da serventia;

IV - backups automatizados *off-site*, com redundância geográfica;

V - realização obrigatória de testes documentados de restauração com periodicidade mínima semestral para Classe 3 e anual para Classes 1 e 2;

VI - preservação dos registros de testes de restauração pelo prazo mínimo de 5 (cinco) anos, sem prejuízo de prazo superior quando exigido pela Corregedoria competente em procedimento específico;

VII - implementação dos mecanismos de tolerância a falhas, alta disponibilidade ou redundância por meio de tecnologias diversas, físicas ou virtuais, locais ou em nuvem, desde que assegurado nível de resiliência igual ou superior ao exigido neste Anexo.

5.1. Os prazos de guarda previstos neste item aplicam-se exclusivamente aos registros técnicos de testes de restauração e não afastam os prazos de guarda documental e probatória estabelecidos nas Disposições Gerais do Anexo IV.

6. Equipamentos e suporte técnico

I - disponibilidade de equipamentos adequados à operação regular dos sistemas;

II - disponibilidade de digitalizadores e impressoras compatíveis com a gestão documental;

III - existência de suporte técnico próprio ou contratado com atendimento contínuo.

7. Capacitação mínima operacional

I - treinamento periódico dos responsáveis e colaboradores quanto à operação segura dos sistemas e rotinas de backup;

II - registro formal das capacitações realizadas.

ANEXO II

SEGURANÇA DA INFORMAÇÃO E CONTROLES TÉCNICOS

Disposição geral:

Este Anexo estabelece os controles técnicos mínimos de segurança da informação a serem observados pelas serventias extrajudiciais. Os controles nele descritos constituem expressões concretas de requisitos funcionais mínimos de proteção. A adoção de tecnologias distintas das exemplificadas será admitida, desde que comprovadamente aptas a assegurar grau equivalente ou superior de segurança, integridade, disponibilidade e rastreabilidade, devendo tal equivalência ser objetivamente demonstrável, de forma técnica.

1. Controle de acesso e autenticação

I - autenticação individualizada para todos os usuários;

II - autenticação multifator (AMF/MFA) obrigatória para acessos administrativos, de gestão de sistemas, bancos de dados e funcionalidades críticas;

III - vedação expressa ao uso de contas genéricas ou credenciais compartilhadas;

IV - segregação lógica de perfis conforme princípio da necessidade.

2. Criptografia

I - utilização de criptografia para dados em trânsito, com protocolos equivalentes a TLS 1.2 ou superior, ou versões mantidas e suportadas;

II - utilização de criptografia para dados críticos em repouso, conforme definição do art. 2º, V, com robustez equivalente, no mínimo, a AES-256 ou padrão tecnicamente equivalente ou superior reconhecido pela comunidade técnica especializada;

III - vedação ao uso de algoritmos, versões ou modos depreciados;

IV - gestão formal e segura de chaves criptográficas, com controle de acesso restrito, segregação de funções e registro de operações relevantes.

V - revisão periódica dos padrões criptográficos adotados, com substituição obrigatória de protocolos ou algoritmos que se tornem obsoletos ou inseguros, assegurada a adoção de padrões reconhecidos como adequados pela comunidade técnica especializada e compatíveis com o estado da técnica.

2.1. Parâmetros mínimos de RPO por classe

I – Classe 3: RPO máximo de 4 (quatro) horas;

II – Classe 2: RPO máximo de 12 (doze) horas;

III – Classe 1: RPO máximo de 24 (vinte e quatro) horas.

§1º Os valores estabelecidos neste item constituem parâmetros funcionais mínimos de ponto máximo de perda de dados admissível, podendo ser superados por solução tecnicamente mais protetiva.

§2º A demonstração de atendimento ao RPO deverá constar do PCN/PRD e do dossiê técnico ou relatório simplificado, conforme a classe.

2.2. Parâmetros mínimos de RTO por classe

I – Classe 3: RTO máximo de 8 (oito) horas;

II – Classe 2: RTO máximo de 24 (vinte e quatro) horas;

III – Classe 1: RTO máximo de 24 (vinte e quatro) horas, admitida solução simplificada de restauração documentada no PCN/PRD, compatível com os recursos estruturais da classe.

§1º O RTO constitui parâmetro funcional máximo de tempo admissível para o restabelecimento das operações essenciais da serventia após incidente que implique indisponibilidade relevante de sistemas ou dados críticos, devendo sua definição e comprovação constar expressamente do PCN/PRD.

§2º A demonstração de atendimento ao RTO deverá ocorrer por meio de testes formais e documentados de restauração, observada a periodicidade mínima prevista neste Anexo e no Anexo I, integrando o dossiê técnico ou relatório simplificado, conforme a classe da serventia.

§3º Os parâmetros estabelecidos neste item constituem padrões mínimos obrigatórios, admitida a adoção de metas mais protetivas quando técnica e economicamente viável.

3. Monitoramento e trilhas de auditoria

I - *logs* protegidos contra alteração não autorizada, com mecanismos de integridade verificável e controle de acesso restrito;

II - identificação inequívoca do usuário, data, hora e tipo de operação;

III - sincronização de tempo por fonte confiável;

IV - retenção mínima das trilhas de auditoria pelo prazo de 5 (cinco) anos, admitido prazo uniforme superior quando tecnicamente justificado;

V - possibilidade de utilização de solução SIEM e coleta centralizada de logs, preservada a segregação lógica por serventia;

VI - adoção de soluções tecnológicas equivalentes ou superiores às exemplificadas, inclusive baseadas em automação avançada ou inteligência artificial, desde que assegurados os requisitos de imutabilidade, rastreabilidade e retenção mínima previstos neste Anexo.

3.1. A referência a SIEM, IDS/IPS, correlação automatizada ou monitoramento contínuo possui natureza exemplificativa, não constituindo requisito de aquisição de ferramenta específica, reputando-se atendido o controle quando a serventia demonstrar, por meios técnicos proporcionais à sua classe, a coleta, a proteção contra adulteração, a retenção mínima e a capacidade de auditoria dos logs, inclusive mediante soluções nativas do fornecedor, centralização simplificada, alertas básicos e revisões periódicas documentadas, preservados os requisitos de imutabilidade, rastreabilidade e retenção mínima.

4. Gestão de incidentes de segurança da informação

I - manutenção de procedimentos documentados de resposta a incidentes;

II - classificação por gravidade (crítico, alto, médio, baixo);

III - comunicação à Corregedoria competente em até 72 horas nos casos críticos;

IV - registro detalhado, análise de causa raiz e documentação de lições aprendidas;

V - integração com obrigações da LGPD.

5. Gestão de vulnerabilidades

I - atualização periódica de sistemas e aplicações;

II - tratamento de vulnerabilidades classificadas como críticas em prazo máximo de 30 (trinta) dias, quando inexistente evidência de exploração ativa. Identificada exploração ativa, risco iminente ou comprometimento relevante, deverão ser adotadas medidas imediatas de contenção e correção emergencial, preferencialmente em até 72 (setenta e duas) horas, com registro formal das providências, inclusive das medidas mitigatórias aplicadas durante a janela de correção;

III - mitigação imediata quando houver exploração ativa ou risco iminente;

IV - registro formal das providências adotadas;

V - possibilidade de integração a programa estruturado de avaliação de vulnerabilidades.

6. Testes e validação de controles

I - testes periódicos de restauração de backups;

II - simulações anuais de cenários de desastre para validação do PCN e PRD;

III - avaliações técnicas periódicas de segurança;

IV - para Classe 3, realização de teste de intrusão (pentest) ou metodologia técnica equivalente, no mínimo, a cada 2 (dois) anos e, adicionalmente, sempre que houver alteração relevante de infraestrutura, arquitetura, exposição de serviços à internet ou substituição de fornecedor crítico, devendo a periodicidade ser reduzida quando a análise de risco do PCN/PRD indicar aumento relevante de superfície de ataque;

V - adoção de metodologias de teste compatíveis com boas práticas reconhecidas internacionalmente, admitida a utilização de frameworks técnicos supervenientes, desde que preservado o objetivo de validação efetiva dos controles.

6.1. Quando a serventia adotar solução tecnológica centralizada, compartilhada ou fornecida por entidade representativa, operador nacional ou fornecedor único, o requisito de teste de intrusão poderá ser comprovado mediante relatório técnico coletivo que abranja o ambiente efetivamente utilizado, desde que contenha descrição do escopo, metodologia aplicada, data de execução, resultados obtidos, plano de correção e declaração de aderência assinada pelo responsável técnico da entidade mantenedora, permanecendo a serventia responsável pela implementação local das medidas corretivas que lhe competirem.

6.2. Considera-se atendido o requisito de teste de intrusão referido no item IV quando (i) a serventia operar integralmente em ambiente SaaS/centralizado sem exposição de infraestrutura própria à internet, e (ii) houver relatório técnico coletivo válido do ambiente efetivamente utilizado, complementado, quando houver componentes locais relevantes, por varredura de vulnerabilidades (scanner) e validação de configuração de borda, sem necessidade de novo teste de intrusão completo, salvo se a análise de risco do PCN/PRD indicar superfície de ataque local relevante.

6.3. As 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 teste de intrusão (pentest), considerando-se cumprido o requisito mediante: (i) apresentação do 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 de trabalho locais possuem sistema operacional com suporte ativo, antivírus atualizado e firewall de sistema habilitado.

7. Interoperabilidade e neutralidade tecnológica

I - adoção preferencial de padrões abertos e formatos não proprietários (ex.: PDF/A, XML);

II - prevenção de dependência exclusiva de fornecedor.

ANEXO III

POLÍTICA MÍNIMA DE SEGURANÇA DA INFORMAÇÃO

Disposição geral:

Este Anexo estabelece o conteúdo mínimo da Política Interna de Segurança da Informação de observância obrigatória, que deverá conter, no mínimo, os elementos indicados neste Anexo, podendo ser ampliada ou estruturada segundo metodologias reconhecidas de governança e *compliance*, desde que preservados os requisitos funcionais aqui estabelecidos.

1. Objetivo

Assegurar confidencialidade, integridade, disponibilidade, rastreabilidade e conformidade legal (*compliance*).

2. Abrangência

I - Aplicável ao delegatário, interino, interventor, colaboradores, estagiários e terceiros.

3. Princípios

Confidencialidade; Integridade; Disponibilidade; Rastreabilidade; Conformidade Legal.

4. Estrutura mínima obrigatória

4.1 Governança e responsabilidades;

4.2 Regras de controle e revogação de acesso;

4.3 Diretrizes de uso aceitável;

4.4 Integração com PCN e PRD, com RTO e RPO definidos;

4.5 Proteção física de ativos;

4.6 Procedimentos de gestão de incidentes;

4.7 Gestão de vulnerabilidades, observados integralmente os prazos e critérios técnicos definidos no Anexo II, vedada flexibilização por norma interna;

4.8 Proteção de Dados Pessoais (LGPD):

I - observância integral da Lei nº 13.709/2018;

II - caracterização do responsável pela serventia como controlador de dados;

III - registro das operações de tratamento;

IV - procedimentos para atendimento aos direitos dos titulares;

V - comunicação de incidentes à ANPD, nos termos e prazos definidos pela legislação e regulamentação vigentes;

VI - designação de encarregado (DPO), quando exigido.

4.9 Criptografia

I - previsão expressa de proteção de dados em trânsito e em repouso;

II - gestão segura de chaves;

III - renovação tempestiva de certificados digitais.

IV - mecanismo de revisão periódica dos padrões criptográficos adotados, com substituição tempestiva de algoritmos ou protocolos que se tornem vulneráveis, preservada a equivalência ou superioridade técnica.

4.10 Gestão de fornecedores

I - avaliação prévia de segurança;

II - cláusulas contratuais de confidencialidade e segurança;

III - definição clara de responsabilidades em caso de incidentes;

IV - monitoramento contínuo do cumprimento contratual.

5. Revisão e auditoria

I - revisão periódica documentada;

II - manutenção de registros auditáveis por 5 anos;

III - submissão à fiscalização correicional.

IV - atualização obrigatória da Política Interna de Segurança da Informação sempre que houver alteração legislativa ou regulatória relevante, especialmente em matéria de proteção de dados pessoais, devendo-se adotar interpretação sistemática e evolutiva das obrigações legais aplicáveis.

ANEXO IV

ETAPAS PARA CUMPRIMENTO

Disposições gerais:

I) As etapas previstas neste Anexo constituem marcos sucessivos e cumulativos de conformidade, devendo ser observada a ordem sequencial aqui estabelecida. A execução de medidas pertencentes a etapas posteriores pode ser registrada junto ao Sistema Justiça Aberta, mas não supre nem antecipa o cumprimento integral dos requisitos da etapa imediatamente anterior.

II) Dentro de cada etapa, a conclusão de cada requisito, um a um, deverá ser informada ao Sistema Justiça Aberta. A declaração de conclusão de cada etapa pressupõe o cumprimento integral de todos os seus itens e a manutenção efetiva dos requisitos já implementados nas etapas precedentes, vedada qualquer declaração parcial, proporcional ou condicionada.

III) A comprovação de conclusão deverá ser formalizada por meio de dossiê técnico específico da etapa concluída, contendo atas, relatórios, registros de configuração, contratos revisados, registros de capacitação e evidências técnicas.

IV) Para as Classes 2 e 3, as evidências de conclusão deverão estar acompanhadas de mecanismo idôneo de verificação de integridade, considerado atendido, no mínimo, mediante:

a) geração de *hash* dos arquivos integrantes do dossiê, com lista de *hashes* assinada digitalmente pelo responsável pela serventia ou responsável técnico designado; e

b) guarda do dossiê em repositório com controle de acesso e registro auditável de alterações, ou em armazenamento com imutabilidade/*retention lock*, quando disponível. O emprego de carimbo do tempo ou mecanismo externo equivalente será exigível apenas quando a serventia optar por auditoria externa, por custódia por terceiro, ou quando houver compartilhamento do repositório probatório com entidade mantenedora.

V) Para a Classe 1, admite-se mecanismo simplificado de comprovação documental, desde que apto a demonstrar, de forma objetiva, a veracidade e a integridade das evidências apresentadas. Em todos os casos, os documentos deverão permanecer arquivados por prazo mínimo de 5 (cinco) anos.

VI) Para a Classe 1, a comprovação de conclusão das etapas previstas neste Anexo poderá ser realizada por meio de declaração de conformidade registrada no Sistema Justiça Aberta, acompanhada da guarda, pelo prazo mínimo de 5 (cinco) anos, dos contratos de serviços de tecnologia da informação, notas fiscais correspondentes e relatório simplificado de implementação assinado pelo responsável pela serventia, dispensada a manutenção de dossiê técnico estruturado em formato ampliado.

VII) O relatório simplificado, aplicável especialmente às serventias enquadradas na Classe 1, deverá conter, no mínimo:

a) identificação da serventia, da classe de enquadramento e da etapa do Anexo IV a que se refere;

b) descrição objetiva do requisito normativo e da solução técnica adotada;

c) demonstração sucinta da equivalência funcional entre a solução implementada e o requisito previsto neste Provimento;

d) indicação das evidências técnicas ou documentais disponíveis para fiscalização, ainda que mantidas sob guarda local; e

e) declaração formal de responsabilidade assinada pelo titular da delegação, interino ou interventor, atestando a veracidade das informações e a manutenção das evidências pelo prazo mínimo de 5 (cinco) anos.

VIII) Para as Classes 2 e 3, considera-se igualmente atendida a exigência de integridade do dossiê técnico quando as evidências forem consolidadas em documento eletrônico único, assinado digitalmente pelo responsável técnico, acompanhado de relatório de hash, sendo facultativa a adoção de repositório com imutabilidade quando demonstrada sua desproporcionalidade econômica.

IX) Para fins de fiscalização correicional, considera-se suficiente, como pacote mínimo probatório, a apresentação:

a) de relatório único, em formato aberto, contendo descrição do requisito, solução adotada, data de implementação e responsável;

b) de evidência técnica mínima (prints, logs de configuração, relatórios automatizados do fornecedor ou do sistema) anexada ao relatório; e

c) de lista de hash assinada digitalmente quando aplicável.

X) É vedado exigir, como condição de conformidade, formalidades não previstas neste Provimento, ressalvada a possibilidade de a Corregedoria competente determinar, mediante decisão fundamentada, providências técnicas adicionais indispensáveis à proteção do acervo, à continuidade do serviço ou ao cumprimento de norma superveniente.

ETAPA 1 — GOVERNANÇA, ESTRUTURAÇÃO ORGANIZACIONAL E CONFORMIDADE LEGAL

Escopo da etapa: instituir a base normativa, organizacional e documental que viabiliza a conformidade integral com o Provimento, assegurando responsabilidade definida, alinhamento à LGPD, controle formal de acessos e prevenção imediata de vulnerabilidades críticas.

Condições objetivas de conformidade: ao final desta etapa, a serventia deverá possuir governança formal instituída, responsabilidades claramente atribuídas, política interna vigente e publicizada, controles mínimos de autenticação implementados, inventário de ativos concluído e base documental apta a demonstrar conformidade inicial em eventual fiscalização correicional.

1.1. Designar formalmente:

I - responsável técnico interno pela implementação;

II - responsável pela serventia como controlador de dados pessoais;

III - encarregado/DPO, quando aplicável.

1.2. Elaborar, aprovar e divulgar internamente a Política de Segurança da Informação, contemplando integralmente os elementos mínimos do Anexo III e estabelecendo (planejando), de forma expressa e estruturada, as diretrizes, objetivos estratégicos, cronogramas, responsabilidades e demais parâmetros que fundamentarão a elaboração, na Etapa 2, do Plano de Continuidade de Negócios (PCN) e do Plano de Recuperação de Desastres (PRD). Nesta Etapa 1, exige-se a incorporação dessas diretrizes à Política interna, com definição preliminar de escopo, governança e critérios de continuidade. A formalização técnica completa, operacional e documentada do PCN e do PRD, com definição detalhada de riscos, medidas de mitigação, RTO e RPO, ocorrerá obrigatoriamente na Etapa 2, vedada tanto sua exigência integral nesta Fase 1 quanto sua postergação para etapa posterior à segunda;

1.3. Implementar autenticação individualizada e autenticação multifator obrigatória para acessos administrativos, vedadas credenciais compartilhadas;

1.4. Instituir registro das operações de tratamento de dados pessoais, nos termos do art. 7º, §1º.

1.5. Incidentes classificados como críticos deverão ser comunicados à Corregedoria competente nos prazos e condições definidos no Anexo II, sem prejuízo das comunicações exigidas pela legislação específica;

1.6. Sem prejuízo do prazo máximo previsto no item anterior, constitui meta de governança e padrão de diligência reforçada que a comunicação à Corregedoria competente ocorra, sempre que possível, em até 24 (vinte e quatro) horas da ciência do incidente, especialmente quando houver risco relevante de indisponibilidade prolongada, comprometimento de dados pessoais ou potencial impacto sistêmico;

1.7. Elaborar inventário completo de ativos tecnológicos, integrações, bancos de dados, certificados digitais, softwares, histórico de atualizações e contratos;

1.8. Regularizar licenciamento de softwares e revisar todos os contratos com terceiros que envolvam tratamento, armazenamento ou processamento de dados da serventia, assegurando cláusulas expressas e exequíveis de: (i) confidencialidade; (ii) reversibilidade; (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; e (vii) conformidade integral com a Lei nº 13.709/2018;

1.9. Produzir declaração de conclusão da Etapa 1, a ser necessariamente firmada pelo titular da delegação, pelo interino na serventia vaga ou pelo interventor. Registrar a conclusão desta Etapa no Sistema Justiça Aberta.

ETAPA 2 — INFRAESTRUTURA E CONTINUIDADE OPERACIONAL

Escopo da etapa: estruturar a base material que sustenta os sistemas informatizados, garantindo disponibilidade mínima, estabilidade elétrica, segurança física e planejamento formal de continuidade.

Condições objetivas de conformidade: ao término desta etapa, a serventia deverá dispor de infraestrutura física adequada, conectividade compatível com sua classe, planos formais de continuidade (PCN e PRD) com RTO e RPO definidos, e capacidade mínima de manter ou restabelecer as operações dentro dos parâmetros normativos.

2.1. Implementar infraestrutura energética adequada (fonte estável, aterramento técnico e SAI/UPS com autonomia mínima de 30 minutos).

2.2. Estabelecer plano de contingência energética compatível com a classe.

2.3. Adequar ambiente físico com controle de acesso restrito e proteção contra incêndio, inundações e variações térmicas.

2.4. Implementar conectividade compatível com a classe, com roteador, switch e, quando necessário, múltiplos links.

2.5. Formalizar o Plano de Continuidade de Negócios (PCN) e o Plano de Recuperação de Desastres (PRD), em documentos distintos ou integrados, desde que contenham, cumulativamente:

I - identificação e avaliação estruturada de riscos;

II - definição objetiva das medidas de mitigação;

III - estabelecimento expresso de RTO e RPO compatíveis com a classe da serventia; e

IV - 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, sendo vedada a declaração de conclusão da etapa sem a presença de todos esses elementos.

2.6. Garantir disponibilidade de equipamentos adequados e suporte técnico contínuo.

2.7. Implementar proteção básica de endpoint (antivírus, antimalware ou solução tecnicamente equivalente) em todas as estações e servidores utilizados pela serventia, como condição mínima de integridade operacional da infraestrutura

2.8. Formalizar documento técnico simplificado da arquitetura tecnológica adotada, contendo, no mínimo:

I - topologia básica de rede;

II - indicação dos ambientes utilizados (local, nuvem, híbrido, SaaS ou compartilhado);

III - fluxos de dados críticos;

IV - localização física ou lógica dos backups;

V - integrações externas relevantes; e

VI - mecanismos de alta disponibilidade ou redundância.

2.9. Produzir declaração de conclusão da Etapa 2, a ser necessariamente firmada pelo titular da delegação, pelo interino na serventia vaga ou pelo interventor. Registrar a conclusão desta Etapa no Sistema Justiça Aberta.

ETAPA 3 — PROTEÇÃO DO ACERVO DIGITAL E RESILIÊNCIA TECNOLÓGICA

Escopo da etapa: assegurar integridade, confidencialidade e recuperabilidade do acervo eletrônico, prevenindo perda de dados, interceptação indevida e comprometimento sistêmico.

Condições objetivas de conformidade: ao final desta etapa, todos os dados críticos deverão estar protegidos por criptografia adequada, com rotinas automatizadas de backup proporcional à classe, armazenamento off-site, monitoramento ativo e defesas perimetrais implementadas.

Disposição geral - A implementação das medidas previstas nesta etapa pressupõe o cumprimento integral e comprovado da Etapa 2, não podendo ser declarada concluída enquanto inexistentes ou incompletos os requisitos estruturais de infraestrutura e continuidade operacional anteriormente estabelecidos. Esta etapa consolida modelo de segurança em camadas (defesa em profundidade), integrando controles de identidade, rede, aplicação e armazenamento.

3.1. Implementar criptografia para dados em trânsito e em repouso, inclusive backups, com gestão formal de chaves criptográficas que contemple, no mínimo:

I - inventário atualizado de chaves e certificados;

II - segregação de custódia;

III - controle formal de acesso;

IV - política documentada de rotação e renovação periódica;

V - registro das operações de geração, renovação e revogação; e

VI - revisão periódica dos padrões criptográficos adotados.

3.2. Implantar rotinas automatizadas de backup completo e incremental, observando, cumulativamente:

I - realização de cópias completas em periodicidade compatível com a classe da serventia, observados os seguintes parâmetros mínimos:

a) Classe 3: intervalo não superior a 24 (vinte e quatro) horas;

b) Classe 2: intervalo não superior a 48 (quarenta e oito) horas;

c) Classe 1: intervalo não superior a 72 (setenta e duas) horas, admitida solução tecnicamente equivalente que assegure o cumprimento do RPO aplicável;

II - execução de cópias incrementais compatíveis com o RPO definido para a classe da serventia;

III - armazenamento dos dados de backup em, no mínimo, dois ambientes tecnicamente independentes, assegurada redundância geográfica ou lógica equivalente, admitidas as seguintes arquiteturas, isoladas ou combinadas:

a) ambiente de nuvem com redundância geográfica automática e mecanismos de imutabilidade de dados (WORM, versionamento bloqueado ou tecnologia equivalente);

b) mídia eletrônica mantida em local fisicamente distinto das instalações principais (off-site);

c) solução híbrida que combine armazenamento local redundante com replicação externa;

d) garantia de que pelo menos um dos ambientes de backup esteja protegido contra criptografia maliciosa, exclusão indevida ou comprometimento sistêmico simultâneo, por meio de mecanismos de isolamento lógico, bloqueio de retenção, controle de acesso reforçado ou tecnologia equivalente.

3.2.1. A exigência de múltiplos ambientes tecnicamente independentes poderá ser cumprida exclusivamente por arquitetura em nuvem, desde que demonstrada, por meio de documentação técnica formal, a existência cumulativa de:

I - redundância geográfica automática em regiões distintas;

II - política de retenção imutável com bloqueio contra exclusão administrativa;

III - segregação lógica de acesso;

IV - registro auditável de operações; e

V - viabilidade comprovada de restauração integral do acervo.

3.2.1.1. Para as serventias das Classes 1 e 2, considera-se atendido o requisito de redundância e independência técnica o armazenamento de cópia de segurança em serviços de nuvem comerciais de amplo mercado, desde que os arquivos de backup sejam submetidos à criptografia forte (AES-256 ou superior) antes do envio (criptografia na origem), assegurando-se que a chave de descriptografia permaneça sob custódia exclusiva da serventia e não do fornecedor (provedor) de armazenamento.

3.2.2. As serventias localizadas em regiões com limitações estruturais de conectividade, especialmente em áreas remotas ou de infraestrutura digital intermitente, poderão adotar arquitetura predominantemente física ou híbrida, desde que assegurada redundância externa mínima e compatibilidade com o RPO e o RTO definidos no PCN e no PRD.

3.2.3. A escolha da arquitetura de backup deverá observar a proporcionalidade regulatória conforme a classe da serventia e as condições socioeconômicas e tecnológicas regionais, vedada solução que implique ponto único de falha ou dependência estrutural não mitigada de fornecedor exclusivo.

3.3. Monitorar rotinas de backup com alertas automáticos e registro formal de falhas.

3.4. Implantar firewall stateful com IPS/IDS e segmentação lógica de rede.

3.5. Implementar solução avançada de proteção de endpoint, quando compatível com a classe da serventia, incluindo monitoramento ativo, detecção de comportamento anômalo ou recursos equivalentes de resposta a incidentes.

3.6. Utilizar SGBD com integridade transacional e logs ativos.

3.7. Implementar mecanismos de tolerância a falhas ou alta disponibilidade compatíveis com a classe.

3.8. Implementar trilhas de auditoria técnicas imutáveis, com sincronização de tempo por fonte confiável, identificação inequívoca do usuário, registro de data e hora e mecanismo de verificação de integridade, assegurando sua integração obrigatória às rotinas de backup e recuperação, com preservação íntegra e rastreável, observados os prazos mínimos de retenção previstos neste Provimento.

3.9. Produzir declaração de conclusão da Etapa 3, a ser necessariamente firmada pelo titular da delegação, pelo interino na serventia vaga ou pelo interventor. Registrar a conclusão desta Etapa no Sistema Justiça Aberta.

ETAPA 4 — MONITORAMENTO, AUDITORIA E VALIDAÇÃO DE CONTROLES

Escopo da etapa: consolidar a rastreabilidade, validar empiricamente os controles implementados e instituir modelo preventivo de gestão de riscos.

Condições objetivas de conformidade: ao final desta etapa, a serventia deverá possuir trilhas de auditoria íntegras, monitoramento contínuo, gestão formal de vulnerabilidades, testes documentados de restauração e simulações de desastre validadas.

4.1. Emitir relatório de conformidade de auditoria, atestando a aderência integral das trilhas de auditoria aos requisitos técnicos previstos no Anexo II, mediante procedimento documentado de verificação que comprove, cumulativamente, a imutabilidade, a identificação inequívoca do usuário, a sincronização temporal por fonte confiável, retenção mínima nos termos do Anexo II, e a efetiva integração às rotinas de backup e recuperação.

4.1.1. O relatório de conformidade deve ser entendido como validação de requisitos estruturais das trilhas de auditoria. Deverá atestar não apenas se o dado “volta”, mas se o sistema efetivamente registra quem fez o que, quando fez, se o tempo está sincronizado e se estes registros são realmente imutáveis.

4.2. Instituir rotina documentada de atualização periódica de sistemas e aplicações.

4.3. Implementar gestão formal de vulnerabilidades, com:

I - tratamento de vulnerabilidades classificadas como críticas nos prazos e condições definidos no Anexo II, com registro formal das providências adotadas no dossiê técnico;

II - adoção de medidas imediatas de contenção e correção emergencial, preferencialmente em até 72 (setenta e duas) horas, quando houver exploração ativa, risco iminente ou comprometimento relevante já identificado;

III - registro formal, auditável e cronologicamente organizado das providências adotadas, com indicação de responsável e data de conclusão.

4.4. Realizar simulação anual de desastre para validação do PCN e PRD.

4.5. Realizar testes documentados de restauração de backups, conforme periodicidade da classe.

4.6. Realizar avaliações técnicas periódicas de segurança.

4.7. Para as serventias enquadradas na Classe 3, realizar teste de intrusão (pentest) ou metodologia técnica equivalente, observado o disposto no Anexo II, item 6, inclusive quanto às hipóteses de validação coletiva, dispensa condicionada e periodicidade mínima.

4.8. Documentar análise de causa raiz e lições aprendidas para todos os incidentes.

4.9. Produzir declaração de conclusão da Etapa 4, a ser necessariamente firmada pelo titular da delegação, pelo interino na serventia vaga ou pelo interventor. Registrar a conclusão desta Etapa no Sistema Justiça Aberta.

ETAPA 5 — INTEROPERABILIDADE, CONSOLIDAÇÃO E GOVERNANÇA EVOLUTIVA

Escopo da etapa: integrar a serventia ao ecossistema de fiscalização, consolidar as evidências documentais produzidas nas etapas anteriores e institucionalizar processo permanente e contínuo de revisão, aprimoramento e evolução tecnológica, vedada interpretação que restrinja as obrigações aqui previstas a momento único ou conclusivo.

Condições objetivas de conformidade: ao final desta etapa, a serventia deverá estar plenamente integrada às plataformas de fiscalização, com interoperabilidade técnica assegurada, política revisada periodicamente, capacitação contínua implementada e declaração formal de conformidade realizada.

5.1. Adequar sistemas para interoperabilidade com plataformas eletrônicas de fiscalização (art. 19).

5.2. Adotar padrões abertos e neutralidade tecnológica, prevenindo dependência exclusiva de fornecedor.

5.3. Instituir capacitação periódica com registro formal das ações realizadas.

5.4. Revisar formalmente a Política de Segurança e padrões criptográficos sempre que houver alteração normativa relevante ou evolução tecnológica.

5.5. Manter registros auditáveis por, no mínimo, 5 anos.

5.6. Manter plano formal de reversibilidade e portabilidade de dados, acompanhado de simulação documentada de extração integral do acervo digital em formato interoperável e não proprietário, cuja realização deverá preceder a declaração de conclusão desta etapa, sendo vedada sua homologação sem evidência técnica de viabilidade concreta de transferência organizada ao sucessor, nos termos do art. 6º, III.

5.6.1. A simulação documentada de extração integral do acervo deverá ser realizada:

I - no mínimo, a cada 24 (vinte e quatro) meses, para as serventias enquadradas na Classe 3;

II - no mínimo, a cada 30 (trinta) meses, para as serventias enquadradas na Classe 2;

III - no mínimo, a cada 36 (trinta e seis) meses, para as serventias enquadradas na Classe 1;

IV - imediatamente, sempre que houver alteração relevante de fornecedor, arquitetura tecnológica ou modelo de governança. Em todos os casos, deverá ser mantido registro auditável do procedimento.

5.6.2. A simulação documentada de extração integral poderá ser realizada:

I - em ambiente de contingência, réplica, laboratório isolado ou cópia técnica representativa do acervo;

II - por meio de exportação estrutural completa acompanhada de validação técnica de consistência e integridade, admitida verificação por amostragem estatisticamente representativa dos atos eletrônicos;

III - de forma escalonada ou segmentada por módulos ou bases, desde que demonstrada, por evidência técnica formal, a viabilidade concreta de reconstrução integral do acervo.

5.6.2.1. Quando a serventia demonstrar, por meio de justificativa técnica formal e evidências documentadas, que a realização da simulação integral bienal implica impacto operacional desproporcional em razão do volume do acervo digital, da arquitetura tecnológica adotada ou da limitação estrutural de conectividade, admitir-se-á a substituição da repetição integral por validação técnica estrutural de portabilidade, desde que:

I - seja comprovada a viabilidade concreta de extração integral do acervo por meio de testes segmentados, exportações estruturais completas acompanhadas de verificação de integridade e reconstrução parcial representativa; e

II - a justificativa técnica e as evidências sejam incluídas no dossiê técnico da etapa, sujeitas à fiscalização correicional.

5.7. Produzir declaração de conclusão da Etapa 5, a ser necessariamente firmada pelo titular da delegação, pelo interino na serventia vaga ou pelo interventor. Registrar a conclusão desta Etapa no Sistema Justiça Aberta.

ANEXO V

MODELO DE ATA PARA REGISTRO DO TESTE DE RESTAURAÇÃO (ANEXO IV, ETAPA 4)

Disposições gerais:

I) O presente modelo possui caráter referencial e orientativo, destinando-se a padronizar a evidência mínima aceitável para comprovação do teste documentado de restauração de backups previsto neste Provimento. Admitir-se-á formato diverso, desde que contenha, de forma objetiva e verificável, os elementos essenciais de identificação do teste, escopo, metodologia adotada, resultados obtidos, validação dos parâmetros de RTO e RPO aplicáveis e identificação dos responsáveis.

II) A formalização do teste observará a proporcionalidade segundo a classe da serventia, admitindo-se, para a Classe 1, registro simplificado que contenha, no mínimo: (i) identificação da data do teste; (ii) sistemas e bases restauradas; (iii) confirmação da restauração integral; (iv) tempo efetivo de recuperação; e (v) assinatura do responsável.

III) É vedada a exigência de formalidades adicionais não previstas neste Anexo como condição de validade do teste, reputando-se atendido o dever normativo quando demonstrada, de forma objetiva e verificável, a capacidade de recuperação integral do acervo nos parâmetros de RTO e RPO definidos no PCN e no PRD da serventia.

ATA PARA REGISTRO DO TESTE DE RESTAURAÇÃO

1. Aos XXXX dias do mês de XXXX de XXXX, às XXXX horas, na serventia XXXX (CNS XXXX), situada à XXXX sob responsabilidade do(a) delegatário(a) XXXX, reuniu-se a equipe designada para a realização do teste documentado de restauração de backup, em cumprimento às disposições deste Provimento relativas à validação periódica de restauração de backups e continuidade operacional.

2. Participaram do teste:

I) XXXX (responsável técnico interno);

II) XXXX (colaborador/preposto);

III) XXXX (fornecedor/empresa), se aplicável.

2.1. O responsável pela serventia (Delegatário, Interino ou Interventor) declara ter acompanhado, supervisionado ou validado o procedimento, assumindo responsabilidade pessoal e funcional pela veracidade das informações registradas e pela autenticidade das evidências técnicas anexadas.

3. Escopo do teste: restauração do(s) sistema(s) XXXX e do(s) banco(s) de dados XXXX incluindo verificação de integridade de:

I) base de dados;

II) repositório de documentos/atos eletrônicos;

III) trilhas de auditoria, quando aplicável.

4. Validação de parâmetros operacionais (RTO e RPO):

I) Horário de início da restauração: XXXX

II) Horário de conclusão da restauração: XXXX

III) Tempo total efetivo de recuperação (RTO aferido): XXXX

IV) RTO definido no PCN/PRD: XXXX

V) Ponto temporal do último dado íntegro restaurado: XXXX

VI) Perda temporal efetiva de dados (RPO aferido): XXXX

VII) RPO definido para a classe da serventia: XXXX

Declara-se que os parâmetros encontram-se:

( ) Em conformidade

( ) Em desconformidade

Em caso de desconformidade, indicar justificativa técnica e providências adotadas.

5. Arquitetura de backup vigente no momento do teste:

I) Solução tecnológica utilizada (nome e versão): XXXX

II) Identificador do backup restaurado: XXXX

III) Tipo de backup (completo/incremental): XXXX

IV) Local de armazenamento primário e secundário: XXXX

V) Método de criptografia empregado: XXXX

VI) Mecanismo de verificação de integridade utilizado: XXXX

VII) Classe da serventia: XXXX

6. Procedimento resumido adotado:

I) Seleção do ponto de restauração referente a XX/XX/XXXX às XXXX horas;

II) Execução da restauração do banco de dados;

III) Restauração do repositório documental;

IV) Validação de serviços e acessos;

V) Checagem de integridade por meio de XXXX

VI) Validação amostral de atos eletrônicos (amostra de XXXX itens), com conferência de leitura, consistência e rastreabilidade.

7. Resultados consolidados:

I) Aderência ao RTO: ( ) Atendido ( ) Não atendido;

II) Aderência ao RPO: ( ) Atendido ( ) Não atendido;

III) Método de verificação de integridade utilizado e resultado obtido: XXXX

IV) Inconsistências detectadas (se houver): XXXX

8. Medidas corretivas ou preventivas deliberadas:

Medida 01:

a) Descrição: XXXX

b) Responsável: XXXX

c) Prazo para conclusão: XX/XX/XXXX

Medida 02:

a) Descrição: XXXX

b) Responsável: XXXX

c) Prazo para conclusão: XX/XX/XXXX

Medida 03

a) Descrição: XXXX

b) Responsável: XXXX

c) Prazo para conclusão: XX/XX/XXXX

9. Evidências técnicas mínimas anexadas:

I) Log ou relatório automatizado do processo de restauração;

II) Identificador único do backup restaurado;

III) Comprovante de verificação de integridade (hash ou equivalente);

IV) Evidência da validação amostral;

V) Identificação do ambiente em que o teste foi executado.

VI) Outras evidências: XXXX

10. Encerrado o teste às XXXX horas, lavrou-se o presente registro, ao qual se vinculam as evidências técnicas identificadas no item 9, numeradas sequencialmente e arquivadas em repositório com controle de acesso e registro auditável, assegurada sua guarda íntegra, imutável e auditável pelo prazo mínimo de 5 (cinco) anos, nos termos deste Provimento.

11. O responsável pela serventia declara, sob responsabilidade pessoal e funcional, que o teste foi realizado conforme os parâmetros oficiais vigentes e que as informações registradas refletem fielmente os resultados obtidos.

( ) Conformidade integral

( ) Conformidade parcial (com plano corretivo anexo)

( ) Não conformidade (com medidas emergenciais adotadas)

(Local e data)

Responsável pela serventia

Responsável técnico interno

Demais participantes (se houver)