ANEXO 4

NSI004 – Procedimentos de *backup* e recuperação de dados

(Incluído pela Portaria GP.TRT4 nº 8.605/2013 e alterado pelas Portarias GP.TRT4 nº 7.138/2014, 4.786/2020, 299/2022, 4.920/2022 e 4.095/2023)

1. Objetivo

1.1. Estabelecer diretrizes e padrões para os procedimentos de backup, testes e recuperação de dados realizados pela Secretaria de Tecnologia da Informação e Comunicações, no âmbito do Tribunal Regional do Trabalho da 4ª Região.

2. Motivações

2.1. Alinhamento às normas, regulamentações e melhores práticas, relacionadas à matéria.

2.2. Garantia de que a salvaguarda das informações seja realizada de forma otimizada, atendendo às necessidades do Tribunal.

2.3. Alinhar expectativas no processo de salvaguarda e *restore* dos dados armazenados em backup, visto que tal procedimento é uma das ações do processo de restauração/restabelecimento do ambiente. (incluído pela Portaria GP.TRT4 nº 299/2022)

3. Conceitos e definições

3.1. *Backup* tipo "*archive*" – é o utilizado pelos *backups* mensais e anuais, tem retenção maior, mas só contém a versão do arquivo no momento do *archive*.

3.2. *Backup* tipo "backup" – é o ordinário, utilizado nos *backups* diários, com retenção menor, mas que contém versões diárias dos arquivos (possibilita o *backup* de várias versões e a navegação por estas versões).

3.3. *Backup* completo – são copiados todos os arquivos existentes no momento do backup.

3.4. *Backup* em fita - mídia magnética. Pode ser movida para cofre resistente a

fogo.

3.5. *Backup* incremental – somente os arquivos novos ou modificados desde o último *backup* são transmitidos.

3.6. Disco rígido - Dispositivo de armazenamento local de dados utilizados pelos computadores.

3.7. Equipamento servidor - Computador com alta capacidade de armazenamento e processamento, destinado ao provimento de serviços e sistemas de TIC.

3.8. Produto, sistema ou serviço - soluções tecnológicas que demandam a salvaguarda de dados por ele utilizados;

3.9. Responsável pelo produto, sistema ou serviço - magistrado, servidor ou área de negócio que responde e/ou define os requisitos da solução.

3.10. RPO (*Recovery-Point Objective*) – o quanto é necessário voltar no tempo para encontrar um *backup* dos dados, ou seja, o tempo máximo de perda de dados. Em outras palavras, RPO (em tradução livre “Objetivo do Ponto de Recuperação”, resumidamente engloba o volume de dados perdidos nos casos de tempo de inatividade do serviço. Se a recuperação de um sistema com erro foi feita rapidamente (em minutos), isso não significa que a empresa perderá apenas esses minutos de trabalho, pois os dados recuperados podem ter sido capturados há uma semana, de modo que a perda real de dados nesse caso seria de uma semana.

3.11. RTO (*Recovery-Time Objective*) – tempo estimado para restaurar os dados ou para tornar os sistemas operacionais novamente. RTO (em tradução livre “Objetivo de Tempo de Recuperação”, define o período de tempo desejado necessário para realizar todas as tarefas de recuperação antes que um aplicativo ou serviço possa executar solicitações normalmente novamente. Resumidamente quanto tempo um serviço ou estrutura de TI pode ficar parada aguardando recuperação. Para fins dessa norma, o RTO deve ser considerado apenas para a restauração dos dados. (alterado pela Portaria GP.TRT4 nº 299/2022)

3.12. Versão ativa - é a última versão do arquivo no backup.

3.13. Versão de arquivos - sempre que um arquivo for criado/alterado/apagado, é criada uma nova versão deste arquivo no backup.

3.14. Versão(ões) inativa(s) – versão(ões) anterior(es) à última versão do arquivo no backup.

3.15. *Virtual Tape Library* (VTL) - tecnologia que emula fitas magnéticas em disco, o que garante gravação e restauração em alta velocidade. No TRT há duas soluções de VTL, em locais físicos distintos, para fins de continuidade e disponibilidade.

4. Referências Normativas

4.1. Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de estão de Segurança da Informação e Comunicações na Administração Pública Federal. (alterado pela Portaria GP.TRT4 nº 299/2022)

4.2. Norma Técnica ABNT NBR ISO/IEC 27001:2022, que estabelece os requisitos para um Sistema de Gestão de Segurança da Informação. (alterado pela Portaria GP.TRT4 nº 4.095/2023)

4.3. Norma ABNT NBR ISO/IEC 27002:2022, que fornece um conjunto de referência de controles de segurança da informação. (alterado pela Portaria GP.TRT4 nº 4.095/2023)

5. Procedimentos de *backup* (alterado pela Portaria GP.TRT4 nº 4.786/2020)

5.1. O responsável pelo produto, sistema ou serviço deve solicitar formalmente à Coordenadoria de Infraestrutura Tecnológica a inserção de dados ao sistema de backup, previamente à entrada em operação de tais soluções.

5.1.1. Cabe ao responsável pelo produto, sistema ou serviço, definir, com apoio da SETIC, os requisitos para realização do backup, tais como: os dados que devem estar contemplados no backup, tempo de retenção, RTO, RPO, dentre outros.

5.1.2. Em caso de alteração dos requisitos para realização do backup, o

responsável deverá atualizar a Coordenadoria de Infraestrutura Tecnológica das novas demandas, para correta salvaguarda das informações.

5.2. Os procedimentos de *backup* realizados pela SETIC serão executados por soluções automatizadas, seguindo especificações técnicas definidas pela equipe técnica responsável, em conformidade com a presente política, abrangendo os dados armazenados no ambiente tecnológico disponibilizado pelo TRT.

5.3. O *backup* dos dados armazenados nos servidores das unidades do interior do Estado será realizado diariamente, à noite.

5.4. Os dados armazenados no disco rígido de estações de trabalho ou de notebooks não serão objeto de *backup* de dados. Nesse sentido, sua recuperação não é garantida em casos de indisponibilidade causados por erros de hardware no disco rígido, apagamentos acidentais ou intencionais, falhas no sistema operacional, ação de códigos maliciosos, dentre outros.

5.5. Os dados objeto de *backup* tipo "*archive"* serão armazenados, ao final do processo, em dois locais: uma cópia no conjunto de fitas primárias, disponíveis para restaurações, e a outra cópia no conjunto de fitas secundárias, armazenadas no cofre.

5.6. A periodicidade, o tempo de retenção, o RPO e o RTO dos *backups* observarão as seguintes regras (excetuados os dados do PJe-JT, que possui regramento próprio):

Tipo de Backup		Arquivos armazenados em diretórios de rede na Capital	Arquivos armazenados em diretórios de rede do interior e dados do inFOR do interior	Dados dos sistemas armazenados no Banco de Dados da Capital (NovaJus4, inFOR Capital, e-Revista e Sistemas Administrativos)
Backup **Intradiário**	**Dias e horários**	Todos os dias, às 10h, 13h, 15h e 18h.	N/A	Todos os dias, a cada duas horas.
	Retenção	Versões objeto do *backup* serão retidas por três (3) dias.	N/A	A versão objeto de *backup* tem retenção de quinze (15) dias.
Backup **diário (tipo backup)**	**Dias e horários**	Todos os dias, com início às 22h.	Todos os dias, com início às 10h.	Completo, todos os dias.
	Retenção	Quinze (15) últimas versões do arquivo, desde que as versões inativas estejam dentro de um prazo de 30 dias. No caso de arquivos deletados, a última versão será mantida pelo prazo de 60 dias.	Trinta (30) últimas versões do arquivo, desde que as versões inativas estejam dentro de um prazo de 30 dias. No caso de arquivo deletados, a última versão será mantida pelo prazo de 60 dias.	A versão objeto de *backup* tem retenção de quinze (15) dias.
Backup **semanal (tipo archive)**	**Dias e horários**	N/A	N/A	N/A
	Retenção	N/A	NA	N/A
Backup **mensal (tipo archive)**	**Dias e horários**	Terceiro final de semana de cada mês	Terceiro final de semana de cada mês	Primeiro final de semana de cada mês
	Retenção	A versão dos arquivos objeto do *backup* será retida pelo período de seis (6) meses.	A versão dos arquivos objeto do *backup* será retida pelo período de seis (6) meses.	A versão objeto de *backup* será retida pelo período de quinze (15) meses.
Backup **anual (tipo archive)**	**Dias e horários**	Durante o recesso	Durante o recesso	Durante o recesso
	Retenção	A versão dos arquivos objeto do *backup* será retida pelo período de cinco (5) anos.	A versão dos arquivos objeto do *backup* será retida pelo período de cinco (5) anos.	A versão objeto do *backup* será retida pelo período de dez (10) anos.
RPO (tempo máximo de perda dos dados)		10 horas	24 horas	2 horas
RTO (tempo estimado para a restauração)		Imediato para restaurações pontuais. 30 horas para restauração completa.	2 horas	28 horas

5.7. A periodicidade, o tempo de retenção, o RPO e o RTO dos *backups* do banco de dados Postgresql relativos ao PJe-JT observarão as seguintes regras:

Tipo de Backup	**BANCO DE DADOS POSTGRESQL**	
***Backup* diário VTL**	**Dias e horários**	Completo, todos os dias.
	Retenção	A versão objeto do *backup* será retida pelo período de quinze (15) dias.
Backup semanal (tipo archive) Tape	**Dia**	Todo final de semana que não coincidir com o backup mensal
	Retenção	15 dias
***Backup* mensal (tipo *archive*) Tape**	**Dia**	Primeiro final de semana de cada mês
	Retenção	A versão objeto do *backup* será retida pelo período de um (1) ano
***Backup* anual (tipo *archive*) Tape**	**Dia**	Em janeiro do ano seguinte, entre os dias 1º e 28, preferencialmente no primeiro domingo.
	Retenção	A versão objeto do *backup* será retida pelo período de cinco (5) anos.
VTL - RPO (tempo máximo de perda dos dados)	4 horas	
VTL - RTO (tempo estimado para a restauração)	20 horas	
RPO (tempo máximo de perda dos dados) Tape	1 semana	
RTO (tempo estimado para a restauração) Tape	20h + procedimentos de inserção das fitas	

5.8. No caso de serviços armazenados em nuvem, a responsabilidade pelo *backup* será da prestadora de serviços, assegurado um prazo de retenção de, no mínimo, 30 dias.

5.9. As mídias de backup, quando transportadas, deverão ser protegidas de extravio e de eventos que possam causar dano físico.

5.9.1. A movimentação de mídias de *backup* deverá ser realizada por servidor designado, com registro, no mínimo, da identificação da mídia e a

data e hora da movimentação.

6. Recuperação de dados

6.1. A recuperação de dados e arquivos, sempre que não puder ser realizada pelo próprio usuário, será solicitada à Secretaria de Tecnologia da Informação e Comunicações, por meio da Divisão de Central de Serviços de Tecnologia da Informação e Comunicações. (alterado pela Portaria GP.TRT4 nº 4.920/2022)

7. Testes de recuperação de dados

7.1. Periodicamente serão realizados testes de recuperação de dados.

7.2. Os testes serão baseados em dados pré-selecionados que garantam a efetividade, eficiência e confiabilidade do procedimento, na periodicidade e forma estabelecidas no quadro que segue: (alterado pela Portaria GP.TRT4 nº 4.920/2022).

Grupo de *backup*	Equipes responsáveis pela recuperação	Periodicidade	Recuperação	Equipe responsável pela validação	Validação
Arquivos armazenados em diretórios de rede na Capital	DIBD	Mensal	Restaurar versão do dia anterior de alguns arquivos do volume lógico (drive) sendo testado.	DIOP	Por amostragem, verificar a integridade de alguns arquivos recuperados.
	DIOP	Mensal	Utilizando o recurso "Versões Anteriores", restaurar versão do dia anterior de arquivos das cópias intradiárias	DIOP	Por amostragem, verificar a integridade de alguns arquivos recuperados.
Arquivos armazenados em diretórios de rede do interior	DIBD	Mensal	Restaurar a versão mais recente de alguns arquivos de uma localidade do interior. Alternar localidade a cada teste.	DIRT	Por amostragem, verificar a integridade de alguns arquivos recuperados.
Dados do inFOR do interior	DIBD	Semestral	Restaurar versão do dia anterior da base de dados do inFOR de uma das localidades do interior. Alternar localidade a cada teste.	CDS	Testar, por amostragem, o funcionamento adequado do sistema em relação a determinado processo em uma unidade do interior.
Dados dos sistemas armazenados no Banco de Dados da Capital	DIBD	Bimestral	Restaurar versão do dia anterior de uma das tablespaces da base de produção, alternando a cada teste o sistema (inFOR, NovaJus4, Folha, RH, PJ4, System) envolvido.	CDS	Testar, por amostragem, o funcionamento adequado do sistema cujas tablespaces foram recuperadas. Testar inFOR, NovaJus4 e ADMEletrônico em relação a determinado processo. Testar sistemas RH e Folha em relação a determinado servidor.

PJe/Banco de dados	DIBD	Trimestral	Restauração efetuada em um servidor específico para essa funcionalidade, em ambiente VMware.	DIBD	Testar a integridade dos dados e funcionamento da base principal do PJe restaurada.

7.3. Os resultados dos testes serão validados, de forma documentada, pelas equipes identificadas no quadro anterior.

7.4. Se restaurações de dados forem realizadas em períodos iguais ou menores que os definidos para os testes, a equipe responsável pela execução dos testes poderá, a partir dos resultados obtidos, considerar que tais ações têm validade como teste naquele período.

8. Atualização da Norma

8.1. As diretrizes previstas na presente norma serão atualizadas sempre que alterados os procedimentos de backup, observada, ainda, a periodicidade prevista para a revisão da Política de Segurança da Informação.