JUSTIÇA FEDERAL
CONSELHO DA JUSTIÇA FEDERAL

PORTARIA N. 540-CJF

Dispõe sobre a institucionalização da política de backup e restauração de dados no âmbito do Conselho da Justiça Federal.

O PRESIDENTE DO CONSELHO DA JUSTIÇA FEDERAL, no uso de suas atribuições legais, tendo em vista o que consta no Processo n. 0002044-26.2021.4.90.8000, e

CONSIDERANDO a necessidade de atender às necessidades e expectativas do órgão quanto à redução de riscos e implementação com maior celeridade dos serviços de Tecnologia da Informação – TI providos pela Secretaria de Tecnologia da Informação – STI;

CONSIDERANDO os termos da Resolução CNJ n. 370, de 28 de janeiro de 2021, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário – ENTIC-JUD;

CONSIDERANDO os Acórdãos n. 1603/2008, 2308/2010, 2585/2012, 1200/2014 e 3051/2014, todos do Plenário do Tribunal de Contas da União, que recomendam a promoção de ações voltadas para a normatização e o aperfeiçoamento dos processos de governança, gestão e uso de Tecnologia da Informação e Comunicação;

CONSIDERANDO o Acórdão n. 1109/2021, do Plenário do Tribunal de Contas da União, que recomenda a aprovação formal e a atualização das políticas gerais e planos específicos de backup;

CONSIDERANDO as iniciativas constantes da Estratégia do Conselho da Justiça Federal para o período de 2021 a 2026, estabelecidas pela Portaria CJF n. 576, de 24 de novembro de 2020,

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES E DEFINIÇÕES

Art. 1º Institucionalizar a política de backup das informações eletrônicas no âmbito do Conselho da Justiça Federal – CJF, com o objetivo de estabelecer diretrizes para o processo de cópia de segurança dos dados armazenados sob a custódia da Secretaria de Tecnologia da Informação – STI, a fim de garantir a integridade, a disponibilidade e a confidencialidade dos dados.

Art. 2º Para o disposto nesta Portaria, considera-se:

I – administrador de backup: responsável pelos procedimentos de configuração, execução, monitoramento e testes dos procedimentos de backup e restauração;

II – administrador de recursos: unidade responsável pela operação técnica dos ativos e serviços de TI, podendo ser área diversa da STI;

III – ativo: aquilo que tem valor – tangível ou intangível – para a organização (tais como informação, software, equipamentos, instalações, serviços, pessoas e imagem institucional);

IV – backup: cópia de segurança de dados em meio digital;

V – backup completo: modalidade em que todos os dados são copiados integralmente;

VI – backup diferencial: modalidade em que somente os arquivos novos ou modificados são copiados desde o último backup completo, tendo como principal vantagem o menor tempo para restauração do backup;

VII – backup incremental: modalidade em que somente os arquivos novos ou modificados são copiados desde o último backup, tendo como principal vantagem o menor tempo para realização do backup;

VIII – backup on-line: uma vez realizado, é acessível dentro da rede de dados do CJF;

IX – backup off-line: uma vez realizado, o backup é armazenado em mídias físicas desconectadas da rede de dados do CJF;

X – backup off-site: uma vez realizado, o backup é armazenado em *data center* diverso e geograficamente separado do centro de dados principal do CJF, podendo também ser realizado por meio de serviço de backup em nuvem;

XI – cliente de backup: é todo equipamento em que é instalado o agente de backup;

XII – custódia: consiste na responsabilidade de se guardar um ativo para terceiros;

XIII – *disaster recovery*: estratégia de recuperação de dados motivada por sinistros de grave amplitude, física ou lógica;

XIV – disponibilidade: garantia de que o dado esteja acessível e utilizável sob demanda de pessoa ou entidade devidamente autorizada;

XV – gestor da informação: agente púbico formalmente responsável pela administração do serviço ou sistema de TI e pelas informações produzidas em seu processo de trabalho, sendo, geralmente, um gestor da área de negócio;

XVI – integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XVII – mídia: meio físico no qual se armazenam os dados de backup;

XVIII – replicação de backup**:** cópia de segurança adicional realizada a partir da cópia original do backup, podendo ser armazenada em outro meio físico;

XIX – restauração: processo de restauração da cópia de segurança;

XX – retenção: período de tempo em que o conteúdo de backup deve ser preservado.

CAPÍTULO II
DAS RESPONSABILIDADES

Art. 3º A Subsecretaria de Infraestrutura e Suporte Técnico – SUTEC, da Secretaria de Tecnologia da Informação, é a unidade administradora do serviço de backup responsável pela operacionalização da política descrita nesta Portaria.

Art. 4º É atribuição do administrador do serviço de backup:

I – providenciar a criação e manutenção dos backups;

II – configurar as ferramentas de backup;

III – manter as mídias preservadas, funcionais e seguras;

IV – efetuar testes de backup e auxiliar nos procedimentos de restauração;

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

VI – restaurar os backups quando necessário;

VII – gerenciar mensagens e registros diários dos backups;

VIII – comunicar ao gestor da informação os erros e as ocorrências nos backups;

IX – propor modificações para o aperfeiçoamento da política de backup;

X – realizar a monitoração e a proteção das informações relativas às bases de dados dos backups *(*catálogo de backup);

XI – definir os parâmetros mínimos para operacionalização da solicitação do backup.

Art. 5º É atribuição do administrador de recurso:

I – solicitar serviço de backup com informações suficientes para a identificação da origem dos dados a serem protegidos;

II – dar permissão ao administrador de backup para configurar e modificar o agente de backup;

III – solicitar restaurações de dados, com anuência do gestor da informação, quando couber;

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

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

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

Art. 6º São atribuições dos gestores da informação:

I – solicitar, formalmente, o backup das informações ao administrador de recurso;

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

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

CAPÍTULO III
DOS PADRÕES OPERACIONAIS

Seção I
Dos princípios gerais

Art. 7° A política de backup e restauração de dados estará alinhada à gestão de continuidade de negócios em nível organizacional, devidamente amparada nas estratégias e políticas de TI do CJF.

Art. 8° As rotinas de backup serão preferencialmente orientadas para a restauração dos dados em menor tempo possível.

Art. 9° As rotinas de backup possuirão requisitos específicos de acordo com o tipo de serviço de TI ou dado salvaguardado, com prioridade aos serviços de TI críticos da organização.

Art. 10. Será elaborada lista de sistemas com designação do respectivo gestor da informação e sua classificação quanto à criticidade (críticos e não críticos).

Art. 11. A criação e a operação dos backups obedecerão às seguintes orientações:

a) será utilizada, sempre que possível, criptografia dos dados armazenados e em trânsito;

b) o backup será programado para a execução automática em horários de menor

utilização dos sistemas e da rede de dados, conforme definição do administrador de backup;

c) os backups serão protegidos por meio de mecanismos de controle de acesso físico e lógico ao local de armazenamento de dados.

Seção II
Da frequência e retenção dos dados de backups

Art. 12. Os backups dos serviços de TI do CJF serão realizados utilizando-se as seguintes frequências temporais:

I – diária;

II – semanal;

III – mensal.

Art. 13. Os backups do ambiente de produção terão, no mínimo, duas cópias, sendo uma on-line e outra off-line ou off-site.

Parágrafo único: Os serviços de TI classificados como críticos contarão com backups em dispositivos off-line e off-site.

Art. 14. A recuperação de dados não será possível em caso de perdas anteriores à conclusão da cópia de segurança.

Art. 15. Os backups seguirão diretrizes diferenciadas, conforme disposto a seguir:

I – ambientes de produção do CJF:

a) provenientes de sistema de arquivos, com retenção mínima de: diário: 60 dias; semanal: 12 semanas; e mensal: 24 meses;

b) provenientes de sistema operacional, com retenção mínima de: diário: 60 dias; semanal: 12 semanas; e mensal: 24 meses;

c) provenientes de servidores de aplicação, com retenção mínima de: diário: 60 dias; semanal: 12 semanas; e mensal: 24 meses;

d) provenientes de banco de dados, com retenção mínima de: diário: 60 dias; semanal: 12 semanas; e mensal: 24 meses.

e) provenientes de trilhas de auditoria (log), com retenção mínima de: diário: 30 dias; semanal: 6 semanas; e mensal: 12 meses.

II – ambientes de homologação e de desenvolvimento do CJF:

a) provenientes de sistema de arquivos, com retenção mínima de: diário: 20 dias; e semanal: 8 semanas;

b) provenientes de sistema operacional, com retenção mínima de: diário: 20 dias; e semanal: 8 semanas;

c) provenientes de servidores de aplicação, com retenção mínima de: diário: 20 dias; e semanal: 8 semanas;

d) provenientes de banco de dados, com retenção mínima de: diário: 20 dias; e semanal: 8 semanas.

III – ambientes de replicação (off-site):

a) provenientes de sistema de arquivos, com retenção mínima de: diário: 30 dias;

b) provenientes de sistema operacional, com retenção mínima de: diário: 30 dias;

c) provenientes de servidores de aplicação, com retenção mínima de: diário: 30 dias;

d) provenientes de banco de dados, com retenção mínima de: diário: 30 dias.

Art 16. Expirado o prazo de retenção do backup, a mídia poderá ser reutilizada ou destruída, conforme diretrizes aplicáveis.

Seção III
Da restauração e testes de backup

Art. 17. Os testes de integridade dos backups de produção com retenção mensal serão realizados por amostragem ao menos mensalmente.

Parágrafo único. Serão realizados testes de integridade dos backups dos serviços considerados críticos pelo Comitê de Governança de Tecnologia da Informação – CGovTI ao menos uma vez por ano.

Art. 18. As cópias do tipo “Recuperação de Desastres” dos sistemas críticos serão feitas com base na replicação do backup e serão mantidas off-site e off-line.

CAPÍTULO IV
DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 19. A política de backup e restauração de dados estabelece como metas:

I – providenciar a implementação dos novos prazos de retenção em todos os ambientes de backup em até um mês após a publicação desta Portaria;

II – elaborar lista de sistemas de informação classificados quanto à criticidade (críticos e não críticos) em até três meses após a publicação desta Portaria;

III – implementar backup off-line e off-site dos serviços de TI críticos em até 18 meses após a publicação desta Portaria.

Art. 20. A política de backup e restauração de dados será atualizada sempre que necessário e revisada, no mínimo, a cada 12 meses.

Art. 21. Esta política será amplamente divulgada às unidades do Conselho da Justiça Federal.

Art. 22. Os casos omissos serão dirimidos pelo CGovTI.

Art. 23. Fica revogada a Portaria CJF n. 85, de 15 de março de 2018.

Art. 24. Esta Portaria entra em vigor na data de sua publicação.

Ministro **HUMBERTO MARTINS**

Presidente

Autenticado eletronicamente por **Ministro HUMBERTO EUSTÁQUIO SOARES MARTINS**, **Presidente**, em 27/10/2021, às 14:29, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.cjf.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0275473** e o código CRC **013045A1**.