INSTRUÇÃO NORMATIVA Nº 300, DE 09 DE JULHO DE 2024

Dispõe sobre a gestão de cópias de segurança no Supremo Tribunal Federal.

***O DIRETOR-GERAL DA SECRETARIA DO SUPREMO TRIBUNAL FEDERAL**, no uso das atribuições que lhe confere o art. 41, inciso X, alínea b, do Regulamento da Secretaria de 2024, e considerando a Resolução 773/2022, que instituiu a Política de Segurança da Informação do Supremo Tribunal Federal, a Resolução 759/2021, que instituiu a Política de Privacidade e de Proteção de Dados Pessoais no âmbito do Supremo Tribunal Federal e o contido no Processo Administrativo eletrônico 003388/2022,*

***R E S O L V E**:*

Art. 1º A gestão de cópias de segurança do Supremo Tribunal Federal (STF) fica regulamentada por esta instrução normativa.

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 2º Para os efeitos desta IN, considera-se:

I – administrador de backup: pessoa ou unidade organizacional especialista em proteção de dados e responsável pela configuração, execução e monitoramento dos procedimentos de cópias de segurança;

II – proprietário do ativo: pessoa ou unidade organizacional responsável pelo gerenciamento do ciclo de vida de um ativo de informação;

III – retenção: período durante o qual o dado copiado deverá ficar retido e disponível para uso;

IV – Recovery point objetive (RPO): indicador que mensura o estado de consistência desejável para recuperação de dados;

V – Recovery time objetive (RTO): indicador que mensura o tempo desejável para restauração de uma cópia de segurança;

VI – Tabela de Temporalidade: prazo de permanência de um documento em um arquivo e a respectiva destinação após esse período.

Parágrafo único. Adicionalmente, aplica-se o glossário de termos de segurança da informação definido e publicado no Repositório Digital do STF (https://bibliotecadigital.stf.jus.br/xmlui/).

Art. 3º A gestão de cópias de segurança está alinhada às estratégias da Política de Segurança da Informação do STF (PSI/STF), tendo como premissas:

I – a simplicidade dos procedimentos, a fim de minimizar erros;

II – a construção de ambiente resiliente, em que seja possível o restabelecimento dos sistemas e dos serviços de tecnologia da informação (TI), em caso de incidentes, desastres ou falhas de mídia de armazenamento;

III – a proteção das cópias de segurança e o melhor custo-benefício no armazenamento e na segurança dos dados.

Art. 4º São objetivos da gestão de cópias de segurança:

I – preservar os ativos de informação;

II – assegurar a simplicidade, a completude e a proteção das cópias de segurança do STF;

III – garantir a integridade e a disponibilidade das informações, quando necessária sua recuperação.

Art. 5º Esta instrução normativa se aplica aos proprietários de ativos de informação e ao administrador de backup.

Parágrafo único. Os proprietários de ativos e o administrador de backup são igualmente responsáveis pela gestão das cópias de segurança, devendo acompanhar a sua efetiva implementação.

CAPÍTULO II

DAS COMPETÊNCIAS

Art. 6º Ao proprietário do ativo compete:

I – realizar a classificação dos serviços e dos sistemas sob sua responsabilidade para adequada implementação das rotinas de cópias de segurança;

II – elaborar e executar o plano de cópia de segurança; e

III – verificar regularmente a integridade das cópias de segurança.

Art. 7º Ao administrador de backup compete:

I – apoiar e validar os planos de cópias de segurança e os procedimentos de arquivamento e de retenção, mantendo-os atualizados; e

II – privilegiar a uniformização do RPO e do RTO entre os vários sistemas e serviços, com o intuito de manter a simplicidade no processo de cópias de segurança.

Parágrafo único. O administrador de backup observará a existência de recursos técnicos, financeiros, operacionais e o plano de continuidade de negócio, quando existente, como critérios de validação do plano de cópia de segurança.

Art. 8º Compete ao proprietário do ativo e ao administrador de backup:

I – planejar e executar testes de recuperação de dados, de forma que seja possível recuperar as imagens de backup do ambiente, quando necessário;

II – validar a integridade do processo de backup;

III – viabilizar que os sistemas críticos de informação possuam cópias de segurança e/ou mecanismos de resiliência suficientes para recuperação do sistema completo;

IV – empregar mecanismos de segurança apropriados para proteção das cópias de segurança de acordo com os recursos disponíveis, observado o plano de continuidade de negócios, quando existente; e

V – reportar a necessidade de investimentos em recursos técnicos, financeiros e operacionais para viabilizar a realização do procedimento de cópias de segurança e de restauração do ambiente.

CAPÍTULO III

DO PLANO DAS CÓPIAS DE SEGURANÇA

Art. 9º As informações serão protegidas por meio de rotinas sistemáticas de cópia de segurança, estabelecidas no plano próprio de que trata o inciso II do art. 7º desta instrução normativa.

Art. 10. O plano de cópia de segurança conterá, no mínimo:

I – escopo, com a especificação do conteúdo e a definição dos itens a serem protegidos;

II – designação do tipo de cópia de segurança, sendo possível a atribuição de mais de um tipo;

III – frequência temporal de realização da cópia de segurança, se diária, semanal, mensal ou anual, sendo possível associá-las;

IV – período de retenção, que deverá ser definido com base na criticidade, frequência de atualização dos dados e características específicas de cada sistema;

V – especificação dos testes de restauração, com periodicidade, abrangência, procedimentos e rotinas;

VI – RPO (recovery point objetive);

VII – RTO (recovery time objetive).

§ 1º O escopo do plano de cópia de segurança poderá incluir:

I – arquivos de sistemas operacionais e de seus respectivos servidores de rede;

II – dados judiciais e corporativos armazenados em diretórios de rede;

III – dados judiciais e corporativos armazenados em banco de dados;

IV – dados dos sistemas de segurança orgânica e de acesso às dependências do STF;

V – mensagens corporativas;

VI – principais registros de eventos (logs) e trilhas de auditoria de sistemas de informação;

VII – código-fonte dos sistemas informatizados, bem como arquivos de configuração, scripts e demais artefatos considerados necessários para restauração do ambiente.

§ 1º Para cada item contemplado no plano, será especificado, quando couber, se é conteúdo imutável e/ou passível de arquivamento e de versionamento.

§ 2º Caso sejam necessárias cópias de segurança referentes a arquivos e bancos de dados que não façam parte do ambiente de produção, tais como desenvolvimento, homologação e testes, a demanda deve ser solicitada ao administrador de backup, acompanhada das devidas justificativas.

§ 3º Os planos, os procedimentos técnicos e os roteiros de cópias de segurança serão definidos para atender às necessidades de negócio e/ou aos requisitos do STF.

CAPÍTULO IV

DA REALIZAÇÃO DAS CÓPIAS DE SEGURANÇA

Art. 11. As tecnologias utilizadas para a realização da cópia de segurança cumprirão os requisitos necessários para preservar a integridade, a confidencialidade e a disponibilidade das informações.

Art. 12. As cópias de segurança devem ser geradas em mídias especificadas pelo fabricante do equipamento e atender ao uso de hardware e software definidos pelo administrador do backup.

Art. 13. Após a realização das cópias de segurança, os logs registrados serão analisados pela solução tecnológica utilizada para sua geração, com vistas a atestar o êxito da operação e/ou adotar as providências cabíveis, no caso de eventuais erros.

CAPÍTULO V

DA PROTEÇÃO DAS CÓPIAS DE SEGURANÇA

Art. 14. As cópias de segurança serão protegidas, por meio de segurança física ou de criptografia, ao serem armazenadas e movimentadas na rede.

Parágrafo único. O disposto no caput deste artigo também se aplica a cópias de segurança remotas e a dados de serviço de nuvem.

Art. 15. O armazenamento das cópias de segurança observará os seguintes critérios:

I – rápida localização;

II – guarda em centro de dados ou em repositório de mídia disposto em local fisicamente distinto do dado original;

III – as cópias de segurança dos sistemas críticos possuirão réplicas armazenadas fora das dependências do STF em pelo menos uma localização que não seja endereçável de forma contínua por meio de chamadas do sistema operacional.

Art. 16. Os locais de armazenamento das mídias conterão mecanismos adequados de segurança, que considerarão, minimamente, os seguintes elementos:

I – restrição e monitoramento do acesso ao local;

II – proteção contra agentes nocivos naturais (poeira, calor, umidade, entre outros);

III – proteção contra interferências eletromagnéticas;

IV – controles de prevenção, detecção e combate a incêndio.

Parágrafo único. Dados corporativos serão armazenados nos repositórios institucionais designados pela STI.

CAPÍTULO VI

DA RESTAURAÇÃO DE DADOS

Art. 17. A cópia de segurança será restaurada nas seguintes situações:

I – recomposição da integridade do ambiente afetado após incidente, desastre ou falha de mídia de armazenamento;

II – atendimento da solicitação formal do proprietário do ativo;

III – realização dos testes de recuperação periódicos; e

IV – realização de auditorias e de investigações legais e forenses.

§ 1º Testes de restauração devem ser realizados periodicamente, com o objetivo de garantir a confiabilidade dos procedimentos de recuperação e a integridade das cópias de segurança.

§ 2º As informações restauradas serão excluídas após a realização dos testes de que trata o § 1° deste artigo.

CAPÍTULO VII

DAS DISPOSIÇÕES FINAIS

Art. 18. O descarte das mídias utilizadas para gravação das cópias de segurança será realizado de forma a evitar que os dados armazenados sejam recuperados posteriormente por terceiros.

Art. 19. Os planos de cópias de segurança serão revisados anualmente, de forma a mantê-los condizentes com as necessidades específicas de cada serviço de TI.

Art. 20. O descumprimento desta instrução normativa será registrado, em sistema informatizado, como incidente de segurança da informação e comunicado ao Comitê Executivo de TI para apuração e adoção das providências necessárias.

Art. 21. Com o objetivo de sistematizar a aplicação deste normativo, fica definido o cronograma constante do Anexo.

Art. 22. Os casos omissos serão resolvidos pelo(a) titular da Secretaria de Tecnologia e Inovação.

Art. 23. Esta instrução normativa entra em vigor na data de sua publicação.

EDUARDO S. TOLEDO

ANEXO

Etapa	***Prazo****
Elaboração dos modelos de planejamento dos roteiros técnicos e de execução das rotinas de cópias de segurança e restauração	*Até 2 (dois) meses*
Revisão da lista de ativos de informação e classificação quanto à sua criticidade (críticos e não críticos)	*Até 4 (quatro) meses*
Elaboração dos planos de cópias de segurança dos sistemas críticos	*Até 6 (seis) meses*
Implementação dos planos de cópias de segurança dos sistemas críticos	*Até 8 (oito) meses*
Elaboração dos planos de cópias de segurança dos sistemas não críticos	*Até 10 (dez) meses*
Implementação dos planos de cópias de segurança dos sistemas não críticos	*Até 12 (doze) meses*
**Os prazos iniciam-se a contar da publicação desta IN.*	

Publicado no DJE/STF em 10/7/2024.