PORTARIA N. 8.605 de 05 de novembro de 2013.

Altera a Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 4ª Região.

A PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a necessidade de aprimorar a atual Política de Segurança da Informação, instituída pela Portaria 4772/2008 da Presidência deste Tribunal, com a normatização de situações ainda não regradas;

CONSIDERANDO a recomendação do Tribunal de Contas da União, no sentido de alinhamento da Política de Segurança às diretrizes nacionais, contemplando itens não normatizados (item 9.1.1 do Acórdão 381/11);

CONSIDERANDO a necessidade de formalizar os procedimentos de backup atualmente realizados pela Secretaria de Tecnologia da Informação e Comunicações, bem como regrar os procedimentos de recuperação de dados e testes;

CONSIDERANDO o parecer favorável da Comissão de Informática deste Tribunal à proposta apresentada pelo Comitê de Segurança da Informação;

RESOLVE:

Art. 1º Alterar a Portaria 4772/2008 da Presidência deste Tribunal para incluir o Anexo 4 (*NSI004 – Procedimentos de backup e recuperação de dados)*, com a seguinte redação:

ANEXO 4

NSI 004 – Procedimentos de backup e recuperação de dados

1. Objetivo

Normatizar e dar publicidade aos procedimentos de backup, testes e recuperação de dados realizados pela Secretaria de Tecnologia da Informação e Comunicações.

2. Conceitos e definições

Para os efeitos desta norma são estabelecidos os seguintes conceitos e

definições:

2.1.TSM Server: é o equipamento servidor de backup, que gerencia todos os backups realizados.

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

3. Versão ativa: é a última versão do arquivo no backup.

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

2.5. 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).

2.6. 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.

2.7. Backup incremental: somente os arquivos novos ou modificados desde o último backup são transmitidos.

2.8. Backup completo: são transmitidos todos os arquivos existentes no momento do backup.

2.9. 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.

2.10. RTO (*recovery-time objective*): tempo estimado para restaurar os dados ou para tornar os sistemas operacionais novamente.

3. Procedimentos de backup

3.1. Os procedimentos de backup realizados pela SETIC serão executados de forma automática e abrangem os dados gravados nos diretórios de rede privativos de cada unidade judiciária e administrativa do Tribunal e nos sistemas computacionais disponibilizados pelo TRT.

3.1.1. O backup dos dados das unidades do interior do Estado será realizado a partir do repositório centralizado em Porto Alegre, após a sincronização dos equipamentos-servidores de cada Foro, realizada ao final de cada dia.

3.1.2. Os dados armazenados em discos rígidos locais não serão copiados e não será garantida sua recuperação em caso de erro físico nas mídias de gravação ou instabilidade no sistema operacional

instalado na máquina.

3.2. Os dados objeto de backup 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.

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

		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 horário	De segunda a sexta-feira, às 10h, 13h, 15h e 18h.	X-X-X-X	Todos os dias, a cada duas horas.
	Retenção	Versões objeto do backup serão retidas por três (3) dias.	X-X-X-X	A versão objeto de backup tem retenção de oito (8) semanas.
Backup diário (tipo backup)	Dias e horário	De segunda a sexta-feira, com início às 22h.	De segunda a sexta-feira, com início às 5h.	De segunda a sexta-feira, de forma incremental, e no final de semana, de forma completa.
	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 arquivos deletados, a última versão será mantida pelo prazo de 60 dias.	A versão objeto de backup tem retenção de oito (8) semanas.
Backup semanal (tipo archive)	Dias e horário	X-X-X-X	X-X-X-X	X-X-X-X
	Retenção	X-X-X-X	X-X-X-X	X-X-X-X
Backup mensal (tipo	Dias e horário	Terceiro final de semana de cada mês	Último final de semana de cada mês	Primeiro final de semana de cada mês

		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)
archive)	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 horário	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 seis (6) 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

3.4. A periodicidade, tempo de retenção, RPO e RTO dos backups dos dados relativos ao Pje-JT observarão as seguintes regras:

		ARQUIVOS DE CONFIGURAÇÃO DO APACHE (Interno e Externo)	**ARQUIVOS DE CONFIGURAÇÃO DO JBOSS**	**BANCO DE DADOS POSTGRES**
Backup incremental diário	Dias e horário	De segunda a sexta-feira, com início às 21h.	De segunda a sexta-feira, com início às 21h.	De segunda a sexta-feira, com início às 21h.
	Retenção	A versão objeto do backup será retida pelo período de trinta (30) dias.	A versão objeto do backup será retida pelo período de trinta (30) dias.	A versão objeto do backup será retida pelo período de trinta (30) dias.
Backup mensal (tipo archive)	Dia	Segundo domingo do mês.	Segundo domingo do mês.	Segundo domingo do mês.
	Retenção	A versão objeto do backup será retida	A versão objeto do backup será retida pelo	A versão objeto do backup será retida pelo

		ARQUIVOS DE CONFIGURAÇÃO DO APACHE (Interno e Externo)	**ARQUIVOS DE CONFIGURAÇÃO DO JBOSS**	**BANCO DE DADOS POSTGRES**
		pelo período de um (1) ano	período de um (1) ano	período de um (1) ano
Backup anual (tipo archive)	Dia	Em janeiro do ano seguinte, entre 01 e 28 de janeiro, preferencialmente no primeiro domingo de janeiro.	Em janeiro do ano seguinte, entre 01 e 28 de janeiro, preferencialmente no primeiro domingo de janeiro.	Em janeiro do ano seguinte, entre 01 e 28 de janeiro, preferencialmente no primeiro domingo de janeiro.
	Retenção	A versão objeto do backup será retida pelo período de cinco (5) anos.	A versão objeto do backup será retida pelo período de cinco (5) anos.	A versão objeto do backup será retida pelo período de cinco (5) anos.
RPO (tempo máximo de perda dos dados)		24 horas	24 horas	24 horas
RTO (tempo estimado para a restauração)		1 hora	4 horas	4 horas

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

4. Recuperação de dados

4.1. 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 Seção de Atendimento ao Usuário.

5. Testes de recuperação de dados

5.1. Periodicamente serão realizados testes de recuperação de dados.

5.2. Os testes serão baseados em dados pré-selecionados que garantam a efetividade, eficiência e confiabilidade do procedimento, na periodicidade e forma estabelecida no quadro que segue:

Grupo de backup	**Equipes responsáveis**	**Periodicidade**	**Recuperação**	**Equipe responsável**	**Validação**

	pela recuperação			**pela validação**	
Arquivos armazenados em diretórios de rede na Capital	SST/SGBD	mensal	Restaurar versão do dia anterior de alguns arquivos do volume lógico (drive) sendo testado.	SST	Por amostragem, verificar a integridade de alguns arquivos recuperados.
Arquivos armazenados em diretórios de rede do Interior	SRT/SGBD	mensal	Restaurar a versão mais recente de alguns arquivos de uma localidade do interior. Alternar localidade a cada teste.	SRT	Por amostragem, verificar a integridade de alguns arquivos recuperados.
Dados do inFOR do interior	SGBD	Semestral	Restaurar versão do dia anterior da base de dados do Infor de uma das localidades do inteior. 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	SGBD	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	SGDB	mensal	Restaurar para base de BUGFIX e para a base de testes (TST) ou de Treinamento (TRN) do Pje a base de produção.	SGBD/ Equipe de apoio do PJe	Testar a integridade dos dados e funcionamento da base restaurada, mediante sua utilização para homologação de novas versões do PJe.

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

5.4. 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 tem validade como teste naquele período.

6. Revisão e atualização das normas

6.1. As normas previstas no presente anexo serão atualizadas sempre que alterados os procedimentos de backup.

6.2. A revisão das normas observará a periodicidade prevista para a revisão da Política de Segurança da Informação.

Art. 2º No prazo de 5 dias a contar da publicação deste Ato será publicado na intranet texto compilado da Portaria 4772/08, com as alterações introduzidas por esta Portaria.

Art. 3º A presente Portaria entra em vigor a partir da data de sua publicação.

MARIA HELENA MALLMANN,

Presidente do TRT da 4ª Região