SUPERIOR TRIBUNAL DE JUSTIÇA

INSTRUÇÃO NORMATIVA STJ/GDG N. 1 DE 25 DE JANEIRO DE 2022.

O DIRETOR-GERAL EM SUBSTITUIÇÃO DA SECRETARIA DO SUPERIOR TRIBUNAL DE JUSTIÇA, usando da atribuição conferida pelo item 17.2, inciso X, alínea *b*, do Manual de Organização do STJ e considerando a Resolução CNJ n. 370, de 28 de janeiro de 2021, e o que consta do Processo STJ n. 007573/2021,

RESOLVE:

Seção I

Das Disposições Iniciais

Art. 1º Fica instituída a Política de Cópia de Segurança e de Recuperação de Dados do Superior Tribunal de Justiça, com o objetivo de estabelecer diretrizes para o processo de cópia, armazenamento e restauração dos dados sob a guarda da Secretaria de Tecnologia da Informação e Comunicação – STI.

§ 1º A política de que trata o *caput* deve garantir a integridade, a disponibilidade e a continuidade da prestação dos serviços suportados pela STI.

§ 2º As informações do STJ disponíveis em aplicações corporativas e ativos de infraestrutura devem ser protegidas por meio de rotinas sistemáticas de cópia de segurança.

Art. 2º Para os efeitos desta instrução normativa, consideram-se:

I – ativo de infraestrutura: equipamento ou sistema de infraestrutura de TI que armazena dados ou informações corporativas;

II – cópia de segurança (*backup*): cópia de dados de um dispositivo de armazenamento a um outro, visando que suas informações possam ser restauradas em caso de perda dos dados originais;

III – recuperação de desastre (*disaster recovery)*: estratégia de recuperação de dados motivada por eventos de grande impacto físico ou lógico;

IV – retenção: período no qual o conteúdo da mídia de cópia de segurança deve ser preservado;

V – restauração: procedimento utilizado para recuperação de dados ou repositório de arquivos utilizando a cópia de segurança;

VI – gestor de cópia de segurança: servidor da STI responsável por supervisionar a execução do processo de cópia de segurança, zelando por sua melhoria contínua e conformidade com esta instrução normativa;

VII – regras de cópia de segurança: conjunto de parâmetros que configuram as cópias de segurança e sua recuperação em cada ativo de infraestrutura;

Fonte: Boletim de Serviço do STJ, 26 jan. 2022.

VIII – administrador do recurso: servidor do quadro da STI que, em conjunto com o gestor de cópia de segurança, é responsável pela definição, análise e revisão das regras de cópia de segurança necessárias para garantir a efetiva recuperação dos dados para os serviços de TI sob sua responsabilidade;

IX – operador de cópia de segurança: servidor do quadro da STI ou profissional terceirizado responsável pelos procedimentos de execução, monitoramento, reconfiguração e testes dos procedimentos de cópia de segurança, arquivamento, duplicação, replicação e restauração;

X – duplicação: movimentação dos dados de ambiente de armazenamento de curta duração para as mídias de cópia de segurança;

XI – mídia de cópia de segurança: meio físico no qual efetivamente são armazenados os dados de uma cópia de segurança;

XII – replicação: processo de cópia e armazenamento síncrono de dados em ambientes distintos com o intuito de restaurá-los caso haja falha em um dos ambientes;

XIII – modalidade de cópia de segurança: diz respeito à forma de cópia do dado considerando o estado das alterações desses dados nos ativos de infraestrutura;

XIV – requisitos específicos de segurança da informação: conjunto de necessidades de segurança que visam proteger informações consideradas sensíveis ou críticas no processo de cópia de segurança.

Seção II

Das Responsabilidades

Art. 3º São atribuições do gestor de cópia de segurança:

I – supervisionar a execução das cópias de segurança zelando por sua conformidade com esta instrução normativa;

II – atuar junto ao administrador do recurso pela definição da melhor técnica (medidas) para garantir a integridade da execução das cópias de segurança;

III – organizar e analisar as demandas recebidas relativas às cópias de segurança;

IV – verificar periodicamente os relatórios gerados pelas ferramentas e/ou pelo operador de cópia de segurança;

V – sugerir mudanças nos relatórios, ferramentas e processos relativos à cópia de segurança;

VI – interceder junto ao operador de cópia de segurança para intervenção imediata a quaisquer problemas detectados;

VII – comunicar ao administrador do recurso os erros e as ocorrências nas cópias de segurança;

VIII – elaborar e manter atualizado manual técnico de cópia de segurança, que deverá conter os planos, os procedimentos e os roteiros técnicos necessários ao processo de cópia.

Parágrafo único. O manual técnico constante no inciso VIII deverá fazer os seguintes detalhamentos:

I – dos requisitos específicos de segurança da informação no processo de cópia;

II – da abrangência dos dados copiados;

III – da frequência e da modalidade dos processos para cada tipo de ativo de infraestrutura.

Art. 4º São atribuições do operador de cópia de segurança, em acordo e sob a supervisão do gestor de cópia de segurança:

I – propor modificações visando ao aperfeiçoamento dos procedimentos de cópia de segurança;

II – configurar a ferramenta de cópia de segurança e seus clientes, conforme acordos estabelecidos;

III – verificar periodicamente os relatórios gerados pelas ferramentas e elaborar para o gestor de cópia de segurança os relatórios consolidados relativos à gestão do ambiente;

IV – comunicar ao administrador do recurso os erros e as ocorrências nas cópias de segurança;

V – analisar mensagens e *logs* diários das cópias de segurança, fazendo o tratamento dos erros de forma que o procedimento de cópia de segurança tenha sequência e os erros na sua execução sejam eliminados;

VI – realizar manutenções periódicas dos dispositivos de cópia de segurança;

VII – realizar o carregamento das mídias necessárias para as cópias de segurança programadas;

VIII – realizar o armazenamento das mídias de cópia de segurança em cofre próprio.

Art. 5º São atribuições do administrador de recurso:

I – coletar informações acerca dos tipos de dados armazenados nos ativos de infraestrutura, informando a natureza e o tratamento que deve ser dispensado aos dados, bem como informar se há necessidades especiais de tempo de retenção das cópias de segurança realizadas nos ativos sob sua responsabilidade;

II – compor equipe de definição das regras de cópia de segurança juntamente ao gestor de cópia de segurança;

III – definir as regras de cópia de segurança considerando a efetiva recuperação dos dados para o ativo de infraestrutura sob sua responsabilidade;

IV – solicitar revisão das regras de cópia de segurança para seu ativo de informação ou serviço correspondente sempre que julgar necessário.

Seção III

Da Modalidade e Tempos de Retenção das Cópias de Segurança

Art. 6º Os ativos de infraestrutura que armazenem dados são objeto de inclusão no processo de cópia de segurança.

Art. 7º As modalidades de cópia de segurança disponíveis a serem consideradas são:

I – *full*: modalidade na qual os dados são copiados integralmente;

II – incremental: modalidade na qual somente os arquivos novos ou modificados são

copiados;

III – diferencial: modalidade na qual os arquivos novos ou modificados da base de dados incremental são copiados;

IV – cumulativa: modalidade que copia todos os blocos alterados após a última cópia de segurança incremental.

Art. 8º O administrador de recursos deve definir os prazos de realização, retenção e descarte das informações armazenadas na cópia de segurança, de acordo com a necessidade de cada serviço.

§ 1º Ficam estipulados os seguintes prazos padrão de retenção de cópia de segurança:

I – noventa dias para máquinas que hospedem serviços de desenvolvimento, homologação e treinamentos;

II – cento e oitenta dias para máquinas que hospedem serviços de produção (inclusive serviço de correio eletrônico);

III – dois anos como prazo máximo de retenção da cópia, mediante justificativa fundamentada;

IV – acima de dois anos de retenção dos dados somente em casos de atendimento a previsões legais.

§ 2º Os prazos estipulados neste artigo deverão ser submetidos à análise da Comissão Permanente de Avaliação de Documentos do STJ, que fará estudo quanto à temporalidade e verificará a necessidade de atualização dos instrumentos de gestão documental.

Seção IV

Dos Procedimentos de Criação e Operação da Cópia de Segurança

Art. 9º A criação das cópias de segurança deverá obedecer às seguintes orientações:

I – a cópia de segurança deverá ser criada na ferramenta de cópia de segurança, seguindo as orientações do gestor de cópia de segurança;

II – a cópia de segurança deverá ser programada para execução automática em horários de menor impacto no desempenho de sistemas e da rede, conforme definição do gestor de cópia de segurança.

Art. 10. A operação das cópias de segurança deverá obedecer às seguintes orientações:

I – a cópia de segurança deverá ser operada e monitorada pelo operador de cópia de segurança;

II – para cada cópia de segurança realizada com sucesso, deve ser gerado relatório automatizado pela própria ferramenta de cópia de segurança, confirmando a execução da operação.

Art. 11. As cópias de segurança são realizadas, inicialmente, em equipamentos especializados para armazenamento de longa retenção de cópia de segurança em disco e, posteriormente, de forma definitiva, em mídias físicas de longa retenção, devidamente identificadas, etiquetadas e numeradas sequencialmente, que serão guardadas nos cofres de segurança do Tribunal.

Parágrafo único. As cópias de segurança serão armazenadas em nuvem ou em

infraestrutura remota (*off site*) de acordo com a natureza dos dados e da origem da cópia.

Seção V

Da Solicitação de Restauração de Cópia de Segurança

Art. 12. A solicitação de restauração de uma cópia de segurança poderá ser realizada sempre que houver a necessidade de recuperação de dados nos ativos de infraestrutura.

Art. 13. A restauração da cópia de segurança deverá ser solicitada pelos gestores das unidades por meio do Serviço de Atendimento ao Cliente da STI (SAC).

Art. 14. A restauração da cópia de segurança será efetuada respeitadas as definições das regras de cópias de segurança definidas para o ativo de infraestrutura correspondente, conforme as opções dispostas na Seção III desta instrução normativa.

Art. 15. O encarregado de dados pessoais do Tribunal deve ser comunicado, em até 48 horas contadas da data de restauração, sobre eventual recuperação de cópia de segurança que contenha dados pessoais.

Seção VI

Sobre o Teste de Recuperação de Dados

Art. 16. As cópias de segurança armazenadas em fita devem ser testadas de forma amostral, a cada mês, para assegurar que a confiabilidade das mídias de cópia de segurança, a integridade dos dados e o tempo de restauração das cópias estejam aderentes aos requisitos de continuidade de negócio, fornecidos pelo administrador de recurso.

§ 1º A prioridade do procedimento de teste será do ambiente de produção dos serviços de TI e, posteriormente, os ambientes de homologação e de desenvolvimento.

§ 2º Os testes devem incluir procedimentos de restauração dos dados para comprovar a eficácia das cópias de segurança.

§ 3º As cópias de segurança devem ser restauradas em ambientes de teste distintos dos de produção, como forma de validação.

§ 4º Uma cópia de segurança será considerada válida quando o ambiente original puder ser recriado em um estado consistente.

Seção VII

Regras do Processo de Descarte

Art. 17. O descarte das mídias de cópia de segurança inservíveis ou inutilizáveis deverá ser realizado mediante proposta apresentada pelo gestor de cópia de segurança dirigida à unidade competente, conforme política de descarte vigente.

§ 1º As mídias a serem descartadas deverão ser destruídas de forma a impedir a sua

reutilização ou acesso indevido às informações por pessoas não autorizadas.

§ 2º O processo de destruição deverá ocorrer nas instalações do Tribunal com o acompanhamento constante de servidor ou de técnico terceirizado competente e designado.

Seção VIII

Das Disposições Finais

Art. 18. Os casos omissos serão resolvidos pelo Secretário de Tecnologia da Informação e Comunicação.

Art. 19. Esta instrução normativa entra em vigor na data de sua publicação.

Documento assinado eletronicamente por **Luiz Antonio de Souza Cordeiro**, **Diretor-Geral - Em Substituição**, em 25/01/2022, às 15:23, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.stj.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2803283** e o código CRC **790BD692**.