PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

ATO Nº 227/2013 (*)

Aprova a Norma Complementar de Cópia de Segurança e de Restauração de Sistemas, Aplicativos, Dados e de Documentos no âmbito do Tribunal Regional do Trabalho da 7ª Região.

A PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO, no uso de suas atribuições legais e regimentais;

CONSIDERANDO as boas práticas de Governança de TI que visam garantir a disponibilidade e integridade de sistemas, aplicativos, dados e de documentos digitais do TRT da 7ª Região;

CONSIDERANDO a necessidade de definir e implementar procedimentos de cópia de segurança (*backup*) e de restauração de sistemas, aplicativos, dados e de documentos digitais do Tribunal Regional do Trabalho da 7ª Região;

RESOLVE:

Art. 1º Aprovar a Norma Complementar nº 01/NC/STI/SESTI, da Secretaria de Tecnologia da Informação, que dispõe sobre procedimentos de cópia de segurança e de restauração de sistemas, aplicativos, dados e de documentos digitais do Tribunal Regional do Trabalho da 7ª Região, na forma do anexo, para observância e aplicação em todo o Regional.

Art. 2º Este ato entra em vigor na data de sua publicação.

PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.
Fortaleza, 29 de maio de 2013.
MARIA ROSELI MENDES ALENCAR
Presidente

(*) Revogado pelo Ato TRT7.GP nº 88/2020 disponibilizado no Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 3031, 05 ago. 2020. Caderno Administrativo do Tribunal Regional do Trabalho da 7ª Região, p. 1.

Fonte: Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 1236, 31 mai. 2013. Caderno Judiciário do Tribunal Regional do Trabalho da 7ª Região, p. 7.

Anexo do Ato 227/2013 - Revogado

Tribunal Regional do Trabalho da 7ª Região Secretaria de Tecnologia da Informação Escritório de Segurança da Tecnologia da Informação	Número da Norma Complementar	Revisão	Emissão	Folha
	01/NC/STI/SESTI	00	00/00/00	1/1
	Cópia de Segurança e Restauração de Sistemas, Aplicativos, Dados e Documentos			

1 OBJETIVO
1.1 Definir e implementar procedimentos de cópia de segurança (*backup*) e restauração de sistemas, aplicativos, dados e documentos digitais do Tribunal Regional do Trabalho da 7ª Região.
2 CONSIDERAÇÕES FINAIS
2.1 Em aplicação as boas praticas de Governança de TI e visando garantir a disponibilidade e integridade de sistemas, aplicativos, dados e documentos digitais do Tribunal Regional do Trabalho da 7ª Região.
2.2 Esta Norma Complementar de Cópia de Segurança e Restauração de Sistemas, Aplicativos, Dados e Documentos armazenadas no DATACENTER deste E. TRT e dos dados armazenados nos computadores servidores do interior, vem definir e implementar procedimentos de cópia de segurança e restauração, excluídas as informações mantidas pelos usuários em suas estações de trabalho.
3 FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR
3.1 Decreto nº 3.505, de 13 de Junho de 2000, que institui a Política de Segurança da Informação nos Órgãos da Administração Pública Federal, Item I Art. 3º, *"dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis".*
3.2 Cobit 4.1, DS 11.5, "Definir e implementar procedimentos de cópia de segurança *(backup)* e restauração de sistemas, aplicativos, dados e documentação em alinhamento com os requisitos de negócio e o plano de continuidade.".
3.3 ABNT NBR ISO/IEC 27002:2005, Código de prática para a gestão de segurança de informação.
4 CONCEITOS E DEFINIÇÕES
4.1 Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições:
a) banco de Dados (DB) - é o conjunto de programas de computador (*softwares*) responsáveis pelo gerenciamento de uma base de dados;
b) cópia de Segurança (backup) - É a cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados;
c) datacenter - É o local onde são concentrados os equipamentos de processamento e armazenamento de dados de uma empresa ou organização;
d) dados - Referem-se a uma escolha de informações organizadas, normalmente o resultado da experiência ou observação de outras informações dentro de um sistema de computador, ou um conjunto de instalações;
e) risco Rígido (HD) - Popularmente chamado também de *HD* (derivação de *HDD* do inglês *hard disk drive*) ou *winchester* (termo em desuso), "memória de massa" ou ainda de "memória secundária" é a parte do computador onde são armazenados os dados;
f) linux - Um termo popularmente utilizado para se referir sistemas operacionais que utilizem o núcleo Linux. O núcleo Linux foi desenvolvido pelo programador finlandês Linus Torvalds, inspirado no sistema Minix;
g) recursos Computacionais - Equipamentos, periféricos, dispositivos e consumíveis de informática, programas de computador de desenvolvimento próprio ou de terceiros, informações contidas nos bancos de dados deste Regional e nos seus equipamentos servidores de rede, acesso à Intranet, à Extranet e à Internet e aos demais serviços a elas relacionados;
h) sistema de Storage - Conjunto de discos rígidos para armazenamento de grandes quantidades de informações;
i) usuários - Todo aquele Magistrados, servidores ocupantes de cargo efetivo ou cargo em comissão, requisitados e cedidos, funcionários de empresas prestadoras de serviços terceirizados, consultores, estagiários, pensionistas, bem como Magistrados e servidores inativos que estão autorizados a obter acesso a informações e sistemas;
j) windows - É uma popular família de sistemas operacionais criados pela Microsoft, empresa fundada por Bill Gates e Paul Allen.
5 COMPETÊNCIA
5.1 Competência da Secretaria de Tecnologia da Informação
5.1.1 Compete à Secretaria de Tecnologia da Informação o gerenciamento das cópias de segurança dos sistemas, aplicativos, dados e documentos digitais pertencentes ao Tribunal Regional do Trabalho da 7ª Região em seus Recursos Computacionais referidos nesta Norma Complementar.
5.2 Competência da Divisão de Infraestrutura de TI
5.2.1 Compete à Divisão de Infraestrutura de TI a execução, recuperação, teste, documentação e guarda das cópias de segurança dos sistemas, aplicativos, dados e documentos digitais pertencentes ao Tribunal Regional do Trabalho da 7ª Região em seus Recursos Computacionais referidos nesta Norma Complementar.
6 RESPONSABILIDADES
6.1 Gerente de Continuidade
Cabe ao Gerente de Continuidade da Secretaria de Tecnologia da Informação:
a) identificar os sistemas informatizados que deverão possuir cópias de segurança;
b) consultar as instâncias superiores e definir a periodicidade das cópias a serem realizadas;
c) consultar as instâncias superiores e definir a criticidade e o tempo de retorno da informação.
6.2 Administrador da Ferramenta
Cabe ao Administrador da Ferramenta de *Backup*:
a) configurar a frequência e o tipo de cópia de segurança a serem realizados;
b) configurar o dispositivo de armazenamento de acordo com a criticidade da informação;
c) definir procedimentos para a recuperação de dados;
d) realizar testes periódicos de acordo com as especificações contidas nesse documento.
6.3 Operador da Ferramenta
Cabe ao Operador da Ferramenta de *Backup*:
a) verificar problemas na execução diária das cópias de segurança;
b) gerenciar as possíveis falhas na realização da cópia de dados;
c) enviar as fitas de Disaster Recovery para o cofre;
d) trazer do cofre as fitas limpas a serem utilizadas em novas cópias de segurança;
e) realizar operações de recuperação de dados;
f) auxiliar o administrador na realização dos testes periódicos.

Fonte: Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 1236, 31 mai. 2013.
Caderno Judiciário do Tribunal Regional do Trabalho da 7ª Região, p. 7.

6.4 O Diretor da Secretaria de tecnologia da Informação através de Portaria indicará os servidores para as funções relacionadas acima e seus respectivos suplentes.

7 TIPOS DE CÓPIA DE SEGURANÇA

Existem três tipos de cópias de segurança, possibilitando a restauração dos dados:

a) cópias diárias - BACKUP;

b) cópias mensais e anuais - ARQUIVAMENTO;

c) cópias de todos os dados referentes às políticas (diária, mensal e anual) para armazenamento em cofre - FITAS DE COFRE.

8 TIPOS DE MÍDIA DE ARMAZENAMENTO

Existem dois tipo de Mídia de armazenamento:

a) disco Rígido (HD) em Sistema de Storage;

b) fitas.

9 TIPOS DE DADOS ARMAZENADOS

As rotinas de *backup* consistem na manutenção de cópias de segurança dos seguintes conteúdos:

a) arquivos de usuários armazenados na rede, tais como documentos do Word e planilhas do Excel;

b) *dump* dos bancos de dados das aplicações corporativas, tais como Oracle (SPT1, SPT2, etc), Caché (Mentorh), Postgres (PJe) e MySQL (Intranet, Site, etc);

c) *e-mails* armazenados no servidor de correio eletrônico, não contemplando as mensagens que tenham sido baixadas para a máquina do usuário por algum programa estilo Outlook;

d) máquinas virtuais, responsáveis pela disponibilização de serviços como PJe, Mentorh, SPT1, etc;

e) arquivos de configuração dos computadores servidores.

10 ESTRUTURAS DE *HARDWARE E SOFTWARE*

10.1 robô de backup IBM System Storage TS3310 com 2 drives e 29 slots para fitas LTO 3.

10.2 robô de backup IBM System Storage TS3200 com 2 drives e 44 slots para fitas LTO3.

10.3 servidor de backup com o Tivoli Storage Manager configurado.

10.4 Switches Fibre Channel Cisco MDS 9148 para interligar os robôs ao servidor de *backup*.

10.5 Rede Gigabit Ethernet.

10.6 Licenças do Software Tivoli Storage Manager.

11 ROTINAS DE ARMAZENAMENTO DE DADOS

11.1 *Backup* Diário:

a) servidores Windows:

- realizado de forma incremental, ou seja, somente os arquivos que sofreram modificação durante o dia são regravados na mídia de armazenamento,
- guardadas 2 versões dos arquivos modificados pelos usuários,
- versões antigas dos arquivos modificados são mantidas por 30 dias;
- uma vez que o arquivo tenha sido removido, apenas 1 versão do mesmo é armazenada,
- uma vez que o arquivo tenha sido removido, a última versão do mesmo é armazenada por 30 dias,
- o backup é efetuado de segunda a sexta-feira a partir das 18 horas;

b) servidores Linux:

- realizado de forma incremental, ou seja, somente os arquivos que sofreram modificação durante o dia são regravados na mídia de armazenamento,
- guardadas 2 versões dos arquivos modificados pelos usuários,
- versões antigas dos arquivos modificados são mantidas por 30 dias;
- uma vez que o arquivo tenha sido removido, apenas 1 versão do mesmo é armazenada,
- uma vez que o arquivo tenha sido removido, a última versão do mesmo é armazenada por 60 dias,
- o *backup* é efetuado de segunda a sexta-feira a partir das 19 horas;

c) servidores do Interior:

- realizado de forma incremental, ou seja, somente os arquivos que sofreram modificação durante o dia são regravados na mídia de armazenamento,
- guardadas 5 versões dos arquivos modificados pelos usuários,
- versões antigas dos arquivos modificados são mantidas por 30 dias;
- uma vez que o arquivo tenha sido removido, apenas 1 versões do mesmo são armazenadas,
- uma vez que o arquivo tenha sido removido, a última versão do mesmo é armazenada por 30 dias,
- o *backup* é efetuado de segunda a sexta-feira a partir das 16 horas;

d) servidores de Virtualização:

- realizado de forma incremental, ou seja, somente os arquivos que sofreram modificação durante o dia são regravados na mídia de armazenamento,
- guardada 1 versão dos arquivos modificados pelos usuários,
- uma vez que o arquivo tenha sido removido, nenhuma versão do mesmo é armazenadas,
- uma vez que o arquivo tenha sido removido, a última versão do mesmo é armazenada por 7 dias,
- o *backup* das máquinas mais críticas é efetuado de segunda a sexta-feira a partir das 17 horas;

e) servidores de Arquivos:

- realizado de forma incremental, ou seja, somente os arquivos que sofreram modificação durante o dia são regravados na mídia de armazenamento,
- guardadas 5 versões dos arquivos modificados pelos usuários,
- versões antigas dos arquivos modificados são mantidas por 30 dias,
- uma vez que o arquivo tenha sido removido, apenas 1 versões do mesmo são armazenadas,
- uma vez que o arquivo tenha sido removido, a última versão do mesmo é armazenada por 30 dias,
- o *backup* é efetuado de segunda a sexta-feira a partir das 20 horas;

f) servidores do Pje:
- realizado de forma incremental, ou seja, somente os arquivos que sofreram modificação durante o dia são regravados na mídia de armazenamento,
- guardadas 30 versões dos arquivos modificados pelos usuários,
- versões antigas dos arquivos modificados são mantidas por 30 dias,
- uma vez que o arquivo tenha sido removido, apenas 1 versões do mesmo são armazenadas,
- uma vez que o arquivo tenha sido removido, a última versão do mesmo é armazenada por 30 dias,
- o backup é efetuado de segunda a sexta-feira a partir das 0 horas;

g) servidor de e-mail:
- realizado de forma incremental, ou seja, somente os arquivos que sofreram modificação durante o dia são regravados na mídia de armazenamento,
- guardada 1 versão dos arquivos modificados pelos usuários,
- versões antigas dos arquivos modificados são mantidas por 7 dias,
- uma vez que o arquivo tenha sido removido, apenas 1 versões do mesmo são armazenadas,
- uma vez que o arquivo tenha sido removido, a última versão do mesmo é armazenada por 7 dias,
- o backup é efetuado de segunda a sexta-feira a partir das 3 horas;

h) servidores Oracle:
- realizado de forma incremental, ou seja, somente os arquivos que sofreram modificação durante o dia são regravados na mídia de armazenamento,
- guardada 1 versão dos arquivos modificados pelos usuários,
- versões antigas dos arquivos modificados são mantidas por 15 dias,
- uma vez que o arquivo tenha sido removido, apenas 1 versões do mesmo são armazenadas,
- uma vez que o arquivo tenha sido removido, a última versão do mesmo é armazenada por 15 dias,
- o *backup* é efetuado de segunda a sexta-feira a partir das 4 horas,

i) servidor do Mentorh:
- realizado de forma incremental, ou seja, somente os arquivos que sofreram modificação durante o dia são regravados na mídia de armazenamento,
- guardadas 7 versões dos arquivos modificados pelos usuários,
- versões antigas dos arquivos modificados são mantidas por 30 dias,
- uma vez que o arquivo tenha sido removido, apenas 1 versões do mesmo são armazenadas,
- uma vez que o arquivo tenha sido removido, a última versão do mesmo é armazenada por 30 dias,
- o backup é efetuado de segunda a sexta-feira a partir das 3:30 horas;

11.2 *Backup* Semanal:
a) servidores de Virtualização:
- realizado de forma incremental, ou seja, somente os arquivos que sofreram modificação durante o dia são regravados na mídia de armazenamento,
- guardada 1 versão dos arquivos modificados pelos usuários,
- uma vez que o arquivo tenha sido removido, nenhuma versão do mesmo é armazenadas,
- uma vez que o arquivo tenha sido removido, a última versão do mesmo é armazenada por 7 dias,
- o backup das máquinas virtuais consideradas como não críticas é realizado no sábado a partir das 8:30 horas;

11.3 Arquivamento Mensal:
a) servidores Oracle:
- o arquivamento mensal é armazenado por 365 dias,
- o arquivamento é executado todo o dia 1º entre os meses de fevereiro e dezembro a partir das 4 horas;

b) servidores Pje:
- o arquivamento mensal é armazenado por 365 dias,
- o arquivamento é executado todo o dia 1º entre os meses de fevereiro e dezembro a partir de 1 hora;

c) servidor Mentorh:
- o arquivamento mensal é armazenado por 5 anos,
- o arquivamento é executado todo o dia 1º entre os meses de fevereiro e dezembro a partir de 4 horas;

11.4. Arquivamento Anual:
a) servidores Oracle:
-o arquivamento anual é armazenado por 5 anos,
-o arquivamento é executado todo o dia 1º de janeiro a partir das 4 horas;

b) servidores Pje:
-o arquivamento anual é armazenado por 5 anos,
- o arquivamento é executado todo o dia 1º de janeiro a partir de 1 hora;

c) servidor Mentorh:
- o arquivamento mensal é armazenado por 5 anos,
- o arquivamento é executado todo o dia 1º de janeiro a partir de 4 horas.

12 ROTINA DE RESTAURAÇÃO DE CÓPIA DE SEGURANÇA
12.1 As cópias de segurança serão restauradas de acordo com a demanda dos usuários. O usuário poderá solicitar a recuperação das informações que sejam de sua propriedade. Para requerer a recuperação de dados, o usuário deverá abrir uma solicitação através da Central de Serviços de TI.
13 ARMAZENAMENTO DAS CÓPIAS DE SEGURANÇA
As cópias de segurança tipo Off-site deverão ficar acondicionadas no cofre de mídia, garantindo assim sua integridade física.
14 TESTE DE CÓPIA DE SEGURANÇA
14.1 Todas as cópias de segurança deverão ser testadas periodicamente, de acordo com a Tabela de Testes de Segurança, Anexo XI.

14.2 O procedimento deverá garantir que o respectivo conteúdo seja recuperado em sua totalidade e de maneira íntegra.
14.3 As informações recuperadas deverão ser validadas de modo a garantir que as mesmas estejam em conformidade para eventuais processos de recuperação.
14.4 Os procedimentos específicos de cada tipo de informação para validação das informações recuperadas a partir do backup serão definidas em documentação complementar.
15 REGISTRO E DOCUMENTAÇÃO DAS CÓPIAS DE SEGURANÇA
Deverá ser mantido registro eletrônico das operações de cópia de segurança atualizado para fins de auditoria.
16 VIGÊNCIA
Esta Norma Complementar entra em vigor na data de sua publicação.
17 ANEXO
I - TABELA DE SERVIDORES WINDOWS;
II - TABELA DE SERVIDORES LINUX;
III - TABELA DE SERVIDORES DO INTERIOR
IV - TABELA DE SERVIDORES DE VIRTUALIZAÇÃO
V - TABELA DE SERVIDORES DE ARQUIVOS
VI - TABELA DE SERVIDORES DO PJe
VII - TABELA DE SERVIDORES DE e-mail
VIII - TABELA DE SERVIDORES ORACLE
IX - TABELA DO SERVIDOR DO MENTORH
X - TAREFAS ADMINISTRATIVAS
XI - TABELA DE TESTE DE CÓPIA DE SEGURANÇA

ANEXO I
TABELA DE SERVIDORES WINDOWS

Cliente	Função	Áreas Copiadas
DMZSRV03	Portal do Servidor	DMZSRV03\SystemState\NULL\System State\SystemState ASR \\dmzsrv03\d$
TRTSRV02	Controlador de Domínio e Servidor de Impressão	TRTSRV02\SystemState\NULL\System State\SystemState ASR \\trtsrv02\e$
TRTSRV04	Controlador de Domínio	TRTSRV04\SystemState\NULL\System State\SystemState ASR
TRTSRV08	Sistema de Rastreamento Jira	TRTSRV08\SystemState\NULL\System State\SystemState ASR \\trtsrv08\c$ \\trtsrv08\d$
TRTSRV30	Controlador de Domínio	TRTSRV30\SystemState\NULL\System State\SystemState ASR

ANEXO II
TABELA DE SERVIDORES LINUX

Cliente	Função	Áreas Copiadas
TRTBKP01	Servidor de Backup	/opt/tivoli/tsm /tsm/instance
TRTDNS01	Servidor DNS	/etc /var/named
TRTDNS02	Servidor DNS	/etc /var/named
TRTREPOSI-TORIO01	Servidor de Controle de Versões	/etc /backup
TRTSRV26	Intranet	/ (exceto /tmp, /sys, /proc, /root, /rpm64) /boot /home /opt /var/log
TRTSRV100	Wiki	/backup /etc /var/www
TRTWWW01	Site	/backup /etc /var/www

ANEXO III
TABELA DE SERVIDORES DO INTERIOR

Cliente	Função	Áreas Copiadas
ARASRV01	Controlador de Domínio e Servidor de Arquivos da Vara	ARASRV01\SystemState\NULL\System State\SystemState ASR \\arasrv01\e$
BATSRV01	Controlador de Domínio e Servidor de Arquivos da Vara	BATSRV01\SystemState\NULL\System State\SystemState ASR \\batsrv01\e$
CAUSRV01	Controlador de Domínio e Servidor de Arquivos da Vara	CAUSRV01\SystemState\NULL\System State\SystemState ASR \\causrv01\e$
CRASRV01	Controlador de Domínio e Servidor de Arquivos da Vara	CRASRV01\SystemState\NULL\System State\SystemState ASR \\crasrv01\e$
CTOSRV01	Controlador de Domínio e Servidor de Arquivos da Vara	CTOSRV01\SystemState\NULL\System State\SystemState ASR \\ctosrv01\e$
FRMSRV01	Controlador de Domínio e Servidor de Arquivos da Vara	\\frmsrv01\d$
FRMSRV02	Controlador de Domínio e Servidor de Arquivos da Vara	FRMSRV02\SystemState\NULL\System State\SystemState ASR
FRMSRV03	Controlador de Domínio e Servidor de Arquivos da Vara	FRMSRV03\SystemState\NULL\System State\SystemState ASR
IGUSRV01	Controlador de Domínio e Servidor de Arquivos da Vara	IGUSRV01\SystemState\NULL\System State\SystemState ASR \\igusrv01\e$
JUASRV01	Controlador de Domínio e Servidor de Arquivos da Vara	JUASRV01\SystemState\NULL\System State\SystemState ASR \\juasrv01\e$
LIMSRV01	Controlador de Domínio e Servidor de Arquivos da Vara	LIMSRV01\SystemState\NULL\System State\SystemState ASR \\limsrv01\e$
MGPSRV01	Controlador de Domínio e Servidor de Arquivos da Vara	MGPSRV01\SystemState\NULL\System State\SystemState ASR \\mgpsrv01\e$
PACSRV01	Controlador de Domínio e Servidor de Arquivos da Vara	PACSRV01\SystemState\NULL\System State\SystemState ASR \\pacsrv01\e$
QUISRV01	Controlador de Domínio e Servidor de Arquivos da Vara	QUISRV01\SystemState\NULL\System State\SystemState ASR \\quisrv01\e$
SOBSRV01	Controlador de Domínio e	SOBSRV01\SystemState\NULL\System

Fonte: Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 1236, 31 mai. 2013.
Caderno Judiciário do Tribunal Regional do Trabalho da 7ª Região, p. 7.

	Servidor de Arquivos da Vara	State\SystemState ASR \\sobsrv01\e$
TNGSRV01	Controlador de Domínio e Servidor de Arquivos da Vara	TNGSRV01\SystemState\NULL\System State\SystemState ASR \\tngsrv01\e$

ANEXO IV

TABELA DE SERVIDORES DE VIRTUALIZAÇÃO

Cliente	Função	Áreas Copiadas
TRTHVM03	Servidor de Máquinas Virtuais	Imagem das máquinas virtuais
TRTHVM04	Servidor de Máquinas Virtuais	Imagem das máquinas virtuais
TRTHVM06	Servidor de Máquinas Virtuais	Imagem das máquinas virtuais
TRTHVM08	Servidor de Máquinas Virtuais	Imagem das máquinas virtuais

ANEXO V
TABELA DE SERVIDORES DE ARQUIVOS

Cliente	Função	Áreas Copiadas
TRTSRV05	Servidor de Arquivos	TRTSRV05\SystemState\NULL\System State\SystemState \\trtsrv05\c$ \\trtsrv05\d$ \\trtsrv05\j$
TRTSRV07	Servidor de Arquivos para as Aplicações Corporativas	ASR SYSTEM STATE \\trtsrv07\f$ \\trtsrv07\i$ \\trtsrv07\k$

ANEXO VI
TABELA DE SERVIDORES DO PJe

Cliente	Função	Áreas Copiadas
TRTPJA01	PJe – JBoss do 1º Grau	/etc /srv
TRTPJA02	PJe – JBoss do 2º Grau	/etc /srv
TRTPJB01	PJe – Postgres do 1º Grau	/etc /var/lib/pgsql/backup
TRTPJB01	PJe – Postgres do 2º Grau	/etc /var/lib/pgsql/backup
TRTPJW01	PJe – Proxy Apache Externo	/etc
TRTPJW02	PJe – Proxy Apache Interno	/etc

ANEXO VII

TABELA DE SERVIDORES DE EMAIL

O backup do servidor de e-mail é realizado no TRTVMA01, apesar do servidor de e-mail em si ser o TRTSRV01.

Cliente	Função	Áreas Copiadas
TRTVMA01	Proxy para backup do servidor de email	/NFS_TRT/

ANEXO VIII
TABELA DE SERVIDORES ORACLE

Cliente	Função	Áreas Copiadas
RAC-CE1P	Banco de Dados dos Sistemas Corporativos tais como SPT1 e SPT2	/etc (**) /u01/ (**) /u04/backup/rman/ (**) /u04/backup/bkp-desen/ (**) /u04/backup/dump (*)

ANEXO IX

TABELA DO SERVIDOR DO MENTORH

Cliente	Função	Áreas Copiadas
TRTSRV15	Sistema de RH Mentorh	TRTSRV15\SystemState\NULL\System State\SystemState ASR \\trtsrv15\c$ \\trtsrv15\d$ \\trtsrv15\e$

ANEXO X
TAREFAS ADMINISTRATIVAS

- Disaster Recovery – Copia os dados de backup para as fitas a serem levadas para o cofre. Realizado de domingo a sexta às 6 horas.
- Backup do Banco – Faz uma cópia do banco de dados do TSM para as fitas a serem levadas para o cofre. Realizado de domingo a sexta às 6 horas, imediatamente após o Disaster Recovery.
- Plano de Recuperação de Desastre– Gera o plano a ser utilizado para recuperação do ambiente após a ocorrência de um desastre. Realizado de domingo a sexta às 6 horas, imediatamente após o Disaster Recovery.
- Expiration – Remove do inventário do TSM os dados expirados. Realizado de segunda a sexta às 15 horas e sábado às 12 horas.
- Reclamation – Otimiza a utilização das fitas, consolidando os dados em menos volumes. Realizado de segunda a sexta às 15 horas e sábado às 12 horas, imediatamente após o Expiration.
- Deleta DB – Remove os backups antigos da base de dados do TSM. Realizado de segunda a sexta às 19 horas

ANEXO XI
TABELA DE TESTE DE CÓPIA DE SEGURANÇA

Cliente	Periodicidade
SERVIDORES WINDOWS	Trimestral
SERVIDORES LINUX	Trimestral
SERVIDORES DO INTERIOR	Trimestral
SERVIDORES DE VIRTUALIZAÇÃO	Trimestral
SERVIDORES DE ARQUIVOS	Trimestral
SERVIDORES DO PJe	Trimestral
SERVIDORES DE EMAIL	Trimestral
SERVIDORES ORACLE	Trimestral
SERVIDOR DO MENTORH	Anual
RECUPERAÇÃO DO AMBIENTE	Anual