PORTARIA PRESIDÊNCIA N. 197, DE 07 DE AGOSTO DE 2023.

Institui a Política de Cópia de Segurança (Backup) e Restauração (Restore) de Dados do Conselho Nacional de Justiça.

A **PRESIDENTE DO CONSELHO NACIONAL DE JUSTIÇA (CNJ)**, no uso de suas atribuições legais e regimentais, e tendo em vista o contido no Processo SEI n. 03304/2023,

CONSIDERANDO o disposto na Resolução CNJ n. 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO o que dispõe a Lei n. 13.709/2018, que versa sobre a Lei Geral de Proteção de Dados Pessoais (LGPD);

CONSIDERANDO a importância de se estabelecer objetivos, princípios e diretrizes de Segurança da Informação alinhados às recomendações constantes da norma NBR ISO/IEC 27001:2013, que trata da segurança da informação;

CONSIDERANDO o contido na Portaria SG n. 47/2017, que dispõe sobre a política de Segurança da Informação do CNJ;

CONSIDERANDO os termos da Portaria CNJ n. 118/2021, que dispõe sobre o portfólio de soluções de tecnologia da informação e comunicação e serviços digitais do Conselho Nacional de Justiça e seu anexo II, que lista as soluções de TIC e serviços digitais por gestor negocial;

RESOLVE:

CAPÍTULO I

DOS CONCEITOS E DEFINIÇÕES

Art. 1º Instituir a Política de Cópia de Segurança (Backup) e Restauração de Dados (Restore) no âmbito do Conselho Nacional de Justiça.

§ 1º Entende-se por backup a cópia das informações armazenadas nos equipamentos e servidores utilizados para prover os serviços tecnológicos oferecidos pelo Conselho Nacional de Justiça.

§ 2º Entende-se por restore a recuperação da informação copiada.

Art. 2º Para os fins desta Portaria, considera-se:

I – administrador do backup: unidade responsável pelo planejamento de soluções de backup, procedimentos de configuração, execução, monitoramento, testes de backup, definição de padrões, configurações e atendimento avançado de resolução de incidentes e problemas;

II – administrador do recurso: unidade responsável pela operação dos serviços ou equipamentos;

III – tempo de retenção: tempo que permanecerá disponível o backup das informações para eventual restauração;

IV – 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;

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

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

VII – periodicidade de backup: frequência em que ocorrerá o backup;

VIII – mídia: meio físico ou virtual no qual efetivamente armazenam-se os dados de um backup.

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

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

XI – 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;

XII – janela de backup: período durante o qual cópias de segurança sob execução agendada ou manual poderão ser executadas;

XIII – gestor negocial: agente público formalmente responsável pela administração de serviço de TI e pelas informações produzidas em seu processo de trabalho;

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

XV – RTO (*Recovery Time Objective)* – Objetivo do Tempo de Recuperação: indicador que mensura o tempo máximo em que um sistema ou uma informação pode ficar indisponível após uma falha; e

XVI – RPO (*Recovery Point Objective*) – Ponto Objetivo de Recuperação: indicador utilizado para apurar a quantidade de recursos mínimos a serem recuperados em caso de falhas ou perda de dados.

CAPÍTULO II

ESCOPO E ABRANGÊNCIA

Art. 3º Esta Política de Backup define diretrizes, responsabilidades e competências que visam à segurança, à proteção e à disponibilidade dos dados digitais custodiados pelos administradores de backup e administradores de recursos, com o objetivo de manter a continuidade do negócio do Conselho Nacional de Justiça.

Art. 4º Todos os serviços críticos do CNJ deverão ser incluídos no processo de backup, conforme definido no Plano de Continuidade.

§ 1º A Política de Backup engloba como escopo todas as informações contidas em Servidores de Arquivos, de Aplicações, de Banco de Dados, de Comunicação (*e-mail*/mensagens) e demais Sistemas Críticos.

§ 2º Informações armazenadas localmente nas estações de trabalho não farão parte do escopo do backup.

Art. 5º Na ausência de Plano de Continuidade, os serviços que estão inclusos no processo de backup serão definidos pelo Comitê de Governança de Tecnologia da Informação e Comunicação (CGETIC).

Art. 6º Para a inclusão de um novo serviço na rotina de backup deverão ser fornecidas, no mínimo, as seguintes informações ao administrador do backup:

I – local ou diretório onde residem os dados;

II – volume dos dados que serão copiados;

III – frequência em que os dados devem ser salvaguardados;

IV – tempo de retenção; e

V – área responsável pelo servidor de dados.

Parágrafo único. A solicitação que trata o *caput* deste artigo deverá ser formalizada pelo sistema de gerenciamento de chamados utilizado pelo CNJ e direcionada para o administrador do backup.

CAPÍTULO III

DISPOSIÇÕES PRELIMINARES

Art. 7º Os gestores negociais deverão ter ciência do tempo de retenção estabelecido para cada tipo de informação e os administradores de backup deverão zelar pelo cumprimento das diretrizes estabelecidas nesta Portaria.

Art. 8º O serviço de backup deve ser orientado para a restauração das informações no menor tempo possível, principalmente havendo indisponibilidade de serviços que dependam da operação de restore.

Art. 9º Todas as falhas nos procedimentos de backups deverão ser tratadas pelo administrador do backup e, em caso de falha, o administrador desse recurso deverá ser notificado.

Art. 10. As rotinas de backup devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado, com prioridade para os serviços de TI classificados como críticos.

CAPÍTULO IV

DAS RESPONSABILIDADES

Art. 11. A administração dos serviços de backup deve seguir os requisitos de segurança definidos pela Unidade Gestora de Segurança da Informação do CNJ.

Parágrafo único. Caberá à Unidade Gestora de Segurança da Informação:

I – definir os requisitos de segurança para o armazenamento dos dados digitais;

II – efetuar auditorias periódicas sobre as contas administrativas do ambiente de armazenamento dos dados digitais;

III – definir critérios de segurança para processos de geração da cópia de segurança dos bancos de dados; e

IV – definir requisitos de segurança para recuperação de dados pontuais.

Art. 12. A administração dos serviços de backup é atribuição da Unidade Gestora de Serviços e Aplicações do CNJ.

Parágrafo único. Caberá à Unidade Gestora de Serviços e Aplicações:

I – apoiar na definição dos prazos de retenção de dados junto aos gestores negociais;

II – auxiliar na definição da periodicidade das cópias de segurança junto aos gestores negociais;

III – certificar que as cópias de segurança são realizadas conforme definição dos gestores negociais;

IV – acompanhar a execução dos backups por meio das ferramentas de monitoramento disponíveis para esse objetivo;

V – configurar as soluções de backup;

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

VII – realizar periodicamente testes de restauração para averiguar os processos de backup e estabelecer melhorias.

Art. 13. 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; e

IV – definir a frequência de realização do backup (diária, semanal, mensal, anual), bem como o tipo (completo, incremental, diferencial) e o escopo (dados digitais a serem backupeados).

CAPÍTULO V

FREQUÊNCIA E RETENÇÃO DOS DADOS

Art. 14. Os backups dos serviços de TI do CNJ devem ser realizados utilizando-se as seguintes frequências temporais:

I – diária;

II – semanal;

III – mensal; e

IV – anual.

Art. 15. Os serviços de TI do CNJ devem ser resguardados observando a correlação frequência/retenção de dados estabelecida a seguir:

I – diária: devem ser retidos por uma semana;

II – semanal: devem ser retidos por um mês;

III – mensal: devem ser retidos por um ano; e

V – anual: devem ser retidos por cinco anos.

Art. 16. A solicitação de salvaguarda dos dados deve ser realizada pelos responsáveis técnicos dos serviços de TI, com a anuência prévia e formal dos gestores negociais, refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação envolvidos e a criticidade da informação para a continuidade da operação da organização.

Parágrafo único. A solicitação deve explicitar, no mínimo, os seguintes requisitos técnicos:

I – escopo (dados digitais a serem salvaguardados);

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

III – frequência temporal de realização do backup (diária, semanal, mensal, anual);

IV – retenção;

V – RPO; e

VI – RTO.

Art. 17. A recuperação de dados não será viabilizada em caso de perdas anteriores à conclusão da cópia de segurança. Dados criados ou modificados entre execuções de cópias de segurança subsequentes não serão protegidos por soluções de backup.

Art. 18. A alteração das frequências e dos tempos de retenção estabelecidos deve ser precedida de solicitação e justificativa formais encaminhadas ao administrador de backup pelo gestor negocial dono da informação.

CAPÍTULO VI

DOS TESTES DE BACKUP

Art. 19. Os backups devem ser testados periodicamente, com o objetivo de garantir a confiabilidade e a integridade dos dados salvaguardados.

Art. 20. Os testes de restauração dos backups devem ser realizados por amostragem, em equipamentos/servidores diferentes dos equipamentos que atendem aos ambientes de produção.

Art. 21. A periodicidade, a abrangência, os procedimentos e as rotinas inerentes aos testes de backup serão definidos em processo específico a ser elaborado pela Unidade Gestora de Serviços e Aplicações, em conjunto com os gestores negociais e a Unidade Gestora de Segurança da Informação.

CAPÍTULO VII

DAS MÍDIAS DE BACKUP

Art. 22. Os backups podem ser armazenados em:

I – disco rígido;

II – fitas magnéticas; e

III – nuvem.

Art. 23. Os dados devem ser periodicamente copiados para um dispositivo de disco distinto daquele em que se encontram, de tal forma que possam ser recuperados e restaurados em caso de corrompimento, de indisponibilidade ou de perda dos dados de produção.

Art. 24. De acordo com a criticidade, as cópias de segurança armazenadas em disco podem ser copiadas para fitas magnéticas apropriadas para esse fim ou em nuvem.

Art. 25. O descarte das mídias de backup inservíveis ou inutilizáveis deverá ser realizado mediante proposta apresentada pelo administrador de backup dirigida à unidade competente, conforme política de descarte vigente.

Parágrafo único. As mídias a serem descartadas deverão ser destruídas, de forma a impedir a sua reutilização ou o acesso indevido às informações por pessoas não autorizadas.

Art. 26. 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.

CAPÍTULO VIII

DO BACKUP DE BANCO DE DADOS

Art. 27. Os dados estruturados, armazenados nos bancos de dados de produção do CNJ, devem ser periodicamente copiados para um dispositivo de disco distinto daquele em que se encontram, de tal forma que possam ser recuperados e restaurados em caso de corrompimento, de indisponibilidade ou de perda dos dados de produção.

Art. 28. O backup em disco deve permitir a restauração íntegra de um banco de dados até o momento imediatamente anterior ao evento que causou a corrupção, a indisponibilidade ou a perda dos dados, observados os períodos de retenção estabelecidos.

Art. 29. O procedimento de backup de banco de dados deve ser realizado preferencialmente fora do horário de expediente, não devendo indisponibilizar o banco de dados do qual esteja sendo extraído.

Art. 30. Como medida adicional de segurança, os backups dos dados de produção podem ser copiados para fita ou nuvem, conforme critério da Unidade Gestora de Serviços e Aplicações.

Art. 31. Devem ser adotadas estratégias específicas e diferenciadas de backup para os dados de produção armazenados em cada ambiente em virtude de critérios como tamanho das bases de dados gerenciadas, criticidade da informação para o CNJ e mecanismos de backup.

CAPÍTULO IX

DAS DISPOSIÇÕES FINAIS

Art. 32. A Política de Backup e Restauração de Dados do CNJ deverá ser revisada bianualmente ou quando necessário.

Art. 33. Esta Portaria entra em vigor na data de sua publicação.