CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO

PORTARIA CNMP-PRESI N° 224 DE 28 DE OUTUBRO DE 2021

Institui a Política de Salvaguarda e Recuperação de Dados Digitais do Conselho Nacional do Ministério Público.

O **PRESIDENTE DO CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO**, no uso das atribuições que lhe conferem o artigo 130-A, § 2°, I, da Constituição Federal e o art. 12, XVII, do Regimento Interno do Conselho Nacional do Ministério Público;

Considerando a Política Nacional de Tecnologia da Informação do Ministério Público (PNTI-MP), instituída pela Resolução CNMP nº 171, de 27 de junho de 2017;

Considerando a Portaria CNMP-PRESI nº 30, de 7 de abril de 2010, que dispõe sobre critérios de uso e segurança dos recursos de Tecnologia da Informação do Conselho Nacional do Ministério Público;

Considerando a regulamentação da Política de Segurança Institucional do Conselho Nacional do Ministério Público, instituída pela Portaria CNMP-PRESI nº 153, de 7 de dezembro de 2017;

Considerando os Planos de Gestão de Riscos e de Segurança Institucional do Conselho Nacional do Ministério Público, instituídos pela Portaria CNMP-PRESI nº 167, de 4 de dezembro de 2018;

Considerando a organização interna e as atribuições das unidades administrativas que compõem a estrutura organizacional do Conselho Nacional do Ministério Público, conforme disposto na Portaria CNMP-PRESI nº 95, de 14 de setembro de 2017;

Considerando a necessidade de proteção de dados pessoais estabelecida pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);

Considerando as recomendações dos órgãos de controle interno e externo e as boas práticas de Segurança de Tecnologia da Informação adotadas nas organizações públicas e privadas, RESOLVE:

Art. 1º Instituir a Política de Salvaguarda de Dados Digitais do Conselho Nacional do Ministério Público – CNMP.

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 2º A Política de Salvaguarda e Recuperação de Dados Digitais objetiva instituir diretrizes, responsabilidades e competências que visam a salvaguarda de dados digitais custodiados pela Secretaria de Tecnologia da Informação – STI.

Parágrafo único. A Política de Salvaguarda e Recuperação de Dados Digitais deve estar alinhada com a gestão de continuidade de negócios em nível organizacional.

Art. 3º Para os fins desta Portaria, considera-se:

I – administrador de backup: unidade responsável pelo planejamento de soluções de backup, pela definição de padrões, pelas configurações e pelo atendimento avançado de resolução de incidentes e problemas;

II – operador de backup: unidade responsável por procedimentos de atendimento de terceiro nível, acompanhamento de execução de planos de backup, realização de restaurações de arquivos de usuários, manutenção de troca de fitas no robô, gerenciamento de estoque de fitas locais, gerenciamento de armazenamento destinado a backup e outros aspectos técnicos envolvidos na salvaguarda de dados digitais;

III – gestor negocial: responsável pela definição de requisitos essenciais ao funcionamento de serviço de TI, pela avaliação da qualidade geral do serviço e pela iniciação de ações de melhoria quando deficiências forem encontradas;

IV – área técnica: unidade responsável pela operação técnica dos ativos e dos serviços de TI;

V – ativo de TI: qualquer componente ou recurso que precise ser gerenciado de forma a garantir a entrega de um serviço de TI e que, para o propósito desta política, necessite de salvaguarda de dados digitais;

VI – ativo de TI crítico: ativo de TI que possua elevada importância para a continuidade das atividades e dos serviços da organização bem como para a concretização dos seus objetivos;

VII – backup: cópia de segurança de dados computacionais, que pode ser utilizada ou consultada após sua restauração, em caso de indisponibilidade, perda ou alteração dos dados originais;

VIII – backup completo: modalidade de backup em que todos os dados a serem

salvaguardados são copiados integralmente (cópia de segurança completa) para uma unidade de armazenamento, independentemente de terem sido ou não alterados desde o último backup;

IX – backup diferencial: modalidade de backup em que são salvaguardados apenas dados novos ou modificados desde o último backup completo efetuado;

X – backup incremental: modalidade de backup em que são salvaguardados apenas os dados novos ou modificados desde o último backup de qualquer modalidade efetuado;

XI – backup integral: modalidade de backup, também conhecido como "imagem", que consiste no espelhamento, cópia "bit a bit", de servidor ou procedimento assemelhado, de modo que, em caso de necessidade, seja possível restaurar rapidamente o sistema a um estado anterior "estável";

XII – criticidade: grau de importância dos dados para a continuidade das atividades e dos serviços da organização;

XIII – dado "bloqueado para o uso": dado não excluído de unidades de armazenamento de backups no exercício do direito de eliminação de dados pessoais do titular, garantido que:

a) não pode ser usado para nenhuma operação de tratamento de dados;

b) não seja acessível de nenhuma outra forma pela organização;

c) seja protegido com os mecanismos apropriados de segurança técnica e organizacional; e

d) seja descartado permanentemente se e quando possível;

XIV – descarte: eliminação correta de dados, documentos, unidades de armazenamento e acervos digitais;

XV – disponibilidade: garantia de que o dado esteja acessível e utilizável sob demanda de pessoa física ou determinado serviço de TI, órgão ou entidade devidamente autorizados;

XVI – janela de backup: intervalo de tempo durante o qual cópias de segurança sob execução agendada ou manual poderão ser executadas;

XVII – plano de backup: documentação técnica dos procedimentos utilizados para se realizar um backup;

XVIII – plano de continuidade de negócios (PCN): plano que define as etapas necessárias para recuperação dos processos de negócio logo após uma interrupção, identificando também os gatilhos para invocação, as pessoas a serem envolvidas, as comunicações, dentre outras providências;

XIX – restauração: processo de recuperação e disponibilização de dados

salvaguardados em determinado backup;

XX – retenção: intervalo de tempo pelo qual os dados devem ser salvaguardados e estar aptos à restauração;

XXI – recovery point objective (RPO): ponto no tempo em que os dados dos serviços de TI devem ser recuperados após uma situação de parada ou perda, correspondendo ao prazo máximo em que se admite perder dados no caso de um incidente;

XXII – recovery time objective (RTO): tempo estimado para restaurar os dados e tornar os serviços de TI novamente operacionais, correspondendo ao prazo máximo em que se admite manter os serviços de TI inoperantes até a restauração de seus dados, após um incidente;

XXIII – serviço de TI: conjunto de atividades técnicas executadas pela STI ou por provedor de serviço externo sob delegação e supervisão daquela, com vistas a apoiar os processos de negócio, gerando valor e facilitando a obtenção dos resultados pretendidos pelas unidades organizacionais do CNMP;

XXIV – unidade de armazenamento: dispositivo para armazenamento de dados em suporte digital;

XXV – unidade de armazenamento de backup: unidade de armazenamento com características específicas para retenção de cópia de segurança de dados digitais;

XXVI – unidade de armazenamento de backup offline: unidade de armazenamento de backup não acessível pela rede da organização, seja por meio de chamadas de sistema operacional, de chamadas de Application Programming Interface – API ou por qualquer outro meio de acesso remoto;

XXVII – unidade de armazenamento de backup offsite: unidade de armazenamento de backup localizada em local fisicamente diferente da sede do CNMP.

Art. 4º A salvaguarda dos dados digitais do CNMP abrange exclusivamente ativos de TI institucionais gerenciados ou custodiados pela STI.

§ 1º Não serão salvaguardados nem recuperados dados armazenados localmente nos dispositivos dos usuários ou em quaisquer outros dispositivos fora do centro de processamento de dados mantido pela STI.

§ 2º A salvaguarda dos dados em formato digital pertencentes a ativos de TI do CNMP, mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços de TI em nuvem, deve estar garantida nos acordos ou nos contratos que formalizam a relação entre os envolvidos.

Art. 5º Caberá ao Comitê de Governança da Tecnologia da Informação – CGTI a definição dos ativos de TI críticos do CNMP, cuja salvaguarda de dados digitais seja necessária.

CAPÍTULO II
DAS RESPONSABILIDADES

Art. 6º Os titulares bem como, durante suas ausências, os substitutos do Núcleo de Suporte Técnico – NST e do Serviço de Infraestrutura e Produção – SERVIP atuarão, respectivamente, como administrador e operador de backup do CNMP.

Art. 7º O administrador de backup e o operador de backup deverão, com intervalo máximo de 2 (dois) anos, capacitar seu corpo técnico para as tecnologias, os procedimentos e as soluções utilizados nos planos de backup.

Art. 8º São atribuições do administrador de backup:

I – propor soluções de cópia de segurança dos dados digitais corporativos produzidos ou custodiadas pelo CNMP;

II – definir os procedimentos de restauração e neles auxiliar;

III – tomar medidas preventivas para evitar falhas;

IV – reportar imediatamente à STI os incidentes ou os erros que causem indisponibilidade ou impossibilitem a execução ou a restauração de backups;

V – disponibilizar informações que subsidiem as decisões referentes à gestão de capacidade relacionada aos procedimentos de execução de backup;

VI – propor modificações visando ao aperfeiçoamento da Política de Backup e Recuperação de Dados Digitais, objeto desta Portaria;

VII – elaborar planos de backup para os ativos de TI sob sua administração técnica direta, levando-se em consideração as necessidades ou os requisitos de negócio a serem atendidos bem como os requisitos de privacidade e segurança da informação envolvidos e a criticidade da informação para a continuidade da operação da organização;

VIII – providenciar a execução dos testes de restauração.

Art. 9º São atribuições do operador de backup:

I – configurar as soluções de backup;

II – providenciar a criação e a manutenção dos backups;

III – restaurar ou recuperar os backups em caso de necessidade;

IV – operar e manusear as unidades de armazenamento de backups;

V – verificar diariamente os eventos gerados pela solução de backup, tomando as providências necessárias para remediação de eventuais falhas;

VI – informar ao administrador de backup qualquer problema que impossibilite a restauração de um backup;

VII – manter as unidades de armazenamento de backups preservadas, funcionais e seguras;

VIII – gerenciar mensagens e registros de auditoria diários dos backups.

Art. 10. São atribuições das áreas técnicas:

I – solicitar restaurações de dados, com anuência do gestor negocial;

II – sanar dúvidas técnicas do administrador de backup acerca das informações salvaguardadas;

III – validar, tecnicamente, o resultado das restaurações eventualmente solicitadas;

IV – validar, tecnicamente, o resultado dos testes de restauração dos backups.

Art. 11. São atribuições dos gestores negociais:

I – solicitar, formalmente, a salvaguarda das informações geridas e dar anuência à solicitação feita pela área técnica para recuperação de dados;

II – validar, negocialmente, o resultado das restaurações eventualmente solicitadas;

III – validar, negocialmente, o resultado dos testes de restauração dos backups.

Art. 12. A solicitação de restauração de dados que tenham sido salvaguardados depende de prévia e formal autorização dos respectivos gestores negociais.

Parágrafo único. O operador de backup terá a prerrogativa de negar a restauração de dados cujo conteúdo não seja condizente com a atividade institucional, cabendo recurso da negativa ao gestor da unidade do demandante.

CAPÍTULO III
DOS PLANOS DE BACKUP DE DADOS DIGITAIS

Art. 13. Deverão ser estabelecidos planos de backup para os ativos de TI, sendo permitidos planos contendo agrupamento por categorias ou conjuntos de ativos de TI.

§ 1º Os ativos de TI críticos deverão ter planos individuais, só podendo ser agrupados caso não seja possível a dissociação.

§ 2º O agrupamento só será permitido se os ativos de TI abrangidos possuírem os mesmos requisitos de salvaguarda e restauração de dados digitais, devendo estar registrada, no plano de backup, a lista dos ativos de TI contemplados, incluindo a indicação da criticidade dos ativos de TI críticos.

§ 3º Só poderão entrar em operação os ativos de TI que possuam planos de backup.

Art. 14. Os planos de backup devem explicitar, no mínimo, os seguintes requisitos técnicos:

I – escopo (dados digitais a serem salvaguardados);

II – tipo de backup (completo, diferencial, incremental, integral);

III – frequência temporal;

IV – tempo de retenção;

V – RPO;

VI – RTO.

Art. 15. Os planos de backup deverão ser orientados para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.

Parágrafo único. Os planos de backup devem prever, preferencialmente, backups completos e integrais desde que tecnicamente viável.

Art. 16. A elaboração ou a adequação dos planos de backup que contenham ativos de TI críticos será sempre prioritária em relação aos demais.

Art. 17. Os planos de backup deverão ser disponibilizados pela STI, em local de fácil acesso, para consulta dos gestores negociais, que podem solicitar retificação, desde que o pedido esteja devidamente motivado e aprovado pelo CGTI.

CAPÍTULO IV
DOS PADRÕES OPERACIONAIS

Seção I
Das Ferramentas

Art. 18. Os planos de backup devem prever a utilização de soluções próprias e especializadas para este fim, de forma regular e automatizada, e, preferencialmente, redundante.

Parágrafo único. O administrador de backup deve identificar a viabilidade de utilização

de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso.

Art. 19. Os ativos de TI utilizados como ferramentas para a realização dos processos de backup são considerados ativos de TI críticos.

Seção II

Da Frequência Temporal e do Tempo de Retenção

Art. 20. Os planos de backup podem definir as seguintes frequências temporais:

I – diária;

II – semanal;

III – mensal;

IV – anual.

Art. 21. Os planos de backup devem definir o tempo de retenção dos backups, considerando-se os requisitos legais e normativos específicos.

Parágrafo único. Na inexistência de requisitos legais ou específicos, os planos de backup deverão observar tempos de retenção mínimos, em associação com as respectivas frequências temporais e criticidade abaixo listadas:

I – frequência diária para ativo de TI crítico, retenção de 2 (dois) meses;

II – frequência diária para ativo de TI não crítico, retenção de 1 (um) mês;

III – frequência semanal para ativo de TI crítico, retenção de 4 (quatro) meses;

IV – frequência semanal para ativo de TI não crítico, retenção de 2 (dois) meses;

V – frequência mensal para ativo de TI crítico, retenção de 12 (doze) meses;

VI – frequência mensal para ativo de TI não crítico, retenção de 6 (seis) meses;

VII – frequência anual para ativo de TI crítico, retenção de 60 (sessenta) meses;

VIII – frequência anual para ativo de TI não crítico, retenção de 24 (vinte e quatro) meses.

Art. 22. Serão admitidos frequências temporais e tempos de retenção diferentes dos definidos nesta seção, sendo necessário formalização prévia justificada tecnicamente, manifestação favorável do titular da STI e anuência do CGTI.

Seção III

Do Uso da Rede

Art. 23. O administrador de backup deve considerar o impacto da execução dos planos de backup sobre o desempenho da rede de dados do CNMP, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI.

§1º Os dados de backup trafegados na rede devem ser protegidos adequadamente por meio seguro, utilizando-se criptografia, sempre que possível.

§ 2º No caso de trânsito em redes remotas, a utilização de criptografia será obrigatória.

Art. 24. A execução do backup, como especificado no plano de backup, deve concentrar-se, preferencialmente, no período de janela de backup.

Parágrafo único. O período de janela de backup deve ser determinado pelo administrador de backup em conjunto com a área técnica responsável pela administração da rede de dados do CNMP.

Seção IV

Das Unidades de Armazenamento

Art. 25. As unidades de armazenamento utilizadas na salvaguarda dos dados digitais devem considerar as seguintes características dos dados resguardados:

I – a criticidade do dado salvaguardado;

II – o tempo de retenção do dado;

III – a probabilidade de necessidade de restauração;

IV – o tempo esperado para restauração;

V – o custo de aquisição da unidade de armazenamento de backup;

VI – a vida útil da unidade de armazenamento de backup.

Art. 26. Poderão ser utilizadas técnicas de compressão de dados ou criptografia para o armazenamento, contanto que o acordo de nível de serviço aplicado ao serviço de recuperação dos dados seja respeitado.

Parágrafo único. O uso de criptografia para os dados armazenados nas unidades de armazenamento é sempre desejável e, no caso do uso de unidades de armazenamento remotas, obrigatório.

Art. 27. As unidades de armazenamento dos backups devem ser acondicionadas em

locais apropriados, com controle de fatores ambientais sensíveis, como umidade e temperatura, e com acesso restrito a pessoas autorizadas pelo administrador de backup.

Parágrafo único. O acesso lógico às unidades de armazenamento de backup deverá ser segregado de outros equipamentos e serviços na rede, limitando-se o acesso direto por ferramentas de backup utilizadas para realização das atividades de cópia ou restauração.

Art. 28. Deverão ser mantidas unidades de armazenamento de backup offline e offsite.

Art. 29. Após o tempo de retenção definido no plano de backup, fica autorizado, com manifestação favorável do titular da STI e anuência do CGTI, o descarte ou o reaproveitamento de unidades de armazenamento de backup.

Parágrafo único. Quando da necessidade de descarte, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los, atentando-se ao descarte sustentável e ambientalmente correto.

Seção V
Da Recuperação

Art. 30. As solicitações de recuperação de backups deverão ser devidamente iniciadas na ferramenta de requisição de serviço de TI e, no caso de não ser registrada pelo gestor negocial, deverá ser encaminhada para sua aprovação prévia.

Art. 31. A recuperação não será viabilizada em caso de perdas anteriores à conclusão do backup.

Parágrafo único. Dados criados ou modificados entre execuções de procedimentos de salvaguarda subsequentes não serão protegidos por soluções de backup.

Art. 32. O administrador de backup deverá adotar mecanismos para o adequado monitoramento e gerenciamento de dados “bloqueados para o uso” durante as execuções de procedimentos de recuperação de backups.

Subseção I
Dos Testes Periódicos

Art. 33. Os backups devem ser testados periodicamente, com o objetivo de garantir a sua confiabilidade e a integridade dos dados salvaguardados.

Parágrafo único. Os testes deverão ser documentados em processos administrativos para fins de auditoria.

Art. 34. Os testes de restauração dos backups devem ser realizados, por amostragem, em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos e tecnológicos disponíveis.

Art. 35. A periodicidade, a abrangência, os procedimentos e os planos inerentes aos testes de backup serão definidos pelo administrador de backup em conjunto com a área técnica e, caso necessário, pelos gestores negociais.

Parágrafo único. A periodicidade dos testes não poderá ser superior a 3 (três) meses para ativos de TI críticos e a 6 (seis) meses para ativos de TI não críticos.

CAPÍTULO V
DAS DISPOSIÇÕES FINAIS

Art. 36. Casos excepcionais não abordados nesta Portaria serão decididos pela Secretaria-Geral, com análise da STI e, caso necessário, dos gestores negociais.

Art. 37. Esta Portaria em vigor na data de sua publicação.

Brasília, 28 de outubro de 2021.

ANTÔNIO AUGUSTO BRANDÃO DE ARAS