PODER JUDICIÁRIO
TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO

PORTARIA Nº 7.138, DE 20 DE NOVEMBRO DE 2014.

Altera os Anexos 1, 2 e 4 da Portaria nº 4.772/2008, a qual institui 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 o que consta nos processos administrativos eletrônicos nº 0003394-28.2013.5.04.0000 (PA), 0003728-96.2012.5.04.0000 (PA) e 0004550-85.2012.5.04.0000 (PA);

RESOLVE:

Art. 1º Alterar os incisos I, II e IV do item 3.2 do Anexo 1 (NSI001 – Controle de Acesso à Internet) da Portaria nº 4.772/2008, que passam a vigorar com a seguinte redação:

> 3.2 (...)
> I – acessar páginas de conteúdo considerado ofensivo, ilegal, impróprio ou incompatível com as atividades funcionais ou com a política de segurança da informação, tais como pornografia, pedofilia, racismo, sítios de compras, jogos e páginas de distribuição e de compartilhamento de software.
> II – utilizar programas de troca de mensagens em tempo real (bate-papo) ou programas para troca de conteúdo via rede ponto-a-ponto (peer-to-peer), exceto os definidos como ferramenta de trabalho e homologados pela Secretaria de Tecnologia da Informação e Comunicações.
> (...)
> IV – acessar sítios que representem ameaça à segurança da informação ou que possam comprometer de alguma forma a integridade da rede de computadores do TRT.

Art. 2° Alterar o Anexo 2 (NSI002 – Controle de Uso do Correio Eletrônico) da Portaria nº 4.772/2008, que passa a vigorar com a seguinte redação:

Documento digitalmente assinado em 24/11/2014, nos termos da Lei 11.419/06. Processo 0003394-28.2013.5.04.0000-(PA)
Confira a autenticidade em www.trt4.jus.br. Identificador: ADME.70955.73956.86141.69499-9

ANEXO 2
NSI002 – Do Serviço de Correio Eletrônico Institucional

1. Objetivo

Esta norma estabelece regras e padrões para a utilização do serviço de correio eletrônico no âmbito do TRT da 4ª Região.

2. Conceitos

Para os efeitos desta norma são estabelecidos os seguintes conceitos e definições:

2.1 Serviço de correio eletrônico institucional – serviço de envio e recebimento de mensagens eletrônicas (também conhecidas por "*e-mails"*) no âmbito do TRT da 4ª Região.

2.2 Caixa postal – conta de correio eletrônico onde são armazenadas as mensagens recebidas e/ou enviadas.

2.2.1 Caixa postal institucional pessoal – conta de correio eletrônico de um único usuário (magistrado, servidor ou estagiário).

2.2.2 Caixa postal institucional da unidade – conta de correio eletrônico de uma unidade administrativa ou judiciária, constante da estrutura organizacional do Tribunal.

2.2.3 Caixa postal de sistema – conta de correio eletrônico de um sistema informatizado que necessite esse recurso para o seu funcionamento.

2.3 Lista de distribuição – agrupamento de diversos endereços eletrônicos, que permite a distribuição conjunta de uma mensagem eletrônica a todos os seus integrantes, sem caixa postal específica.

2.4 Endereço eletrônico – conjunto de caracteres que individualiza e identifica o remetente e o destinatário da mensagem eletrônica. É formado por um identificador e por um domínio, separados pelo símbolo arroba (@).

2.4.1 Identificador – parte inicial do endereço eletrônico, localizada antes do símbolo arroba (@).

2.4.2 Domínio – parte final do endereço eletrônico, localizada após o símbolo arroba (@).

2.5 Arquivo de registro de mensagens (logs) – compila registros de eventos relevantes, utilizados para restaurar um sistema, diagnosticar problemas, ou realizar auditorias.

2.6 Usuário de correio eletrônico – magistrado, servidor e estagiário.

2.7 *Spam* – mensagem enviada a um grande número de endereços eletrônicos, que não possua caráter institucional e/ou cujo objeto não seja inerente à atividade funcional do usuário ou da unidade.

Documento digitalmente assinado em 24/11/2014, nos termos da Lei 11.419/06. Processo 0003394-28.2013.5.04.0000-(PA)
Confira a autenticidade em www.trt4.jus.br. Identificador: ADME.70955.73956.86141.69499-9

2.8 *Phishing* – fraude eletrônica, caracterizada pela tentativa de obtenção de dados e informações pessoais com o uso de meios técnicos e de engenharia social.

2.9 *Malware* – programas indesejados, desenvolvidos com a finalidade de executar ações danosas e atividades maliciosas em um computador ou sistema (ex.: *worm*, *bot*, *spyware*, *backdoor*, cavalo de tróia e *rootkit).*

2.10 Material criptografado – dados e/ou informações codificadas por meio de técnicas que impossibilitam o seu entendimento/leitura, cuja reversão ocorre somente com a utilização de uma senha previamente conhecida e/ou dispositivo criptográfico (ex.: *token*, *smart card*).

2.11 *Hoax* – mensagem eletrônica encaminhada a muitos destinatários e de conteúdo geralmente alarmante e com pouca ou nenhuma veracidade, cujo objetivo é a propagação de boatos e informações distorcidas.

3. Referências Normativas

3.1 Instrução Normativa GSI/PR nº 1, de 13.06.2008, do Gabinete de Segurança Institucional da Presidência da República, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

3.2 Norma Complementar nº 01/IN01/DSIC/GSIPR, de 15.10.2008, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal, direta e indireta.

3.3 Norma Complementar nº 07/IN01/DSIC/GSIPR (Revisão 01), de 15.07.2014, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece diretrizes para a implementação de controles de acesso à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

3.4 Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro da organização.

3.5 Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação.

4. Caixas postais de correio eletrônico (criação, alteração e exclusão)

4.1 As caixas postais são identificadas unicamente por meio de seu endereço eletrônico.

Documento digitalmente assinado em 24/11/2014, nos termos da Lei 11.419/06. Processo 0003394-28.2013.5.04.0000-(PA)
Confira a autenticidade em www.trt4.jus.br. Identificador: ADME.70955.73956.86141.69499-9

4.2 No âmbito deste Tribunal, o domínio do endereço eletrônico é “trt4.jus.br”.

4.3 As caixas postais têm capacidade de armazenamento limitada a 25 gigabytes (GB).

4.4 Somente será criada caixa postal institucional pessoal, caixa postal institucional da unidade ou caixa postal de sistema.

4.5 As solicitações de criação, alteração e exclusão de caixas postais devem ser encaminhadas à Secretaria de Tecnologia da Informação e Comunicações.

4.6 No caso de alteração de endereço eletrônico, o endereço antigo será mantido apenas pelo período de três meses, a contar da alteração.

4.7 Caixa Postal Institucional Pessoal

4.7.1 Magistrados e Servidores

4.7.1.1 Todo magistrado e servidor terá uma caixa postal institucional pessoal.

4.7.1.2 A solicitação de caixa postal institucional pessoal para magistrado incumbe à Secretaria de Apoio aos Magistrados e, para servidor, à Secretaria de Gestão de Pessoas.

4.7.1.3 O identificador do endereço de correio eletrônico será formado pelo primeiro nome e pelo último sobrenome do magistrado ou servidor, separados pelo sinal de ponto.

4.7.1.4 O identificador do endereço de correio eletrônico poderá, em situações excepcionais, a critério da Secretaria de Tecnologia da Informação e Comunicações, ser a primeira letra do nome do usuário, seguida do sobrenome.

4.7.1.5 A adequação dos endereços de correio eletrônico ao padrão ora estabelecido deve ser solicitada pelo próprio interessado.

4.7.1.6 A caixa postal institucional pessoal de magistrados e/ou servidores falecidos ou afastados em decorrência de exoneração, redistribuição, aposentadoria, remoção e cedência a outro órgão, ou retorno à origem, serão excluídas, definitivamente, em 20 dias a contar da informação da Secretaria de Apoio aos Magistrados ou da Secretaria de Gestão de Pessoas acerca dos fatos acima referidos.

4.7.2 Estagiários

4.7.2.1 O gestor da unidade poderá solicitar, por escrito, a criação de caixa postal institucional pessoal ao estagiário somente quando houver essa necessidade para o serviço a ser desempenhado.

4.7.2.2 O envio de mensagem por estagiário será restrito aos endereços eletrônicos mantidos pelo Tribunal.

4.7.2.3 O identificador do endereço eletrônico do estagiário será formado pela primeira letra do seu nome seguida do último sobrenome, acrescido pela palavra “estagiário”, separados pelo sinal de ponto.

Documento digitalmente assinado em 24/11/2014, nos termos da Lei 11.419/06. Processo 0003394-28.2013.5.04.0000-(PA)
Confira a autenticidade em www.trt4.jus.br. Identificador: ADME.70955.73956.86141.69499-9

4.7.2.4 O uso do correio eletrônico pelo estagiário será de total responsabilidade do gestor da unidade, a quem incumbirá solicitar, por escrito, a exclusão dessa caixa postal imediatamente após o desligamento do estagiário da respectiva unidade administrativa ou judiciária.

4.8 Caixa Postal Institucional da Unidade

4.8.1 As unidades administrativas e judiciárias previstas na estrutura organizacional do Tribunal poderão ter caixa postal institucional da unidade.
4.8.2 O gestor da unidade será também o gestor da respectiva caixa postal, competindo-lhe:
a) solicitar a criação, a alteração e a exclusão da caixa postal institucional da unidade;
b) autorizar o acesso de outros servidores, mediante delegação no sistema de correio eletrônico, bem como excluir esse acesso.
4.8.3 A caixa postal institucional da unidade terá um único endereço de correio eletrônico, cujo identificador será formado pela denominação da unidade ou por sigla que permita a sua identificação.
4.8.4 As comissões, os grupos de trabalho e outros núcleos formalmente constituídos, ainda que não constantes na estrutura organizacional do Tribunal, poderão, em caráter excepcional, ter caixa postal institucional quando o desempenho das atividades que lhes são afetas necessitar a troca de mensagens eletrônicas com o público externo.
4.8.5 A caixa postal referida no item acima fica a critério da Presidência, a quem compete solicitar a sua criação, indicar o magistrado, o servidor ou a unidade que será responsável pelo respectivo gerenciamento, bem como, se for o caso, estabelecer o período de duração dessa caixa.

4.9 Caixa Postal de Sistema
4.9.1 A caixa postal de sistema será criada quando houver essa necessidade para o funcionamento de um sistema informatizado.
4.9.2 O gestor da unidade responsável pelo desenvolvimento ou manutenção do sistema informatizado será também o gestor da respectiva caixa postal, competindo-lhe:
a) solicitar a criação, alteração e exclusão da caixa postal de sistema;
b) autorizar o acesso de outros servidores, mediante delegação no sistema de correio eletrônico, bem como excluir esse acesso.
4.9.3 O identificador do endereço de correio eletrônico será formado pela denominação ou sigla que permita a identificação do respectivo sistema informatizado.

5. Lista de distribuição (criação, alteração e exclusão)

5.1 É permitida a criação de lista de distribuição, com o objetivo de facilitar e otimizar a troca de informações sobre assuntos de interesse do Tribunal.

Documento digitalmente assinado em 24/11/2014, nos termos da Lei 11.419/06. Processo 0003394-28.2013.5.04.0000-(PA)
Confira a autenticidade em www.trt4.jus.br. Identificador: ADME.70955.73956.86141.69499-9

5.2 A criação de lista de distribuição pode ser solicitada pelo gestor da unidade a qual se destina ou pela Presidência.

5.3 A solicitação deve ser encaminhada, por escrito, à Secretaria de Tecnologia da Informação e Comunicações, acompanhada de justificativa e, quando destinada à atividade temporária, do período de sua duração.

5.4 Cada lista de distribuição terá um gestor, a quem incumbe:

a) manter permanentemente atualizado o rol de integrantes da lista de distribuição;

b) solicitar exclusão como gestor e indicar, simultaneamente, o novo responsável pela lista de distribuição;

c) solicitar exclusão da lista de distribuição, quando esta não for mais necessária.

5.5 O identificador do endereço eletrônico será formado pela denominação ou sigla, que permita, de forma clara, a identificação de sua finalidade, ou do grupo de endereços eletrônicos nela reunidos, seguido da palavra “lista”, separados por hífen.

5.6 A lista de distribuição será composta exclusivamente por endereços eletrônicos do Tribunal e será bloqueada para o recebimento de mensagem eletrônica enviada pelo público externo, excepcionando-se, a critério da Presidência, aquelas integradas por representantes externos (ex.: Comitê Gestor Regional do Sistema Processo Judicial Eletrônico da Justiça do Trabalho – PJe-JT e Conselho Consultivo da Escola Judicial).

5.7 A Secretaria de Tecnologia da Informação e Comunicações deve manter, permanentemente, tabela atualizada com as listas de distribuição do Tribunal e seus respectivos gestores.

6. Utilização dos recursos do sistema de correio eletrônico

6.1 O uso do correio eletrônico institucional restringe-se a mensagem cujo objeto seja, necessariamente, inerente à atividade funcional do usuário ou da unidade, sendo vedado o uso para fins particulares.

6.2 O acesso ao correio eletrônico, a partir de estações de trabalho fornecidas pelo Tribunal, será feito apenas a partir do navegador de internet.

6.3 É vedada a tentativa de acesso a caixas postais às quais o usuário não tenha autorização de acesso.

6.4 O tamanho máximo da mensagem eletrônica, incluindo os anexos, não pode exceder 20 megabytes (MB).

6.5 O envio de mensagem eletrônica para lista de distribuição que englobe elevado número de endereços eletrônicos somente é permitido em caráter excepcional e por aquelas unidades administrativas autorizadas pela Presidência.

6.6 É de responsabilidade do usuário:

Documento digitalmente assinado em 24/11/2014, nos termos da Lei 11.419/06. Processo 0003394-28.2013.5.04.0000-(PA)
Confira a autenticidade em www.trt4.jus.br. Identificador: ADME.70955.73956.86141.69499-9

a) utilizar o correio eletrônico institucional de acordo com os preceitos desta Norma;
b) eliminar periodicamente as mensagens eletrônicas contidas nas caixas postais;
c) manter apenas o seu acesso à conta institucional pessoal de correio eletrônico, sendo vedada a disponibilização desse acesso a terceiros;
d) informar ao Escritório de Segurança da Informação o recebimento de mensagem que contrarie o disposto no item 6.7.

6.7 É vedado aos usuários o envio de qualquer mensagem eletrônica contendo:
a) informações privilegiadas, confidenciais e/ou de propriedade do Tribunal para destinatários não autorizados;
b) materiais obscenos, ilegais ou antiéticos;
c) materiais preconceituosos ou discriminatórios;
d) materiais caluniosos ou difamatórios;
e) propaganda com objetivo comercial;
f) listagem com endereços eletrônicos institucionais;
g) *malwares* (item 2.8)*;*
h) material de natureza político-partidária, associativa ou sindical, que promova a eleição de candidatos para cargos eletivos;
i) material protegido por lei de propriedade intelectual;
j) entretenimentos e "correntes";
l) assuntos ofensivos;
m) músicas, vídeos ou animações que não sejam de interesse específico do trabalho;
n) *Spam, phishing e hoa*x (itens 2.7, 2.8 e 2.11);
o) materiais criptografados.

7. Monitoramento e Auditoria

7.1 O uso do correio eletrônico será monitorado por meio de ferramentas com o intuito de impedir o recebimento de *spam*, *hoax*, *phishing*, mensagens contendo vírus e outros arquivos, que coloquem em risco a segurança da infraestrutura tecnológica do Tribunal ou que contenham conteúdo impróprio.

7.2 Os relatórios decorrentes das auditorias ordinárias feitas pelo Escritório de Segurança da Informação serão encaminhados ao Comitê de Segurança da Informação.

7.3 Verificados indícios de incidentes que atentem contra a segurança da informação, a chefia imediata ou superior solicitará ao Comitê de Segurança da Informação a realização de auditoria extraordinária.

7.4 A Secretaria de Tecnologia da Informação e Comunicações armazenará os arquivos de registro de mensagens eletrônicas (logs), pelo período mínimo de 30 dias.

7.5 A eliminação dos arquivos de registro de mensagens eletrônicas (logs) e de caixas postais será adiada em caso de auditoria, bem como de notificação administrativa ou judicial.

Documento digitalmente assinado em 24/11/2014, nos termos da Lei 11.419/06. Processo 0003394-28.2013.5.04.0000-(PA)
Confira a autenticidade em www.trt4.jus.br. Identificador: ADME.70955.73956.86141.69499-9

7.6 A Secretaria de Tecnologia da Informação e Comunicações encaminhará, até o dia 5 de dezembro de cada ano, relatório às unidades e aos respectivos gestores, com o rol das listas de distribuição e caixas postais a elas vinculadas, bem como a lista de eventuais caixas postais de estagiários lotados na respectiva unidade.

7.7 Cabe ao gestor conferir os dados do relatório referido no item anterior e, até o dia 15 de dezembro do mesmo ano, ratificar o conteúdo desse relatório à Secretaria de Tecnologia da Informação e Comunicações, ou informar as alterações porventuras havidas.

Art. 3° Alterar o Anexo 4 (NSI004 – Procedimentos de backup e recuperação de dados) da Portaria nº 4.772/2008, que passa a vigorar com a seguinte redação:

ANEXO 4
NSI004 – 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 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.*

2.2 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).

2.3 Backup completo – são transmitidos todos os arquivos existentes no momento do backup.

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

2.5 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.

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

2.7 Tivoli Storage Manager (TSM) Server – é o equipamento servidor de backup, que gerencia todos os backups realizados.

2.8 Versão ativa – é a última versão do arquivo no backup.

Documento digitalmente assinado em 24/11/2014, nos termos da Lei 11.419/06. Processo 0003394-28.2013.5.04.0000-(PA)
Confira a autenticidade em www.trt4.jus.br. Identificador: ADME.70955.73956.86141.69499-9

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

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

3. Referências Normativas

3.1 Instrução Normativa GSI/PR nº 1, de 13.06.2008, do Gabinete de Segurança Institucional da Presidência da República, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

3.2 Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro da organização.

3.3 Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação.

4. Procedimentos de backup

4.1 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.

4.1.1 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.

4.1.2 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.

4.2 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.

4.3 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):

Documento digitalmente assinado em 24/11/2014, nos termos da Lei 11.419/06. Processo 0003394-28.2013.5.04.0000-(PA)
Confira a autenticidade em www.trt4.jus.br. Identificador: ADME.70955.73956.86141.69499-9

		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	De segunda a sexta-feira, 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	De segunda a sexta-feira, com início às 22h.	De segunda a sexta-feira, com início às 5h.	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 arquivos 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	N/A	N/A
Backup mensal (tipo archive)	Dias e horários	Terceiro final de semana de cada mês	Último 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 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

Documento digitalmente assinado em 24/11/2014, nos termos da Lei 11.419/06. Processo 0003394-28.2013.5.04.0000-(PA)
Confira a autenticidade em www.trt4.jus.br. Identificador: ADME.70955.73956.86141.69499-9

4.4 A periodicidade, o tempo de retenção, o RPO e o 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 diário	Dias e horários	Incremental, de segunda a sexta-feira, com início às 21h.	Incremental, de segunda a sexta-feira, com início às 21h.	Completo, todos os dias.
	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 quinze (15) 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 pelo período de um (1) ano	A versão objeto do backup será retida pelo período de um (1) ano	A versão objeto do backup será retida pelo período de um (1) ano
Backup anual (tipo archive)	Dia	Em janeiro do ano seguinte, entre os dias 1º e 28, preferencialmente no primeiro domingo.	Em janeiro do ano seguinte, entre os dias 1º e 28, preferencialmente no primeiro domingo.	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.	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	02 horas
RTO (tempo estimado para a restauração)		1 hora	4 horas	19 horas

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

5. Recuperação de dados

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.

6. Testes de recuperação de dados

Documento digitalmente assinado em 24/11/2014, nos termos da Lei 11.419/06. Processo 0003394-28.2013.5.04.0000-(PA)
Confira a autenticidade em www.trt4.jus.br. Identificador: ADME.70955.73956.86141.69499-9

6.1 Periodicamente serão realizados testes de recuperação de dados.

6.2 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:

Grupo de backup	Equipes responsáveis pela recuperação	Periodicidade	Recuperação	Equipe responsável pela validação	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 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.

Documento digitalmente assinado em 24/11/2014, nos termos da Lei 11.419/06. Processo 0003394-28.2013.5.04.0000-(PA)
Confira a autenticidade em www.trt4.jus.br. Identificador: ADME.70955.73956.86141.69499-9

Grupo de backup	Equipes responsáveis pela recuperação	Periodicidade	Recuperação	Equipe responsável pela validação	Validação
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.

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

6.4 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.

7. Revisão e atualização das normas

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

Documento digitalmente assinado em 24/11/2014, nos termos da Lei 11.419/06. Processo 0003394-28.2013.5.04.0000-(PA)
Confira a autenticidade em www.trt4.jus.br. Identificador: ADME.70955.73956.86141.69499-9

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

Art. 4º Republique-se a Portaria nº 4.772/2008, com as alterações ora efetuadas.

Art. 5º Esta Portaria entra em vigor na data de sua publicação.

CLEUSA REGINA HALFEN
Presidente do TRT da 4ª Região/RS

Documento digitalmente assinado em 24/11/2014, nos termos da Lei 11.419/06. Processo 0003394-28.2013.5.04.0000-(PA)
Confira a autenticidade em www.trt4.jus.br. Identificador: ADME.70955.73956.86141.69499-9