CONSELHO SUPERIOR DA JUSTIÇA DO TRABALHO
SECRETARIA JURÍDICA, PROCESSUAL E DE APOIO ÀS SESSÕES

RESOLUÇÃO CSJT N.º 434, DE 06 DE MARÇO DE 2026.

Institui a Política de *Backup* no âmbito da Justiça do Trabalho de primeiro e segundo graus.

O **CONSELHO SUPERIOR DA JUSTIÇA DO TRABALHO**, em Sessão Ordinária Virtual com início à 0 (zero) hora do dia 27/02/2026 e encerramento às 23 horas e 59 minutos do dia 06/03/2026, sob a presidência do Exmo. Conselheiro Luiz Philippe Vieira de Mello Filho, com a presença dos Exmos. Conselheiros Guilherme Augusto Caputo Bastos, José Roberto Freire Pimenta, Maria Helena Mallmann, Breno Medeiros, Alexandre Luiz Ramos, Marcia Andrea Farias da Silva, Ricardo Hofmeister de Almeida Martins Costa, Jorge Álvaro Marques Guedes, Eugênio José Cesário Rosa, Denise Alves Horta e Manuela Hermes de Lima, e da Exma. Vice-Procuradora-Geral do Trabalho, Dr.ª Teresa Cristina D'Almeida Basteiro,

considerando o que dispõe a Lei n.º 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD);

considerando a Resolução n.º 363, de 12 de janeiro de 2021, do Conselho Nacional de Justiça (CNJ), que estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais;

considerando o disposto na Resolução CNJ n.º 396, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

considerando a importância de estabelecer objetivos, princípios e diretrizes de Segurança da Informação alinhados às recomendações constantes da norma da Associação Brasileira de Normas Técnicas (ABNT) NBR ISO/IEC 27001:2022, que trata da segurança da informação;

considerando a Instrução Normativa n.º 5, de 30 de agosto de 2021,

Fonte: Diário Eletrônico da Justiça do Trabalho: caderno administrativo [do] Conselho Superior da Justiça do Trabalho, Brasília, DF, n. 4440, p. 2-8, 25 mar. 2026.

do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal;

considerando que a continuidade dos serviços fornecidos pela Justiça do Trabalho para dar suporte a suas operações depende de sua capacidade de resistir a perdas de dados imprevistas e outros incidentes de segurança graves;

considerando que a gestão de cópias de segurança e respectivos procedimentos são pré-requisitos para permitir posterior recuperação de informações e serviços críticos da Justiça do Trabalho;

considerando a necessidade de estabelecer diretrizes gerais e responsabilidades referentes a proteção de dados, com vistas a garantir a integridade, a confidencialidade e a disponibilidade das informações;

considerando que a recuperação de dados é condição indiscutível para assegurar a resposta a incidentes graves e para minimizar perdas de operações críticas e danos à imagem da Justiça do Trabalho; e

Considerando a decisão proferida nos autos do Processo CSJT-Ato-1000992-40.2025.5.90.0000,

RESOLVE:

Capítulo I
Das Disposições Gerais

Art. 1º Fica instituída a Política de *Backup* no âmbito da Justiça do Trabalho de primeiro e segundo graus com vistas a assegurar a resiliência e a durabilidade dos dados, por meio de soluções de cópia de segurança e recuperação, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação dos procedimentos de cópia, armazenamento seguro e recuperação de dados.

Art. 2º Para fins do disposto nesta Resolução, considera-se:

I - Administrador de *Backup*: profissional responsável por gerenciar e implementar o sistema de *backup* de dados de uma organização; seu objetivo principal é garantir que todos os dados críticos da empresa sejam copiados e armazenados de forma segura, para que possam ser restaurados rapidamente em caso de perda ou falha;

II - Administrador de Recurso: responsável pela operação dos serviços ou equipamentos;

III - ambiente de *backup:* infraestrutura física e lógica que permite armazenar e gerenciar os *backup*s de dados; inclui *hardware, software* e rede;

IV - *backup:* cópia de segurança dos dados armazenada nos equipamentos e nos servidores utilizados para prover os serviços tecnológicos;

V - *backup* completo: modalidade de *backup* em que todos os dados a serem salvaguardados são copiados integralmente (cópia de segurança completa) para uma unidade de armazenamento, independentemente de terem sido ou não alterados desde o último *backup*;

VI - *backup* completo virtual ou incremental "para sempre": modalidade de *backup* que consolida o *backup* completo anterior por meio dos *backup*s incrementais baseados nele, sem necessidade de novo *backup* completo;

VII - *backup* diferencial: modalidade de *backup* em que são salvaguardados apenas dados novos ou modificados desde o último *backup* completo efetuado;

VIII - *backup* incremental: modalidade de *backup* em que são salvaguardados apenas os dados novos ou modificados desde o último *backup* de qualquer modalidade efetuada;

IX - *Business Impact Analysis* (BIA) – Análise de Impacto nos Negócios: etapa do processo de gestão de continuidade de negócio que tem por objetivo determinar os serviços críticos, os requisitos e as prioridades da continuidade do negócio, bem como os impactos toleráveis pela organização em face de uma disrupção;

X - compartimento: segregação lógica dentro de uma conta; utilizada por alguns provedores de nuvem;

XI - conta de provedor: conjunto lógico em que um usuário cria ambientes computacionais e os gerencia no provedor de nuvem; em alguns provedores, também pode ser conhecida como *tenancy*;

XII - criticidade do dado: grau de importância dos dados para a continuidade das atividades e dos serviços da organização;

XIII - dado crítico: na ausência de normatização que classifique a criticidade dos dados, para a aplicação desta Política somente os dados do Sistema Processo Judicial Eletrônico (PJe) serão entendidos como críticos na Justiça do Trabalho;

XIV - dado desidratado: dado que utiliza ponteiros e depende de fonte primária;

XV - dados estruturados: dados organizados em formato predefinido e compreensível para computadores; essa organização se baseia em esquema ou modelo que define a relação entre os elementos dos dados, tais como tipo de dado, tamanho do campo e regras de validação; exemplos: banco de dados como Oracle, PostgreSQL, SQL Server;

XVI - dado hidratado: dado que não utiliza ponteiros e não depende da fonte primária para sua utilização;

XVII - dado não crítico: na ausência de normatização que classifique a criticidade dos dados, excluindo-se os dados do Sistema Processo Judicial Eletrônico (PJe), todos os demais serão entendidos como não críticos para a aplicação desta Política;

XVIII - dados não estruturados: não apresentam formato predefinido ou organização rígida; consistem em informações textuais, imagens, vídeos, áudios e outros formatos que não se encaixam facilmente em modelos tradicionais de bancos de dados; exemplos: servidor de arquivos, partição de máquinas virtuais, correio eletrônico, *data lakes*;

XIX - *data lake*: coleção de dados não estruturados ou semiestruturados;

XX - *datacenter on premises*: *datacenter* fora da nuvem pública, localizado em ambientes seguros do órgão;

XXI - *datacenter* soberano: aquele que garante a soberania dos dados, uma vez que são mantidos integralmente dentro das fronteiras do País, sob a custódia do Governo Federal ou do órgão; isso elimina riscos associados à transferência internacional de dados e assegura total conformidade com as regulamentações nacionais; XXII - descarte: eliminação correta de dados, documentos, unidades de armazenamento e acervos digitais;

XXIII - disponibilidade: garantia de que o dado esteja acessível e utilizável sob demanda de pessoa física ou determinado serviço de TI, órgão ou entidade devidamente autorizados;

XXIV - *Data Recovery Time Objective* (DRTO) – Tempo de Recuperação Alvo: métrica que determina o tempo necessário para restaurar o dado após um período de inatividade com interrupção mínima das operações;

XXV - Gestor Negocial: agente público formalmente responsável pela administração do serviço e pelas informações produzidas no respectivo processo de trabalho;

XXVI - janela de *backup*: período durante o qual cópias de segurança sob execução agendada ou manual poderão ser executadas;

XXVII - mídia: meio físico ou virtual no qual efetivamente armazenam-se os dados de um *backup*;

XXVIII - *Maximum Tolerable Period of Disruption* (MTPD) – Período Máximo de Interrupção Tolerável: tempo máximo que a organização aceita para retorno dos serviços após um evento de desastre;

XXIX - periodicidade de *backup*: frequência em que ocorrerá o *backup*;

XXX - Plano de *Backup*: documento ou conjunto de diretrizes que descrevem como os *backups* serão realizados; detalha procedimentos, políticas e práticas que serão adotados para garantir a integridade dos dados e a capacidade de recuperação em caso de perda;

XXXI - processo de *backup*: implementação prática do Plano de *Backup*; execução real das tarefas e dos procedimentos descritos no Plano para realizar os *backup*s de forma eficaz e regular;

XXXII - recuperação dos dados: processo de recuperação dos dados danificados, corrompidos ou inacessíveis contidos em mídias de armazenamento de produção por meio da restauração de cópias de segurança;

XXXIII - recurso de proteção de imutabilidade: característica concedida ao dado, que impede sua alteração ou deleção por qualquer conta privilegiada ou ativo até que a data configurada seja alcançada;

XXXIV - Região: geolocalização sujeita a um evento único que gera indisponibilidade (natural ou não); locais que trabalham independentemente um do outro, uma vez que, em razão da distância entre os *datacenters*, não é possível a integração síncrona dos equipamentos;

XXXV - réplica: cópia, em local ou dispositivo distinto, do dado hidratado; geralmente é configurada para ocorrer em tempo real;

XXXVI - *restore:* restauração do dado copiado;

XXXVII - *Recovery Point Objective Data* (RPO) – Ponto de Recuperação Alvo: métrica que determina o período máximo de perda de dados que uma organização está disposta a aceitar após um incidente ou interrupção;

XXXVIII - solução de *backup*: conjunto de ferramentas e processos que permitem copiar e armazenar dados de forma segura, para que seja possível restaurá-los em caso de perda ou falha;

XXXIX - *storage*: equipamento que disponibiliza solução de armazenamento de dados em discos sólidos ou rotacionais;

XL - supervisor de virtualização, também chamado de *hypervisor: software ou firmware* que opera diretamente no *hardware* de um servidor, permitindo a criação e a gestão de máquinas virtuais (VMs); atua como camada de abstração entre o *hardware* físico e o *software* de um sistema operacional, permitindo que vários sistemas operacionais guest sejam executados simultaneamente em um único host; para efeito deste documento, deve ser considerado apenas o tipo que executa diretamente no *hardware*, diferentemente de plataformas de gerenciamento centralizadas que administram e orquestram múltiplos servidores e *hypervisors*, mas não operam diretamente no *hardware*;

XLI - tempo de retenção: tempo em que o *backup* permanecerá disponível para eventual restauração;

XLII - unidade de armazenamento de *backup*: unidade de armazenamento com características específicas para retenção de cópia de segurança de dados digitais;

XLIII - Unidade Gestora de Segurança da Informação: departamento ou equipe dentro de uma organização responsável por gerenciar e implementar o programa de segurança da informação da organização; e

XLIV - Zona de Disponibilidade ou Domínio de Disponibilidade: *datacenter* ou conjunto de *datacenters* dentro de uma mesma Região, que pode conter uma ou mais Zonas de Disponibilidade; funcionam como clusters geográficos, de forma que trabalham como *datacenter* único, apesar de hospedados em locais físicos distintos, situação em que a latência é mínima e há possibilidade de integração total entre os equipamentos.

Capítulo II
Do Escopo e da Abrangência

Art. 3º Esta Política abrange apenas *backup* e recuperação de dados.

§1º Informações armazenadas localmente nas estações de trabalho

não farão parte do escopo do *backup*.

§2º Não serão tratados os procedimentos de tomada de decisão em caso de evento que gere indisponibilidade de serviço que antecede o início da recuperação do dado.

§3º Não serão tratados nesta Política os procedimentos de restauração de serviços; os procedimentos que sucederem à recuperação dos dados devem ser tratados no Plano de Continuidade do órgão.

§4º Para efeitos desta Política, considera-se que as réplicas não são, em sua essência, ativos de *backup*, ainda que, quando implementadas, em geral figurem como primeiro recurso para garantia da disponibilidade.

§5º Mudanças executadas nos serviços de TIC que impliquem riscos de perda de dados somente deverão ser executadas após a realização de cópia de segurança de seus dados.

Art. 4º Os Tribunais Regionais do Trabalho deverão elaborar seu Plano de *Backup*, observando as diretrizes definidas nesta Política.

Capítulo III
Disposições Preliminares

Art. 5º A solicitação de *backup* dos dados deve ser realizada pelo gestor negocial, assessorado pelos responsáveis técnicos dos serviços de TI, e refletir os requisitos de negócio da organização, bem como os requisitos de segurança da informação envolvidos e a criticidade da informação para a continuidade da operação da organização.

§1º Para a inclusão de novo serviço a ser protegido, deverão ser fornecidas, no mínimo, as seguintes informações ao Administrador do *Backup*:

I - localização dos dados;

II - volume dos dados que serão protegidos e taxa de crescimento estimada;

III - categoria de criticidade do dado (crítico ou não-crítico); e

IV - área responsável pelo serviço.

§2º A solicitação que trata o caput deverá ser realizada via Formulário de Solicitação de Proteção de Serviço e direcionada para o Administrador do *Backup*.

Art. 6º Os ativos envolvidos no processo de *backup* são considerados ativos críticos para a organização e deverão ter contrato de suporte e garantia vigentes.

Art. 7º Os Gestores Negociais deverão ter ciência do tempo de retenção ou da quantidade de versões estabelecidos para cada tipo de informação, e os Administradores de *Backup* deverão zelar pelo cumprimento das diretrizes estabelecidas nesta Resolução.

Art. 8º A solução de *backup* deverá ser orientada para a recuperação dos dados no menor tempo possível, em especial quando houver indisponibilidade de serviços que dependam da recuperação dos dados.

Art. 9º Na definição do DRTO, do RPO e do período de retenção dos dados de *backup*, é necessário certificar que as janelas de *backup* e de restauração para o pior cenário atendam aos tempos máximos disponíveis e aceitáveis para realização dos procedimentos.

Parágrafo único. O DRTO e o MTPD (período máximo de interrupção tolerável) não poderão superar os definidos no BIA (Análise de Impacto de Negócio) do órgão.

Art. 10. As falhas na execução dos procedimentos de *backup* deverão ser tratadas pelo Administrador do *Backup* ou, em caso de delegação, pelo Administrador do Recurso; persistindo a falha, o Gestor Negocial do recurso deverá ser notificado.

Art. 11. O ambiente de *backup* contendo o dado hidratado deverá ser hospedado em equipamentos físicos distintos do ambiente de produção e virtualmente isolados por camadas de redes (VLAN) distintas, supervisor de virtualização distinto e *hardware* distinto, de maneira a dificultar que um incidente que comprometa a produção também possa comprometer o ambiente de *backup*.

Art. 12. Devem existir, no mínimo, três cópias da informação:
I - dados originais;
II - cópia primária; e
III - cópia secundária.

§1º A cópia primária deve ficar armazenada em mídias diferentes dos dados originais, tais como: disco rotacional, disco de estado sólido, fita, armazenamento em *storage* objeto.

§2º A cópia secundária deve ficar armazenada em ambiente desconectado ou armazenada com recurso de proteção de imutabilidade e distante geograficamente do local de armazenagem dos dados originais; quando possível, a segunda cópia de segurança deve ser armazenada em outra região geográfica.

Art. 13. Em caso de hospedagem e tratamento dos dados de

produção em *datacenters* fora do território brasileiro, deverá haver obrigatoriamente ao menos uma cópia de segurança atualizada armazenada em *datacenters* soberanos.

Capítulo IV
Das Responsabilidades

Art. 14. A administração dos serviços de *backup* deverá seguir os requisitos de segurança definidos pela Unidade Gestora de Segurança da Informação do órgão. Parágrafo único. Caberá à Unidade Gestora da Segurança da Informação, auxiliada pelo Administrador de *Backup*:

I - verificar periodicamente as contas administrativas do ambiente de armazenamento dos dados digitais;

II - definir critérios de segurança para processos de geração e restauração de *backup*; e

III - definir requisitos de segurança para os testes de recuperação de dados.

Art. 15. A administração dos serviços de *backup* deverá ser responsabilidade de área específica designada pelo órgão.

§1º Caberá a cada instituição definir formalmente a área responsável pela administração dos serviços de *backup*, que terá as seguintes atribuições:

I - apoiar os gestores técnicos e negociais na definição dos prazos de retenção de dados;

II - auxiliar os gestores técnicos e negociais na definição da periodicidade das cópias de segurança;

III - garantir que as cópias de segurança sejam realizadas conforme definição dos gestores negociais;

IV - acompanhar a execução dos *backup*s, por meio das ferramentas de monitoramento disponíveis para esse objetivo;

V - configurar as soluções de *backup*;

VI - manter os ativos de armazenamento das cópias de segurança preservadas, funcionais e seguras;

VII - elaborar e validar a documentação de teste e restauração dos *backup*s; e

VIII - realizar periodicamente testes de restauração para averiguar os processos de *backup* e estabelecer melhorias.

§2º O Administrador de *Backup* será responsável pelo planejamento de soluções de *backup*, que contempla documentação, procedimentos de configuração, execução, monitoramento, testes de *backup*, definição de padrões, configurações e atendimento avançado de resolução de incidentes e problemas.

§3º É facultada a delegação de algumas das atividades de que trata o

§ 2º para o Administrador de Recursos, desde que autorizada pela Administração do Tribunal no Plano de *Backup*.

Art. 16. São atribuições dos Gestores Negociais e demandantes da solução:

I - solicitar, formalmente, a salvaguarda das informações geridas, auxiliado pelo gestor técnico, para recuperação de dados;

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

III - validar, negocialmente, o resultado dos testes de restauração dos *backup*s.

Capítulo V
Da Frequência e da Retenção dos Dados

Art. 17. A frequência das versões e o tempo de retenção dos dados têm por objetivo a consulta e a restauração nos casos de auditoria, erro humano, corrupção por criptografia indesejável dos dados realizada por ataque cibernético (*ransomware*) ou perda dos dados originais por dano físico no equipamento de armazenamento.

Art. 18. Os *backup*s dos dados de TIC da Justiça do Trabalho deverão ser realizados utilizando-se, no mínimo, os critérios definidos nas Tabelas 1 e 2 constantes do Anexo.

§1º O período de retenção e a quantidade de versões deverão ser implementados conforme o art. 12.

§2º Caso a modalidade "incremental para sempre" esteja disponível, não serão necessários novos *backup*s *full* e diferenciais.

§3º Caso a modalidade de proteção de dados contínua esteja disponível, ela poderá substituir as versões da modalidade incremental pelo período definido.

§4º Os dados críticos estruturados deverão ter o registro de suas operações (*logs*) protegidos na menor periodicidade disponível: por horário no caso tradicional, de 15 em 15 minutos no caso de ponteiros, ou com proteção contínua quando estiver disponível.

§5º No cenário de escassez de recursos, desde que aprovado pelo Presidente do tribunal, o tempo de retenção poderá ser reduzido de 5 (cinco) anos para até 6 (seis) meses, que é o tempo de retenção dos dados não críticos, hipótese em que os *backup*s anuais e dois semestrais são dispensados.

Art. 19. Para os dados de TIC, como máquinas virtuais e registros de operação de infraestrutura de TIC, a periodicidade será definida no Plano de *Backup*.

Art. 20. Os *backup*s contínuos ou realizados a cada hora protegem contra os eventos mais comuns de perda de dados: ataques de cibercrime, erro humano e *malware*.

Parágrafo único. As modalidades de *backup* a que se refere o caput deverão ser implementadas com ferramentas que permitam a restauração para qualquer RPO do período em até 15 minutos.

Art. 21. Quando os serviços de armazenamento dos dados, proteção e plataforma do ambiente em produção forem contratados como serviço em nuvem pública, o gestor deverá certificar-se de que os requisitos desta Política são empregados pelo provedor para o alcance da durabilidade e para o Acordo de Nível de Serviço contratados (SLA), hipótese em que será necessário manter uma cópia de segurança assíncrona em *datacenter* soberano, com objetivo de preservação da informação em caso de desastre da solução contratada.

§1º Para dados críticos, a periodicidade deverá ser de no máximo 1 (um) dia; e para dados não críticos, de uma semana.

§2º No caso de desligamento do usuário, de forma permanente ou temporária, o *backup* de seus arquivos institucionais de acesso privado deverá ser mantido por 30 (trinta) dias, período após o qual os arquivos poderão ser excluídos a qualquer tempo.

Capítulo VI
Dos Objetivos para Restauração e Recuperação dos Dados

Art. 22. O DRTO e o RPO desejados deverão ser definidos pela área de negócio e não deverão superar os parâmetros aceitáveis para cada Modalidade de Proteção em relação à criticidade do dado protegido definidos na Tabela 3 constante do Anexo.

Capítulo VII
Dos Testes de *Backup*

Art. 23. Os *backups* deverão ser testados periodicamente, a fim de garantir a confiabilidade e a integridade dos dados salvaguardados.

Art. 24. A periodicidade e a abrangência mínimas serão definidas como se segue:

I - sempre que estabelecido ou modificado um processo de *backup*, deverá ser realizado teste de restauração tão logo esteja disponível 1 (uma) versão de cada modalidade: incremental, diferencial e *full*;

II - no mínimo 1 (um) teste de recuperação trimestral para os dados críticos e 1 (um) teste de recuperação anual para os dados não críticos deverão ser realizados;

III - em caso de falha no teste de restauração, o processo deverá ser corrigido, e o *backup* deverá ser testado novamente.

Art. 25. Os testes de restauração dos *backups* poderão ser realizados por amostragem em serviços, equipamentos e servidores diferentes daqueles que atendem aos ambientes de produção.

Capítulo VIII
Do Armazenamento de *Backup*

Art. 26. Os *backup*s podem ser armazenados em:

I - disco rotacional ou dispositivo de disco sólido (SSD/NVME);

II - fitas magnéticas;

III - serviço de armazenamento de objetos (*object storage*); e

IV - serviço de armazenamento em bloco (*block storage*).

Parágrafo único. As cópias de segurança (*backups*) armazenadas fora do órgão deverão ser protegidas por meio de criptografia.

Art. 27. O descarte das mídias de *backup* inservíveis ou inutilizáveis deverá ser realizado mediante proposta apresentada pelo Administrador de *Backup* dirigida à unidade competente, em conformidade com a política de descarte vigente e os princípios de descarte ambientalmente sustentável.

Parágrafo único. As mídias a serem descartadas deverão ser apagadas de forma segura, destruídas ou desmagnetizadas, de modo a impedir o acesso indevido às informações por pessoas não autorizadas.

Art. 28. As unidades de armazenamento dos *backup*s deverão ser acondicionadas em locais apropriados, com controle de acesso e de fatores ambientais sensíveis, tais como umidade e temperatura.

Capítulo IX
Da Proteção de *Data Lakes*

Art. 29. O *backup* de dados não estruturados e semiestruturados armazenados em *data lakes* deverá ser de curta duração, sendo necessário apenas para reconstrução do ambiente em caso de falhas que se mostrem inviáveis de

serem sanadas.

Parágrafo único. Caso seja necessário restaurar dados em um período superior à retenção, o dado deverá ser reconstruído com base nos dados que originaram o *data lake*.

Capítulo X
Das Disposições Finais

Art. 30. Ato da Presidência complementará esta Resolução com planos de ação e com os respectivos procedimentos de implementação.

Art. 31. Os órgãos integrantes da Justiça do Trabalho de primeiro e segundo graus terão até 12 (doze) meses a contar do início da vigência desta Resolução para publicar seus Planos de *Backup*, com nomeação dos responsáveis pelo *backup*.

Art. 32. As evidências da realização dos testes de restauração deverão ser mantidas pelo órgão por até 5 (cinco) anos.

Art. 33. Esta Política deverá ser revisada bianualmente ou quando necessário.

Art. 34. Esta Resolução entra em vigor na data de sua publicação.

VIEIRA DE MELLO FILHO
Ministro Presidente do Conselho Superior da Justiça do Trabalho

Fonte: Diário Eletrônico da Justiça do Trabalho: caderno administrativo [do] Conselho Superior da Justiça do Trabalho, Brasília, DF, n. 4440, p. 2-8, 25 mar. 2026.

TABELAS

Tabela 1 – Periodicidade e Retenção para dados Críticos

Periodicidade	Retenção	Quant. de versões	Modalidade
Anual	5 anos	5	Full
Semestral	3 semestres	3	Full
Mensal	7 meses	6	Diferencial
Semanal	8 semanas	7	Diferencial
Diário	15 dias	15	Incremental
Horário	120 horas	120	Full e Incremental

Tabela 2 – Periodicidade e Retenção para dados Não Críticos

Periodicidade	Retenção	Quant. de versões	Modalidade
Semestral	1 semestre	1	Full
Mensal	7 meses	6	Diferencial
Diário	35 dias	35	Incremental

Tabela 3 - Parâmetros aceitáveis para Modalidade de Proteção vs Tipo de Dado

Modalidade vs Criticidade do Dado	Dado Crítico		Dado não Crítico	
	DRTO	RPO	DRTO	RPO
Proteção contínua ou por ponteiro	15 min.	15 min.	60 min.	60 min.
Disco	500GB/hora	60 min	300GB/hora	24 horas
Mídia Removível ou Nuvem Pública	300GB/hora	24 horas	150GB/hora	48 horas