Tribunal Regional Eleitoral de Goiás

Secretaria de Gestão da Informação

Seção de Jurisprudência e Legislação

PORTARIA Nº 146/2024 - DG

Institui a Norma Corporativa de Gerenciamento de Cópias de Segurança e Restauração de dados 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 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 27001 e 27002;

CONSIDERANDO as boas práticas em segurança da informação previstas no modelo CIS Controls V.8;

CONSIDERANDO a Portaria DG/TSE nº 444, de 08 de julho de 2021, que dispõe sobre a instituição da norma de termos e definições relativa à Política de Segurança da Informação do Tribunal Superior Eleitoral;

CONSIDERANDO a contínua preocupação com a qualidade e celeridade na prestação jurisdicional à sociedade;

CONSIDERANDO a instrução processual do SEI 23.0.000016929-3,

RESOLVE:

DISPOSIÇÕES INICIAIS

Art. 1° Instituir a Norma Corporativa de Gerenciamento de Cópias de Segurança (Backup) e Restauração (Restore) de dados (NCGCSR) 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 dos dados custodiados pelo Tribunal Regional Eleitoral de Goiás.

Art. 2° As disposições deste ato aplicam-se ao gerenciamento dos serviços de Cópias de Segurança (Backup) e Restauração (Restore) de dados do Tribunal.

Art. 3° Não estão cobertos por esta norma os dados armazenados localmente em microcomputadores, notebooks, dispositivos móveis ou outros dispositivos de uso individual.

Art. 4° A salvaguarda e a recuperação dos dados de sistemas de informação custodiados por outras entidades, públicas ou privadas, utilizados pelo TRE-GO, deverão estar estabelecidas em cláusulas contratuais.

DOS CONCEITOS E DEFINIÇÕES

Art. 5° Para os efeitos desta Norma Corporativa de Gerenciamento de Cópias de Segurança (Backup) e Restauração (Restore) de dados - NCGCSR, aplicam-se, como referência, a norma de termos e definições relativa à Portaria DG/TSE nº 444/2021, bem como 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): conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação;

III - Restauração de dados (Restore): conjunto de procedimentos que permitem a recuperação dos dados existentes em backup;

IV - Backup full (completo): modalidade de backup na qual todos os dados a serem salvaguardados, de um determinado serviço, são copiados integralmente;

V - Backup incremental: modalidade de backup na qual são copiados apenas os dados modificados, desde o último backup completo realizado;

VI - Backup diferencial: é um tipo de estratégia de cópia de segurança de dados que envolve a cópia de todos os dados que foram alterados desde o último backup completo. Ele difere do backup incremental, que copia apenas os dados alterados desde o último backup, seja ele completo ou diferencial.

VII - Técnico de backup: servidores das unidades responsáveis pelos procedimentos de configuração, execução, monitoramento e testes dos procedimentos de backup e restore;

VIII - Mídia: meio físico no qual efetivamente se armazena o backup;

IX - Retenção: período de tempo em que o conteúdo da mídia de backup deve ser salvaguardado e estar apto à restauração;

X - Gestor da informação: responsáveis pelas informações, nas áreas de negócio;

XI - Serviço de TI: todo o processo de trabalho suportado por recursos informatizados;

XII - Sistemas críticos: qualquer sistema cuja indisponibilidade cause prejuízo à realização dos serviços essenciais do Tribunal.

XIII - 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;

XIV - Descarte: eliminação correta dos dados, unidades de armazenamento e acervos digitais;

XV - Janela de backup: período de tempo durante o qual, cópias de segurança sob execução agendada ou manual poderão ser executadas;

XVI - Rotina de backup: procedimento utilizado para se realizar um backup;

XVII - Unidade de armazenamento de backup: dispositivo para armazenamento de dados em suporte digital com características específicas para retenção de cópia de segurança de dados digitais.

XVIII - LGPD: Lei Geral de Proteção de Dados que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

DOS OBJETIVOS

Art. 6° São objetivos da Norma Corporativa de Gerenciamento de Cópias de

Segurança e Restauração de dados (NCGCSR):

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.

DOS PRINCÍPIOS GERAIS

Art. 7° As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando um incidente ocasionar indisponibilidade de serviços de TI.

Art. 8° As rotinas de backup devem possuir requisitos mínimos, diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado, dando prioridade aos serviços de TI críticos da organização.

Art. 9° As tecnologias utilizadas para a realização do backup devem cumprir os requisitos necessários para preservar a integridade, a confidencialidade, a disponibilidade e a irretratabilidade das informações.

Art. 10. Os dados abarcados por esta norma deverão ser definidos em um Plano de Gerenciamento de Backup e Restauração de Dados, a ser definido pela área técnica responsável, refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação e de proteção de dados pessoais envolvidos.

Parágrafo único. O Plano de Gerenciamento de Backup e Restauração de Dados deve ser aprovado pelo Comitê de Governança de Tecnologia da Informação e Comunicação - CGTIC.

Art. 11. A solicitação e validação de salvaguarda dos dados referentes aos serviços de TI deve ser realizada pelos responsáveis técnicos dos serviços de TI.

Art. 12. A infraestrutura de backup não pode utilizar os mesmos controladores de domínio do restante da infraestrutura e deve ficar protegida por firewall de rede.

Art. 13. O Plano de Gerenciamento de Backup e Restauração de Dados deve explicitar, no mínimo, os seguintes requisitos técnicos:

I - escopo (dados a serem salvaguardados/restaurados);

II - tipo (completo/total, incremental e diferencial);

III - frequência (diária, semanal, mensal e anual);

IV - tempo de retenção;

V - unidade de armazenamento;

VI - janela de backup;

VII - local de armazenamento das mídias;

VIII - periodicidade de teste de restauração do backup;

Art. 14. A documentação do Plano de Gerenciamento de Backup e Restauração de Dados e das rotinas de backup deve ser armazenada em local seguro e com acesso restrito à seção responsável pelo gerenciamento de backup.

Art. 15. Os backups devem estar em conformidade com a legislação vigente, em especial ao que compete à LGPD.

Art. 16. Os backups devem ser armazenados de forma criptografada, considerando as melhores práticas de mercado e normas vigentes.

Parágrafo único. Deverão ser implementados controles criptográficos nos arquivos que trafegam na rede da organização ou na Internet (data in transit).

DA CÓPIA DE SEGURANÇA

Art. 17. A Norma Corporativa de Gerenciamento de Cópias de Segurança e Restauração 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. 18. 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 45 (quarenta e cinco) dias;

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.

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

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

DA GUARDA DAS MÍDIAS

Art. 19. 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 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. 20. 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 USO DA REDE

Art. 21. Deverá ser considerado, para a execução das rotinas de backup, o seu impacto sobre o desempenho da rede computacional, garantindo que o tráfego necessário para tal não cause a indisponibilidade dos demais sistemas e serviços de TI.

Parágrafo único. O backup das informações armazenadas nos servidores da rede corporativa deve ser realizado em período de baixa utilização de seus recursos computacionais, preferencialmente fora do horário de expediente ordinário das unidades da Secretaria do Tribunal.

DAS UNIDADES DE ARMAZENAMENTO DE BACKUPS

Art. 22. A escolha das unidades de armazenamento utilizadas na salvaguarda dos dados deverá atender as seguintes características dos dados resguardados:

I - a criticidade;

II - o tempo de retenção;

III - a probabilidade de necessidade de restauração;

IV - o tempo esperado para restauração;

V - o custo de aquisição da unidade de armazenamento de backup; e

VI - a vida útil da unidade de armazenamento de backup.

Art. 23. O backup dos dados definidos como críticos, deve ser provido em 2 (duas) mídias distintas, com conteúdo idêntico, para armazenamento em 2 (dois) locais diferentes, observado o seguinte:

I - uma cópia de segurança deve ser armazenada de forma a permitir sua rápida localização e recuperação;

II - outra cópia de segurança deve ser armazenada em local externo à sede do Tribunal.

Parágrafo único. Uma cópia de segurança deve ser, preferencialmente, armazenada em uma localização que não seja endereçável de forma contínua por meio de chamadas do sistema operacional.

Art. 24. Os locais de armazenamento das mídias da cópia de segurança devem ter mecanismos de segurança, considerando, minimamente, os seguintes elementos:

I - o acesso ao local deve ser restrito e monitorado;

II - o acesso ao local deve ser registrado em logs contendo minimamente a identificação do usuário e informações de data e hora de entrada e saída;

III - o local deve possuir controles de prevenção, detecção e combate a incêndio.

Art. 25. Os locais externos de armazenamento da cópia de segurança devem possuir requisitos de segurança adequados e separados do ambiente de armazenagem da cópia principal, de forma que não permaneçam expostos aos mesmos riscos de desastres que a localidade de origem dos dados.

DO DESCARTE DAS MÍDIAS

Art. 26. As mídias a serem descartadas devido a obsolescência tecnológica ou defeito irrecuperável deverão ser eliminadas de forma segura e protegida, por meio de trituração ou quebra dos dispositivos utilizados, respeitando os procedimentos definidos como sustentáveis e ambientalmente corretos. 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).

Art. 27. Nos casos de substituição da solução de backup (hardware ou software), as informações contidas nas mídias da antiga solução devem ser transferidas, em sua totalidade, para mídias compatíveis com a nova solução.

Parágrafo único. A solução de backup obsoleta somente poderá ser desativada após a certificação de que todas as informações foram transferidas para a nova solução implementada.

DOS TESTES DE BACKUP

Art. 28. Os backups devem ser testados periodicamente, com o objetivo de garantir a sua confiabilidade e a integridade dos dados salvaguardados.

Art. 29. Os testes de restauração dos backups devem ser realizados em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, com configurações similares a estes, observados os recursos humanos e

tecnológicos disponíveis.

Art. 30. A periodicidade, a abrangência, os procedimentos e as rotinas inerentes aos testes de backup devem ser devidamente registrados no Plano de Gerenciamento de Backup e Restauração de Dados.

DAS ATRIBUIÇÕES

Art. 31. Das atribuições da área técnica responsável pelo backup:

I - providenciar a criação e manutenção dos backups;

II - configurar a solução de backup;

III - manter as mídias preservadas, funcionais e seguras;

IV - efetuar testes de backup e auxiliar nos procedimentos de restore, tanto do ambiente originário quanto no de replicação (caso exista);

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

VI - restaurar os backups em caso de necessidade;

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

VIII - propor modificações para o aperfeiçoamento da norma de backup;

IX - planejar os recursos necessários para implantar os requisitos desta norma e do Plano de Gerenciamento de Backup e Restauração de Dados;

X - tomar medidas preventivas para evitar falhas.

Art. 32. 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. 33. 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 responsável pela informação à unidade responsável pelo gerenciamento de cópia de segurança;

III - para realização de testes periódicos de restauração;

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

Art. 34. 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 os sistemas de que trata o caput tenham sido comprometidos é obrigatória a revisão de todas as configurações visando garantir o retorno correto do serviço.

Art. 35. 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 que 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. 36. O responsável pela informação deverá validar a integridade das informações restauradas antes da sua utilização.

Art. 37. 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. 38. 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 do Procedimento de Testes de Restauração de Dados, o qual deverá ser disponibilizado na intranet.

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

DISPOSIÇÕES FINAIS

Art. 39. A execução de quaisquer procedimentos que impliquem em riscos de funcionamento nos ativos de informação deverá ser precedida da realização de backup.

Art. 40. Deverão ser utilizadas soluções de backup e restauração de dados adequadas e especializadas, preferencialmente capazes de atuar de maneira automatizada.

Art. 41. Fica estabelecido o prazo de 06 (seis) meses para a adoção das providências necessárias à implementação do disposto nesta norma.

Art. 42. 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. 43. Os casos omissos serão resolvidos pelo Comitê Gestor de Segurança da Informação – CGSI.

Art. 44. Fica revogada a Portaria DG nº 220/2022.

Art. 45. Esta portaria entrará em vigor na data de sua publicação.

Leonardo Sapiência Santos

Diretor-Geral