Art. 4º Para a distribuição equânime dos trabalhos aos membros da comissão deverá ser levada em consideração não apenas a quantidade de processos distribuídos, mas também o montante de recursos distribuídos entre as zonas eleitorais.

Parágrafo único. Caso seja constatada insatisfatória a produtividade de algum membro da comissão, caberá ao presidente notificar o servidor para que apresente esclarecimentos a respeito da situação e, se for o caso, solicitar à Diretoria-Geral a substituição do membro.

Art. 5º Esta portaria entrará em vigor na data de sua publicação, revogando-se a Portaria DG nº 217 /2022.

Goiânia, 4 de novembro de 2022.

Wilson Gamboge Júnior

Diretor-Geral

ANEXO

PORTARIA Nº 221/2022-DG

Servidor	Lotação
Antônio Gomes de Aguiar - Presidente	SAO/COFI
Adriano Jorge Guimarães Lima - titular	COMSERVZON/055ZGO
Maria Sirene Carneiro Matos - titular	SAO/COFI
Maria de Lourdes Macedo de Andrade - titular	SAO/CEIN
Maximiano Braga Vianna de Oliveira - suplente	SAO/CEIN
Mylène Machado Martin Teixeira - titular	SGP/COPS
Frederico Antônio Ferreira - titular	INTEGRAZON/031ZGO
Marucio Machado da Silveira - primeiro suplente	INTEGRAZON/031ZGO
Auxiliadora de Salles Corrêa França - segundo suplente	INTEGRAZON/031ZGO

PORTARIA DG N°220/2022

Institui a Norma Corporativa de Cópias de Segurança e Restauração de dados (NCCSR) no âmbito do Tribunal Regional Eleitoral de Goiás.

O DIRETOR-GERAL DA SECRETARIA DO TRIBUNAL REGIONAL ELEITORAL DE GOIÁS, no uso das atribuições conferidas pelo disposto no artigo 46, inciso XVI, da Resolução TRE/GO nº 275, de 18 de dezembro de 2017, e alterações posteriores,

CONSIDERANDO a necessidade de otimizar a qualidade dos serviços de tecnologia da informação (TI), bem como de alinhá-los aos objetivos de negócio deste Tribunal, visando aumentar a satisfação dos usuários;

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 o disposto na Resolução CNJ n° 396, de 07 de junho de 2021, que instituiu a Estratégia Nacional de Segurança da Informação e Cibernética do Poder Judiciário (ENSEC-PJ) no âmbito dos órgãos do Poder Judiciário;

CONSIDERANDO o disposto na Resolução TSE n° 23.644, de 1º de julho de 2021, que dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

CONSIDERANDO o disposto na Portaria TSE nº 457, de 13 de julho de 2021, que institui norma de gerenciamento de backup e restauração de dados relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral;

CONSIDERANDO o disposto na Resolução TRE-GO n° 355, de 10 de novembro de 2021, que adotou a Política de Segurança da Informação (PSI) da Justiça Eleitoral no âmbito do TRE-GO;

CONSIDERANDO as orientações sobre técnicas de segurança em tecnologia da informação, regulamentadas nas normas NBR ISO/IEC 17799 e 27001;
CONSIDERANDO a contínua preocupação com a qualidade e celeridade na prestação jurisdicional à sociedade;
CONSIDERANDO a instrução processual do SEI 21.0.000008481-3,
RESOLVE:
DISPOSIÇÕES INICIAIS
Art. 1° Instituir a Norma Corporativa de Cópias de Segurança (Backup) e Restauração (Restore) de dados (NCCSR) relativa à Política de Segurança da Informação do Tribunal Regional Eleitoral de Goiás, com objetivo de estabelecer diretrizes para o processo de cópia e armazenamento dos dados sob a guarda da Secretaria de Tecnologia da Informação STI, a fim de garantir a segurança, integridade e disponibilidade.
Art. 2° As disposições deste ato aplicam-se ao gerenciamento dos serviços de Cópias de Segurança (Backup) e Restauração (Restore) de dados do Tribunal.
DOS CONCEITOS E DEFINIÇÕES
Art. 3° Para os efeitos desta Norma Corporativa de Cópias de Segurança (Backup) e Restauração (Restore) de dados - NCCSR, aplicam-se os seguintes termos e definições:
I - Usuários: magistrados, servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, e, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados e outras pessoas que se encontrem a serviço da Justiça Eleitoral, utilizando, em caráter temporário, os recursos tecnológicos deste Tribunal;
II - Cópia de segurança (Backup): cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos dados originais;
III - Restauração de dados (Restore): recuperação dos dados existentes em backup;
IV - Backup full (completo): modalidade de backup na qual todos os dados, de um determinado serviço, são copiados;
V - Backup incremental: modalidade de backup na qual somente são copiados os dados modificados, desde o último backup;
VI - Técnico de backup: servidores das unidades responsáveis pelos procedimentos de configuração, execução, monitoramento e testes dos procedimentos de backup e restore;
VII - Mídia: meio físico no qual efetivamente se armazena o backup;
VIII - Retenção: período de tempo em que o conteúdo da mídia de backup deve ser preservado;
IX - Gestor da informação: responsáveis pelas informações, nas áreas de negócio;
X - Serviço de TI: todo o processo de trabalho suportado por recursos informatizados;
XI - Serviços críticos: qualquer sistema cuja indisponibilidade cause prejuízo a realização dos serviços essenciais do Tribunal.
XII - Datacenter: ambiente projetado para concentrar computadores servidores, equipamentos de processamento e armazenamento de dados, ativos de rede e, por isso, considerado o sistema nervoso de empresas e organizações que utilizam sistemas informatizados.
DOS OBJETIVOS
Art. 4° São objetivos da Norma Corporativa de Cópias de Segurança e Restauração de dados - NCCSR:
I - definir um conjunto de padrões de segurança destinados à realização de cópia e restauração de dados armazenados nos datacenters deste Tribunal;
II - estabelecer diretrizes para a realização de cópias de segurança e restauração de dados;
III - definir os padrões para armazenagem, conservação e descarte das mídias utilizadas para cópias de segurança;
IV - estabelecer critérios para a solicitação da restauração de dados.

DA CÓPIA DE SEGURANÇA

Art. 5° A norma de cópia de dados compreenderá a realização de backups diários, semanais, mensais e anuais dos sistemas e bases de dados existentes no ambiente de produção, conforme necessidades identificadas por intermédio das demandas de cópia de segurança, de modo a salvaguardar as informações corporativas deste Tribunal, em caso de eventual perda.

DO PERÍODO DE RETENÇÃO DAS MÍDIAS

Art. 6° As mídias terão seus períodos de retenção conforme o tipo de backup utilizado:

I - as mídias utilizadas para os backups diários devem ser retidas por 30 (trinta) dias;

II - as mídias utilizadas para os backups semanais devem ser retidas por 04 (quatro) semanas;

III - as mídias utilizadas para os backups mensais devem ser retidas por 01 (um) ano;

IV - as mídias utilizadas para os backups anuais devem ser retidas por 05 (cinco) anos.

§ 1° Em casos especiais, o Gestor da Informação poderá definir, em conjunto com os técnicos de backup, prazos diferenciados para retenção das mídias.

§ 2° Expirado o prazo de retenção dos dados armazenados, a mídia poderá ser reutilizada.

DA GUARDA DAS MÍDIAS

Art. 7° As mídias utilizadas para a realização de cópias de segurança deverão ser armazenadas em locais seguros, com acesso controlado pela Secretaria de Tecnologia da Informação (STI) e distribuídas entre endereços físicos distintos, de tal forma a garantir a restauração das informações corporativas em outro local, no caso de incidente grave que provoque total indisponibilidade do ambiente de produção.

Art. 8° As mídias devem ser etiquetadas com as seguintes informações:

I - descrição dos dados nelas armazenados;

II - tipo de backup realizado;

III - mês e ano da cópia;

IV - prazo de retenção.

DO DESCARTE DAS MÍDIAS

Art. 9° As mídias a serem descartadas devido à obsolescência tecnológica ou defeito irrecuperável deverão ser eliminadas de forma segura e protegida, por meio de trituração ou quebra dos dispositivos utilizados. Caso esse trabalho venha a ser feito por empresa terceirizada, o processo deve ser integralmente acompanhado por um servidor da Secretaria de Tecnologia da informação (STI).

DAS ATRIBUIÇÕES DO TÉCNICO DE BACKUP

Art. 10. É atribuição do técnico de backup:

I - providenciar a criação e manutenção dos backups;

II - configurar a ferramenta de backup;

III - manter as mídias preservadas, funcionais e seguras;

IV - efetuar testes de backup e auxiliar nos procedimentos de restore, tanto no ambiente originário quanto no de replicação;

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

VI - restaurar os backups em caso de necessidade;

VII - gerenciar mensagens e logs diários dos backups;

VIII - comunicar ao administrador de recurso os erros e as ocorrências nos backups;

IX - propor modificações para o aperfeiçoamento da norma de backup.

Art. 11. O técnico de backup deverá respeitar as janelas para execução das cópias, inclusive realizando previsão para a ampliação da capacidade dos dispositivos envolvidos no armazenamento.

DA RESTAURAÇÃO DE CÓPIA DE SEGURANÇA

Art. 12. A restauração da cópia de segurança deverá ser realizada somente nas seguintes situações:

I - para recompor a integridade do ambiente afetado após um incidente, desastre ou falha de uma mídia de armazenamento;

II - para atender a solicitação formal do proprietário do ativo de informação à unidade responsável pelo gerenciamento de cópia de segurança;

III - para realização de testes de restauração periódicos;

IV - para realização de auditorias e investigações legais e forenses.

Art. 13. A restauração da cópia de segurança de sistemas operacionais e de informações deverá ser realizada, preferencialmente, em máquina isolada do ambiente de produção.

Parágrafo único. Caso o sistema de que trata o caput tenha sido comprometido é obrigatória a revisão de todas as configurações visando garantir o retorno correto do serviço.

Art. 14. As solicitações de restauração de dados deverão ser abertas formalmente por meio de ferramentas de abertura de chamados e/ou formulário próprio que deverá conter:

I - os nomes dos arquivos e pastas que deverão ser recuperados e, principalmente, a data do arquivo que se pretende ter acesso;

II - o nome do sistema informatizado, a data, o horário e quais os dados mantidos pelo respectivo banco de dados deverão ser recuperados.

Parágrafo único. Em caso de indisponibilidade de dados ou sistemas críticos em ambiente de produção, a solicitação de restauração de arquivos poderá ser feita por meio de mensagem eletrônica (e-mail), aplicativo de mensagem instantânea ou qualquer outro recurso que possibilite a verificação posterior da solicitação, desde que feita pelo titular da unidade demandante, para o titular da unidade que administra o serviço de backup.

Art. 15. O proprietário do ativo de informação deverá validar a integridade das informações restauradas antes da sua utilização.

Art. 16. Após a restauração da cópia de segurança, deverão ser analisados os registros de eventos (logs) gerados pela solução de backup, para garantir o resultado da operação ou para a adoção de providências cabíveis, no caso de eventuais erros.

Art. 17. Deverão ser estabelecidos procedimentos para testes periódicos, por amostragem, de restauração da cópia de segurança com o intuito de assegurar a integridade dos dados gravados.

§1º A Secretaria de Tecnologia da Informação providenciará a edição de Procedimentos de Segurança da Informação relacionados a Testes de Restaraução de Dados, os quais deverão ser disponibilizados na página da unidade na intranet.

§2º As informações restauradas devem ser excluídas após a realização dos testes de restauração da cópia de segurança.

DISPOSIÇÕES FINAIS

Art. 18. A execução de quaisquer procedimentos que impliquem em riscos de funcionamento nos ativos de informação deverá ser precedida da realização de backup.

Art. 19. Fica estabelecido o prazo de 06 (seis) meses para a adoção das providências necessárias à implementação do disposto nesta norma.

Art. 20. A revisão desta norma de backup ocorrerá sempre que se fizer necessário ou conveniente para o Tribunal, não excedendo o período máximo de 3 (três) anos.

Art. 21. Os casos omissos serão resolvidos pela Diretoria-Geral ou unidade responsável pela Segurança da Informação, que porventura venha ser criada no âmbito deste Tribunal.

Art. 22. Esta portaria entrará em vigor na data de sua publicação.

Wilson Gamboge Júnior

Diretor-Geral