

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.

Ministra **ROSA WEBER**

PORTARIA PRESIDÊNCIA N. 198, DE 07 DE AGOSTO DE 2023.

Institui Grupo de Trabalho para avaliar a necessidade de atualizações e de adequações ao Método Integrado de Gestão de Riscos (MIGRI).

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. 05017/2023,

CONSIDERANDO que a Constituição da República assegura ao Poder Judiciário autonomia administrativa (art. 99) e atribui ao CNJ a missão de zelar pela autonomia do Poder Judiciário e pelo cumprimento do Estatuto da Magistratura (art. 103-B, § 4º, I);

CONSIDERANDO a Resolução CNJ n. 344/2020, que regulamenta o exercício do poder de polícia administrativa no âmbito dos tribunais, dispondo sobre as atribuições funcionais dos(as) agentes e inspetores(as) da polícia judicial;

CONSIDERANDO a Resolução CNJ n. 435/2021, que dispõe sobre a política e o sistema nacional de segurança do Poder Judiciário e dá outras providências;

CONSIDERANDO o entendimento firmado pelo Presidente do Comitê Gestor do Sistema Nacional de Segurança do Poder Judiciário nos autos do Processo SEI 05017/2023;

RESOLVE:

Art. 1º Instituir Grupo de Trabalho para avaliar a necessidade de atualizações e de adequações ao Método Integrado de Gestão de Riscos (MIGRI).

Art. 2º O Grupo de Trabalho será composto pelos seguintes membros:

I – Marcelo CanizaresSchettini Seabra, Secretário de Segurança Institucional do Supremo Tribunal Federal;

II – Hipólito Alves Cardozo, Coordenador de Segurança Institucional do Supremo Tribunal Federal;

III – Luciano Santana Lopes, servidor do Superior Tribunal Militar;

IV – Bernardo Soares Fialho, servidor do Conselho Nacional de Justiça;

V – Emerson Silva Gomes, servidor do Conselho Nacional de Justiça;

VI – Renato Duarte de Almeida, servidor do Conselho Nacional de Justiça;

VII – Vanderli de Mariz Gomes, servidora do Conselho Nacional de Justiça;

VIII – Alexandre Magno de Souza Nunes, servidor do Tribunal de Justiça do Estado do Maranhão;

IX – Wanderson José Gomes do Carmo, servidor do Tribunal de Justiça do Distrito Federal e dos Territórios;

X – Agostinho Gonçalo de Lira Júnior, servidor do Tribunal de Justiça do Distrito Federal e dos Territórios;

XI – Epifânio Passos de Albuquerque, servidor do Tribunal Regional Federal da 1ª Região;

XII – Jefferson Moreira de Oliveira, servidor do Tribunal Regional Federal da 2ª Região;

XIII – Lenildo Pereira Lima, servidor do Superior Tribunal de Justiça;

XIV – Felipe TomanikBoucault Pires Alves, servidor do Tribunal Superior do Trabalho;

XV – Joanir Ricardo Pereira dos Santos, servidor do Tribunal de Justiça do Estado de Santa Catarina.

Parágrafo único. O Grupo de Trabalho será presidido pelo Secretário de Segurança Institucional do Supremo Tribunal Federal e a vice-presidência competirá ao Coordenador de Segurança Institucional da mesma Corte.

Art. 3º O Grupo de Trabalho encerrará suas atividades em 90 (noventa) dias, com a apresentação de propostas ou de relatório final.

Parágrafo único. O prazo previsto no *caput* deste artigo poderá ser prorrogado, mediante justificativa.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

Ministra **ROSA WEBER**

PORTARIA PRESIDÊNCIA N. 203, DE 10 DE AGOSTO DE 2023.