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.

Selecionado e divulgado por INR Publicações

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.

Selecionado e divulgado por INR Publicações

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)

Selecionado e divulgado por INR Publicações