

DECRETO Nº 2932/2023, DE 03 DE JULHO DE 2023.

“DISPÕE SOBRE A INSTITUIÇÃO DA POLÍTICA DE CÓPIA DE SEGURANÇA E RESTAURAÇÃO DE DADOS DA PREFEITURA MUNICIPAL DE TARUMÃ, E DÁ OUTRAS PROVIDÊNCIAS”.

OSCAR GOZZI, PREFEITO MUNICIPAL DE TARUMÃ, DO ESTADO DE SÃO PAULO, NO USO DE SUAS ATRIBUIÇÕES LEGAIS,

CONSIDERANDO o Decreto Municipal nº. 1.792/2017, de 19 de junho de 2017, que dispõe sobre a Política de Segurança da Informação – PSI – no âmbito da Prefeitura de Tarumã;

CONSIDERANDO o objetivo estratégico da municipalidade de prover soluções tecnológicas integradas, sustentáveis e estáveis, com foco na segurança da informação, na simplicidade e na necessidade dos usuários;

CONSIDERANDO a necessidade de minimizar os riscos e enfrentar ameaças associadas a perdas de dados, favorecendo a continuidade de trabalhos e a recuperação de desastres.

DECRETA:

Art. 1º. - Fica instituída a Política de Cópia de Segurança e Restauração de Dados da Prefeitura Municipal de Tarumã, na forma do Anexo I deste Decreto.

Art. 2º. - Este Decreto regerá o tema em consonância com o Decreto Municipal nº. 1.792/2017, de 19 de junho de 2017, que institui a Política de Segurança da Informação – PSI – no âmbito da Prefeitura de Tarumã.

Art. 3º. – As despesas decorrentes da execução do presente Decreto correrão por conta de verbas próprias já consignadas no orçamento vigente, suplementadas se necessário.

Art. 4º. - Este Decreto entrará em vigor na data de sua publicação.

Art. 5º. - Revogam-se as disposições em contrário.

Paço Municipal “Waldemar Schwarz”, em 03 de Julho de 2023, 33º. Ano da Emancipação Política e 31º. Ano da Instalação.

Oscar Gozzi
PREFEITO MUNICIPAL

Gleyson Ramos Guimarães Lima
SECRETÁRIO MUNICIPAL DE GOVERNO

Publicado no **Diário Oficial do Município de Tarumã**

Gleyson Ramos Guimarães Lima
SECRETÁRIO MUNICIPAL DE GOVERNO

ANEXO I
POLÍTICA DE CÓPIA DE SEGURANÇA E RESTAURAÇÃO DE DADOS

UGB Tecnologia da Informação

Política de Cópia de Segurança e Restauração de Dados

Prefeitura Municipal de Tarumã

SUMÁRIO

1. Objetivos	3
2. Definições	3
3. Responsabilidades e atribuições.....	5
4. Escopo do backup e sua formalização.....	6
5. Prazo de retenção	7
6. Procedimentos de backup.....	9
7. Procedimentos de restauração	11
8. Teste de confiança	11
9. Recuperação de desastres	12
10. Descarte de mídias	12
11. Tecnologia utilizada para Backup.....	13
12. Esquema de Backup utilizado	13
13. Disposições finais.....	14
14. Anexo	15
Figura 1: Esquema da estrutura de Backup.....	15
Figura 2: Gerenciador de Backup Bacula e Dashboard principal.....	16
Figura 3: Histórico de backups, com status	17
Figura 4: Clientes de Backup	18
Figura 5: Dashboard de estatísticas do Backup Principal.	19
Figura 6: Dashboard backup espelhos, com informações do programa Rsyn	20

1. Objetivos

Regulamentar a política de backup das informações eletrônicas no âmbito da Prefeitura Municipal de Tarumã, com o objetivo de estabelecer diretrizes para o processo de cópia e armazenamento dos dados sob a guarda do UGB Tecnologia da Informação, visando garantir a segurança, integridade e disponibilidade, em conformidade com a Política de Segurança da Informação instituída por meio do Decreto Municipal Nº. 1792 de 19 de junho de 2017.

2. Definições

Administrador de Backup: servidor devidamente qualificado responsável pelos procedimentos de configuração, execução, monitoramento e testes dos procedimentos de backup e restauração.

Backup Completo (full): Modalidade de backup na qual os dados são copiados em sua totalidade.

Backup Diferencial: Modalidade de backup na qual somente os arquivos novos ou modificados desde o último backup completo são copiados.

Backup Incremental: Modalidade de backup na qual somente os arquivos novos ou modificados desde o último backup, seja ele completo, diferencial ou incremental.

Backup de primeiro nível: Armazenamento do backup em disco local.

Backup de segundo nível: Armazenamento do backup em mídia externa.

Backup off-site: Estratégia de backup que abrange a replicação de dados do backup

em um local geograficamente separado do local dos sistemas de produção.

Clientes de Backup: Equipamento do tipo servidor que esteja devidamente acondicionado em ambiente controlado no qual é instalado o agente de backup.

Recuperação de Desastre: Estratégia de recuperação de dados motivada por eventos de grave amplitude física ou lógica.

Mídia: Meio físico ou virtual no qual efetivamente armazenam-se os dados de um backup.

LTO¹: Tecnologia utilizada para armazenamento em fita magnética. O modelo utilizado pelo UGB Tecnologia da Informação é o LTO versão 6 (LTO6), com capacidades de armazenamento de até 2.35 Terabytes nativos.

Retenção: Período de tempo em que o conteúdo da mídia de backup deve ser preservado.

Objeto: Qualquer dado possível de backup e restauração.

Objeto Multimídia: qualquer dado do tipo áudio, vídeo, imagens.

Tarefa de backup (job): Mecanismo que é executado sob demanda ou de acordo com um agendamento e vincula um ou mais objetos a uma modalidade de backup e um período de retenção.

Storage: Dispositivo de armazenamento de alta disponibilidade e grande capacidade.

CETEC: Centro de Tecnologia da Informação. Próprio municipal que concentra à

¹https://en.wikipedia.org/wiki/Linear_Tape-Open#cite_note-lto6pressrelease-21

estrutura principal do Município de Tarumã.

3. Responsabilidades e atribuições

A UGB Tecnologia da Informação será o Administrador de Backup, ficando responsável pela política e procedimentos relativos aos serviços de backups e restauração, bem como de guardar as mídias móveis e assegurar o cumprimento das normas aplicáveis.

As atribuições do Administrador de Backup incluem:

- propor modificações visando o aperfeiçoamento da política de backup;
- criar e manter as tarefas de backup;
- configurar a ferramenta de backup e os clientes;
- criar e manter mídias;
- testar o backup e a restauração;
- criar notificações e relatórios;
- verificar periodicamente os relatórios gerados pela ferramenta de backup;
- restaurar os backups em caso de necessidade;
- gerenciar mensagens e logs diários dos backups, fazendo o tratamento dos erros de forma que o procedimento de backup tenha sequência e os erros na sua execução sejam eliminados;
- fazer manutenções periódicas dos dispositivos de backup;
- fazer o carregamento das mídias necessárias para os backups programados;
- Administrar os erros e ocorrências nos backups;
- fazer o armazenamento das mídias de backup em local apropriado;

4. Escopo do backup e sua formalização

Todo e qualquer ativo tecnológico que armazene dados e que esteja sob responsabilidade do UGB Tecnologia da Informação, deverá ser considerado para avaliação de inclusão no processo de backup.

O responsável por cada recurso deverá definir quais diretórios e arquivos serão incluídos no backup, tendo como prioridade:

- arquivos de configuração de sistemas utilizados em servidores instalados no Centro de Tecnologia da Informação;
- arquivos de logs dos aplicativos, inclusive log da ferramenta de backup e restauração;
- informações e configurações de banco de dados;
- conteúdo de repositórios de dados associados a sistemas;
- arquivos institucionais de usuários, que estejam devidamente armazenados nos servidores;
- arquivos de aplicações desenvolvidas pela UGB Tecnologia da Informação ou quaisquer outros não descritos neste documento, mas que a perda de suas informações gere prejuízo a esta Instituição.
- O Administrador de Backup ao incluir um novo Cliente de Backup deverá definir quais diretórios e arquivos não serão incluídos na rotina, tendo como referência:
 1. arquivos do sistema operacional ou de aplicações que podem ser realocados através de uma nova instalação;
 2. arquivos temporários;
 3. Arquivos que não estejam dentro do escopo de aplicabilidade da instituição, por exemplo, arquivos particulares de usuários.

Para aplicativos e/ou Banco de Dados devem ser seguidas quando disponível, as

orientações e recomendações sugeridas pelo desenvolvedor e/ou fabricante.

Os procedimentos de backup deverão ser atualizados quando houver:

1. novas aplicações desenvolvidas;
2. novos locais de armazenamento de dados ou arquivos;
3. novas instalações de banco de dados;
4. novos aplicativos instalados;
5. outras informações que necessitem de proteção através de backups deverão ser informadas ao Administrador de Backup, através de ferramenta de controle de atendimentos técnicos.

Para a especificação de um backup, o Administrador deverá formalizar chamado técnico através da ferramenta de controle de atendimentos disponível no momento. O chamado deverá conter as informações relativas ao backup, tais como: identificação do servidor e dados a serem incluídos, com base no Escopo do Backup mencionado anteriormente.

Os procedimentos de backup deverão ser configurados na ferramenta de backup, seguindo as orientações do documento de solicitação de backup.

5. Prazo de retenção

O período de retenção baseia-se no método e capacidade do equipamento utilizado, observando-se os seguintes critérios:

1. diário: sete últimos dias;
2. semanal: trinta últimos dias;
3. mensal: noventa últimos dias;
4. semestral: permanente em fita magnética;
5. anual: permanente em fita magnética;

Expirado o prazo de retenção dos dados armazenados, a mídia poderá ser reutilizada ou destruída, observando sempre seu estado de utilização. No caso de mídias do tipo fita magnética o prazo de armazenamento é de 30 anos, devendo, após esse período, ser copiada para outra mídia, destruída de forma segura e descartada em lugar destinado para tal, obedecendo às leis ambientais em vigência.

Sempre que necessário deverá ser realizada a atualização das mídias de backup, no caso de fitas magnéticas, com a finalidade de preservar o acesso aos dados nelas armazenados.

Deve-se salientar que qualquer estrutura de Backup se torna por natureza totalmente dependente da capacidade dos equipamentos, como tamanho do hardware de armazenamento, tamanho da unidade de Fita Magnética LTO, quantidade de objetos inseridos ou removidos nos Clientes de Backup.

Quanto mais objetos são inseridos na rede pelos usuários, mais ciclos de expansão (upgrades) no hardware de armazenamento torna-se necessário, juntamente com a expansão dos hardwares de backup off-site que também sofreram com a demanda por mais espaço de armazenamento, pois devem refletir o tamanho do storage do Backup principal.

O uso consciente dos recursos por parte de usuários, empresas proprietárias de softwares de gestão, equipe técnica do CETEC, é de total importância para o correto funcionamento da estrutura de Backup. Inserções de objetos em grandes quantidades fora do padrão diário de usabilidade dos Clientes de Backup sem que o Administrador de Backup tenha conhecimento, poderá exceder a capacidade dos equipamentos de Backup impossibilitando assim a execução e finalização sem erros de qualquer tarefa de backup.

Portanto, caso exista a demanda por uma grande inserção de informações nos Clientes de Backup o Administrador de Backup deverá realizar uma nova análise sobre o impacto dessas informações em relação ao funcionamento de toda a estrutura de Backup,

podendo ocorrer a necessidade de novos upgrades no(s) storage(s) de armazenamento.

Para backups contendo objetos do tipo multimídia, os mesmos não fazem parte das regras de backup diário, semanal e mensal do software central de Backup Bacula. Estes objetos são sincronizados via software Rsync diariamente com os espelhos de Backup. Tal rotina garante uma réplica diária de todos os objetos deste tipo. Uma cópia completa desses objetos é feita semestralmente em fita magnética. Objetos do tipo multimídia não são passíveis de compactação e demandam muito espaço e tempo extra para conclusão das tarefas, conflitando com as outras tarefas de backup padrões.

6. Procedimentos de backup

A criação e orquestração dos backups deverão obedecer às seguintes diretrizes:

1. Criação de backups:

1. O backup deverá ser programado para execução automática em horários de menor utilização dos sistemas.
2. O backup deverá ter uma rede dedicada de comunicação entre os Clientes de Backup, para garantir maior rapidez na conclusão de cada tarefa.

2. Orquestração dos backups:

1. o backup deverá ser monitorado pelo Administrador de Backup;
2. Para todos os backups realizados, deve ser gerado um relatório automatizado através da própria ferramenta de backup. O relatório deverá ser analisado diariamente para verificar a sua integridade e conclusão das tarefas.
3. Para os backups que apresentam o status de falha, o Administrador de Backup deverá realizar a análise do motivo que gerou a falha, e caso necessite, documentar em ferramenta de chamado técnico, citando os Clientes de Backup e se houve ação corretiva adotada. Competirá ao Administrador de Backup tratar falhas detectadas no âmbito do ambiente de backup, em caso de erro por parte de softwares de

terceiros os mesmos deverão ser comunicados e o acesso liberado ao(s) recurso(s) para a coleta e armazenamento das informações.

O agendamento de cada backup deverá seguir a abordagem através do Esquema de Backup utilizado:

1. backups diários serão executados de segunda à sexta-feira, com início às 18h, em modo diferencial;
2. Os backups semanais serão executados nos finais de semana, iniciando às sextas-feiras, em modo full. Não haverá execução do backup semanal quando coincidir com o backup mensal;
3. Os backups mensais serão executados na primeira sexta-feira do mês, em modo full. Não haverá execução do backup mensal quando coincidir com o backup semanal.
4. Backups semestrais e anuais serão feitos em unidades de fita magnética nos meses de Janeiro e Dezembro, no modo full.
5. Em caso de falha em algum procedimento de backup ou impossibilidade da sua execução, o Administrador de Backup deverá adotar as providências necessárias para promover a integridade das informações através de ações, como por exemplo, nova execução do backup em horário comercial ou cópia dos dados para outro servidor.
6. Cada backup feito entre servidor de backup central e seus clientes, ocorre dentro do próprio CETEC (Centro de Tecnologia da Informação) com comunicação ponto a ponto.
7. A replicação dos espelhos ocorre com o mesmo padrão do backup central, porém com uma cópia extra do backup central no formato binário nos servidores espelhos de backup.
8. Backup off-site dos espelhos feito através de um link direto de fibra ótica com o Backup central, tanto origem quanto destino estão geograficamente separados.

7. Procedimentos de restauração

A recuperação de backups deverá obedecer às seguintes orientações:

1. A solicitação de recuperação de objetos deverá sempre partir do responsável pelo recurso, através de chamado técnico, utilizando o software de controle de atendimentos para suporte ao usuário que estiver em execução no momento.
2. O chamado técnico deve conter, ao menos, o nome do setor do usuário, o(s) objeto(s) a ser(em) recuperado(s) juntamente com a localização onde se encontra(m), a data da versão que deseja recuperar, e a justificativa para a recuperação. Em caso do usuário não lembrar do último momento que tenha acessado o objeto, uma busca será feita nos demais backups dentro da janela de recuperação.
3. O chamado será encaminhado para o Administrador de Backup, que após a conclusão da tarefa, realizará a validação e confirmação com o usuário, realizando ao término o fechamento do chamado indicando a restauração do(s) objeto(s).
4. É de total importância que a restauração de objetos somente será possível nos casos em que este tenha sido adicionado às políticas e regras de backups, conforme a estratégia adotada.

8. Teste de confiança

Os backups mensais e semestrais deverão ser testados quanto à integridade e recuperabilidade dos objetos, de maneira amostral, no prazo máximo de uma semana após a sua execução.

Caso seja detectada falha no backup ou se o mesmo estiver incompleto, um novo backup deverá ser feito considerando as falhas ocorridas.

Para todos os testes realizados deverá ser gerado um relatório que ficará sob

responsabilidade do UGB Tecnologia da Informação.

9. Recuperação de desastres

As cópias do tipo recuperação de Desastres serão feitas com base na replicação das mídias do backup semanal e mensal e serão armazenadas em outro servidor de mesma capacidade remotamente, garantindo a replicação diária da estrutura principal de backup.

As mídias de recuperação de desastres serão replicadas diariamente após a conclusão das tarefas do Backup principal, tendo o mesmo período de retenção do Backup primário.

Quaisquer procedimentos programados nos equipamentos Clientes de Backup que impliquem riscos ao seu funcionamento ou em quaisquer dispositivos de armazenamento da estrutura de Backup, somente deverão ser executados após a realização do backup dos dados referentes ao Cliente de Backup em processo de manutenção.

10. Descarte de mídias

O descarte de mídias de backup inservíveis ou inutilizáveis deverá ser feito pelo UGB Tecnologia da Informação mediante supervisão do Administrador de Backup.

As mídias de backup a serem descartadas deverão ser destruídas de forma a impedir a sua reutilização ou acesso indevido aos dados por pessoas não autorizadas conforme normas técnicas estipuladas na Política de Segurança da Informação.

11. Tecnologia utilizada para Backup

O(s) software(s) utilizado(s) para gestão dos backups adotados por esta instituição são:

1. Bacula² software de Backup e Recuperação de Dados:

1. Utilizado para padronização através de agentes de backup instalados em cada Cliente de Backup que estejam localizados em ambiente de execução controlado.
2. A origem do backup deve estar sempre on-line (24/7), protegido contra interrupções não programadas com o uso de No-break e Gerador, com capacidade para manter a estrutura em pleno funcionamento, impedindo quedas de energia e interrupção do meio físico de comunicação evitando possíveis falhas na execução dos backups.

2. Rsync³:

1. Replicação do Backup Central para os espelhos, e demais backups dos espelhos, feito através do software Rsync, com amplo uso por diversas instituições, garante uma ampla variedade de personalização na programação dos scripts de backup.
2. Scripts desenvolvidos pela equipe do UGB Tecnologia da Informação: rsync.sh, rsync_apps.sh, rsyncdb.sh, rsync_etc.sh, rsync_multimedia.sh, rsync_vms.sh

12. Esquema de Backup utilizado

O padrão utilizado é o GFS ⁴ (Grandfather-Father-Son), pois garante pools (esquemas) de backups diário, semanal e mensal.

²www.bacula.com

³rsync.samba.com

⁴<https://www.bacula.it/capitluo-iv-estrategias-de-backup-e-o-esquema-gfs/#:~:text=Grandfather%2DFather%2DSon%20Backup%20se,um%20semanal%20e%20outro%20mensal.>

13. Disposições finais

Esta política de backup será reavaliada sempre que surgirem novos requisitos tecnológicos, corporativos e/ou legais.

A implementação dessa política está sujeita a disponibilidade de recursos financeiros e humanos.

Esta política poderá ser complementada por normas e procedimentos específicos.

Casos excepcionais ou não previstos serão tratados pela UGB Tecnologia da Informação juntamente a Secretaria Municipal de Governo.

Um aspecto importante na estrutura e manutenção do backup, é a comunicação por parte de equipe técnica e prestadores de serviço de qual informação, recurso ou dados está sendo removido (não tem mais utilização) ou adicionado (arquivos, Banco de Dados) a estrutura de serviços do CETEC, sendo a não comunicação ao Administrador de Backup da nova origem de backup por parte de equipe técnica ou prestadores de serviço, o backup não será feito pois cada nova fonte de backup deve ser programado no backup Central e também nos espelhos.

14. Anexo

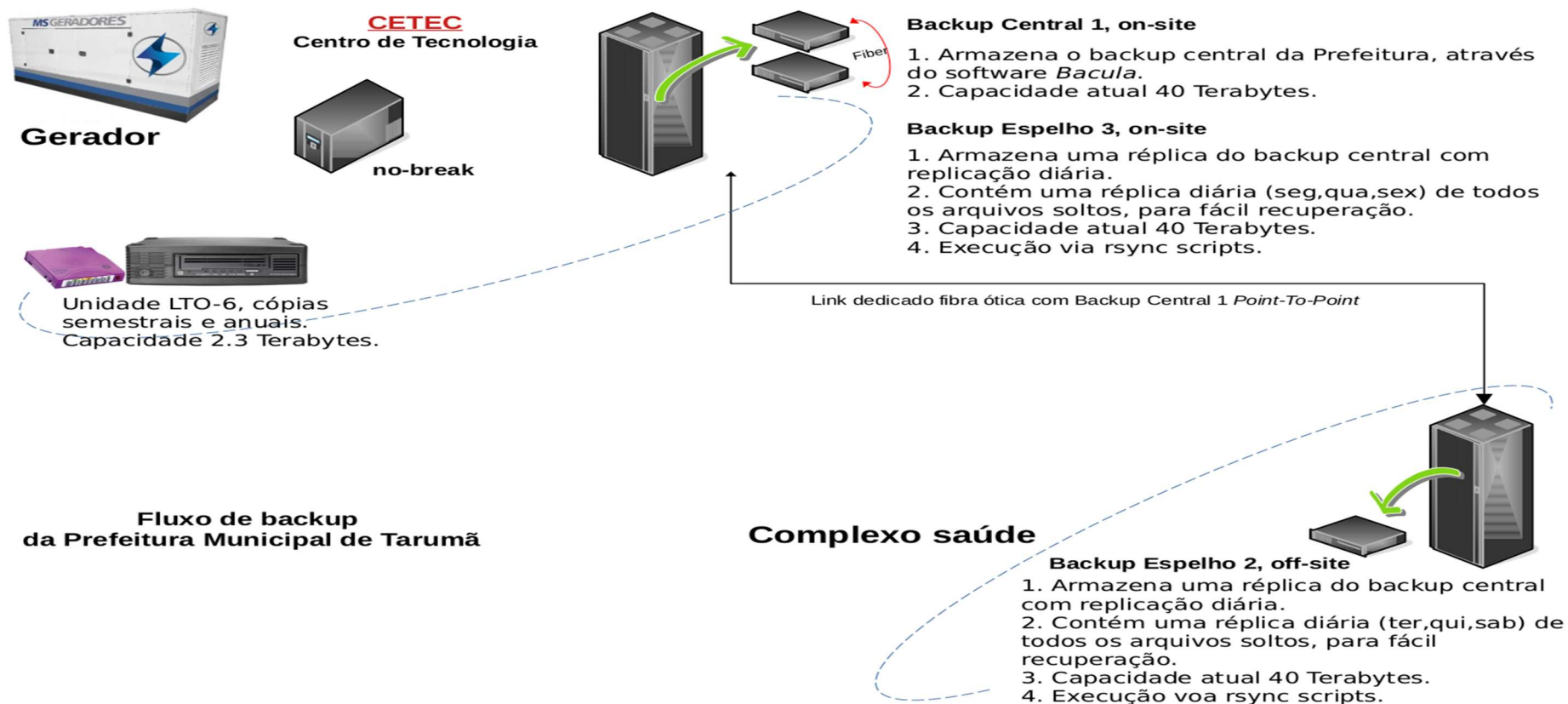


Figura 1: Esquema da estrutura de Backup.

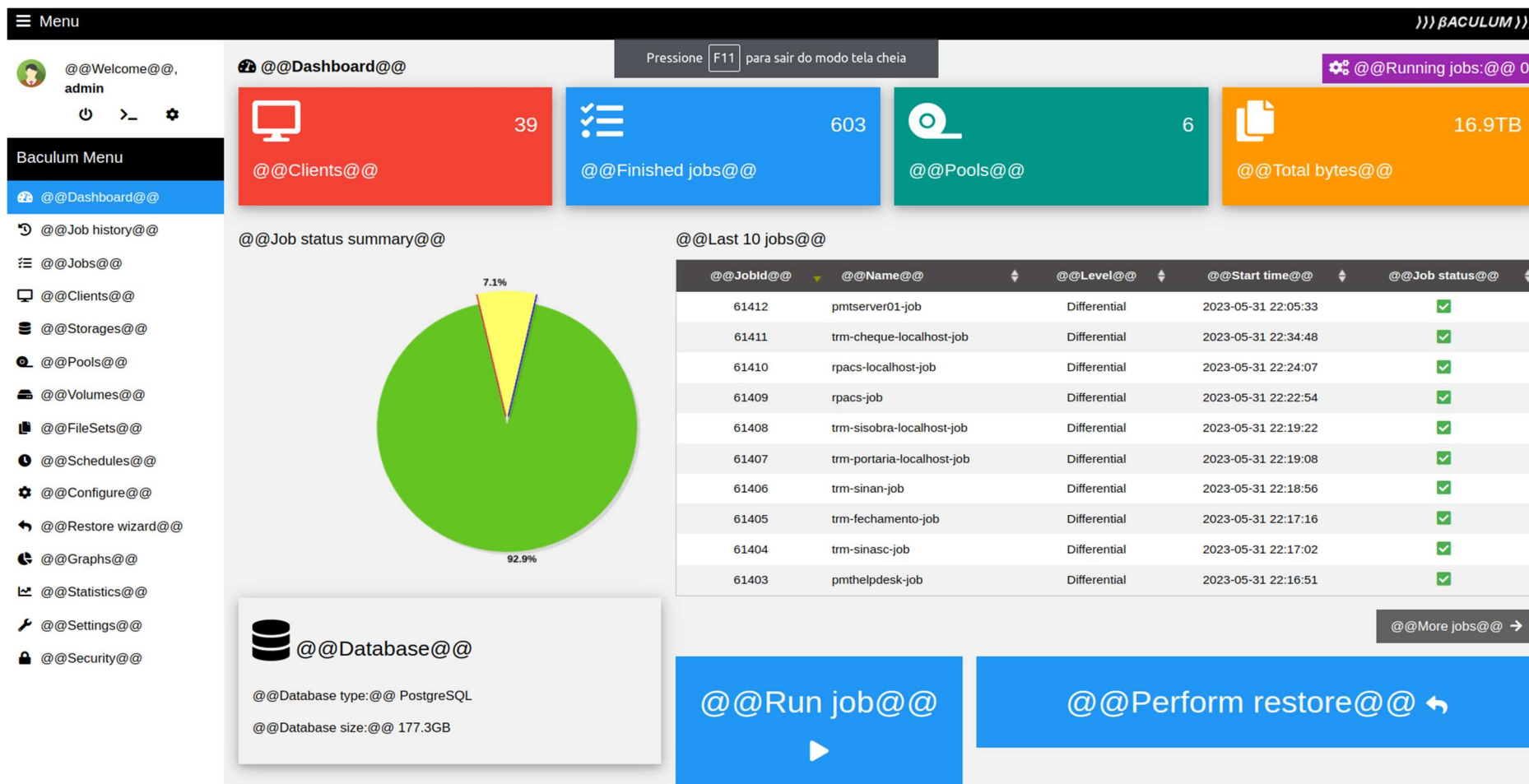


Figura 2: Gerenciador de Backup Bacula e Dashboard principal.

Menu

@@Welcome@@,
admin

Baculum Menu

@@Dashboard@@
@@Job history@@
@@Jobs@@
@@Clients@@
@@Storages@@
@@Pools@@
@@Volumes@@
@@FileSets@@
@@Schedules@@
@@Configure@@
@@Restore wizard@@
@@Graphs@@
@@Statistics@@
@@Settings@@
@@Security@@

@@Job history list@@

@@Add job@@

@@New job wizard@@

@@Run job@@

@@Running jobs@@ 0

Show 10 entries

Copy

CSV

Column visibility

Search:

@@JobId@@	@@Name@@	@@Type@@	@@Level@@	@@Start time@@	@@End time@@	@@Job status@@	@@Size@@	@@Files@@	@@Action@@
61412	pmtserver01-job	Backup	Differential	2023-05-31 22:05:33	2023-05-31 22:11:09	✓	4.2GB	5601	
61411	trm-cheque-localhost-job	Backup	Differential	2023-05-31 22:34:48	2023-05-31 22:34:59	✓	6.0MB	1	
61410	rpacs-localhost-job	Backup	Differential	2023-05-31 22:24:07	2023-05-31 22:34:47	✓	6.0GB	550	
61409	rpacs-job	Backup	Differential	2023-05-31 22:22:54	2023-05-31 22:24:06	✓	2.8kB	3	
61408	trm-sisobra-localhost-job	Backup	Differential	2023-05-31 22:19:22	2023-05-31 22:19:32	✓	0	0	
61407	trm-portaria-localhost-job	Backup	Differential	2023-05-31 22:19:08	2023-05-31 22:19:21	✓	136.0MB	7	
61406	trm-sinan-job	Backup	Differential	2023-05-31 22:18:56	2023-05-31 22:19:07	✓	33.2MB	6	
61405	trm-fechamento-job	Backup	Differential	2023-05-31 22:17:16	2023-05-31 22:18:55	✓	2.7GB	296	
61404	trm-sinasc-job	Backup	Differential	2023-05-31 22:17:02	2023-05-31 22:17:15	✓	181.7MB	12	
61403	pmthelpdesk-job	Backup	Differential	2023-05-31 22:16:51	2023-05-31 22:17:01	✓	0	0	

@@JobId@@

@@Start time@@

@@End time@@

@@Size@@

@@Files@@

@@Action@@

Showing 1 to 10 of 603 entries

Previous

1

2

3

4

5

...

61

Next

Figura 3: Histórico de backups, com status

17

Rua Aroeira, nº 482, Vila das Árvores - Tarumã-SP | CEP: 19820-000 | CNPJ: 64.614.449/0001-22
Fone/Fax: (18) 3373-4500 | site: www.taruma.sp.gov.br | e-mail: gabinete@taruma.sp.gov.br

Assinado por 2 pessoas: GLEYSON RAMOS GUIMARÃES LIMA e OSCAR GOZZI
Para verificar a validade das assinaturas, acesse <https://taruma.1doc.com.br/verificacao/E271-9D22-CCDD-D01A> e informe o código E271-9D22-CCDD-D01A

1D

Menu



@@Welcome@@,
admin





Baculum Menu

- @@Dashboard@@
- @@Job history@@
- @@Jobs@@
- @@Clients@@
- @@Storages@@
- @@Pools@@
- @@Volumes@@
- @@FileSets@@
- @@Schedules@@
- @@Configure@@
- @@Restore wizard@@
- @@Graphs@@
- @@Statistics@@
- @@Settings@@
- @@Security@@

@@Client list@@

+ @@Add client@@

Show 10 entries
Copy
CSV
Column visibility

Search:

Clientid	@@Name@@	@@Uname@@	@@AutoPrune@@
45	node2-fd	5.2.13 (19Jan13) x86_64-redhat-linux-gnu,redhat,(Core)	@@Yes@@
42	pmtbd01-fd	9.6.6 (20Sep20) Microsoft (build 9200), 64-bit,Cross-compile,Win64	@@Yes@@
16	pmtelpdesk-fd	9.6.5 (11Jun20) x86_64-pc-linux-gnu,debian,8.11	@@Yes@@
34	pmtserver-localhost-fd	9.6.5 (11Jun20) x86_64-pc-linux-gnu,debian,8.11	@@Yes@@
2	pmtserver01-fd	9.6.5 (11Jun20) x86_64-redhat-linux-gnu-bacula,redhat,(Core)	@@Yes@@
3	pmtserver02-fd	7.4.4 (202Sep16) x86_64-pc-linux-gnu,debian,9.13	@@Yes@@
5	pmtserver04-fd	5.0.0 (26Jan10) x86_64-redhat-linux-gnu,redhat,	@@Yes@@
9	pmtserver06-fd	5.2.6 (21Feb12) x86_64-pc-linux-gnu,debian,jessie/sid	@@Yes@@
7	pmtserver11-fd	5.2.6 (21Feb12) i486-pc-linux-gnu,debian,7.0	@@Yes@@
8	pmtserver12-fd	5.2.6 (21Feb12) i486-pc-linux-gnu,debian,7.0	@@Yes@@

Clientid

Showing 11 to 20 of 39 entries

Previous
1
2
3
4
Next

Figura 4: Clientes de Backup

18

Rua Aroeira, nº 482, Vila das Árvores - Tarumã-SP | CEP: 19820-000 | CNPJ: 64.614.449/0001-22
 Fone/Fax: (18) 3373-4500 | site: www.taruma.sp.gov.br | e-mail: gabinete@taruma.sp.gov.br

Assinado por 2 pessoas: GLEYSON RAMOS GUIMARÃES LIMA e OSCAR GOZZI
 Para verificar a validade das assinaturas, acesse <https://taruma.1doc.com.br/verificacao/E271-9D22-CCDD-D01A> e informe o código E271-9D22-CCDD-D01A



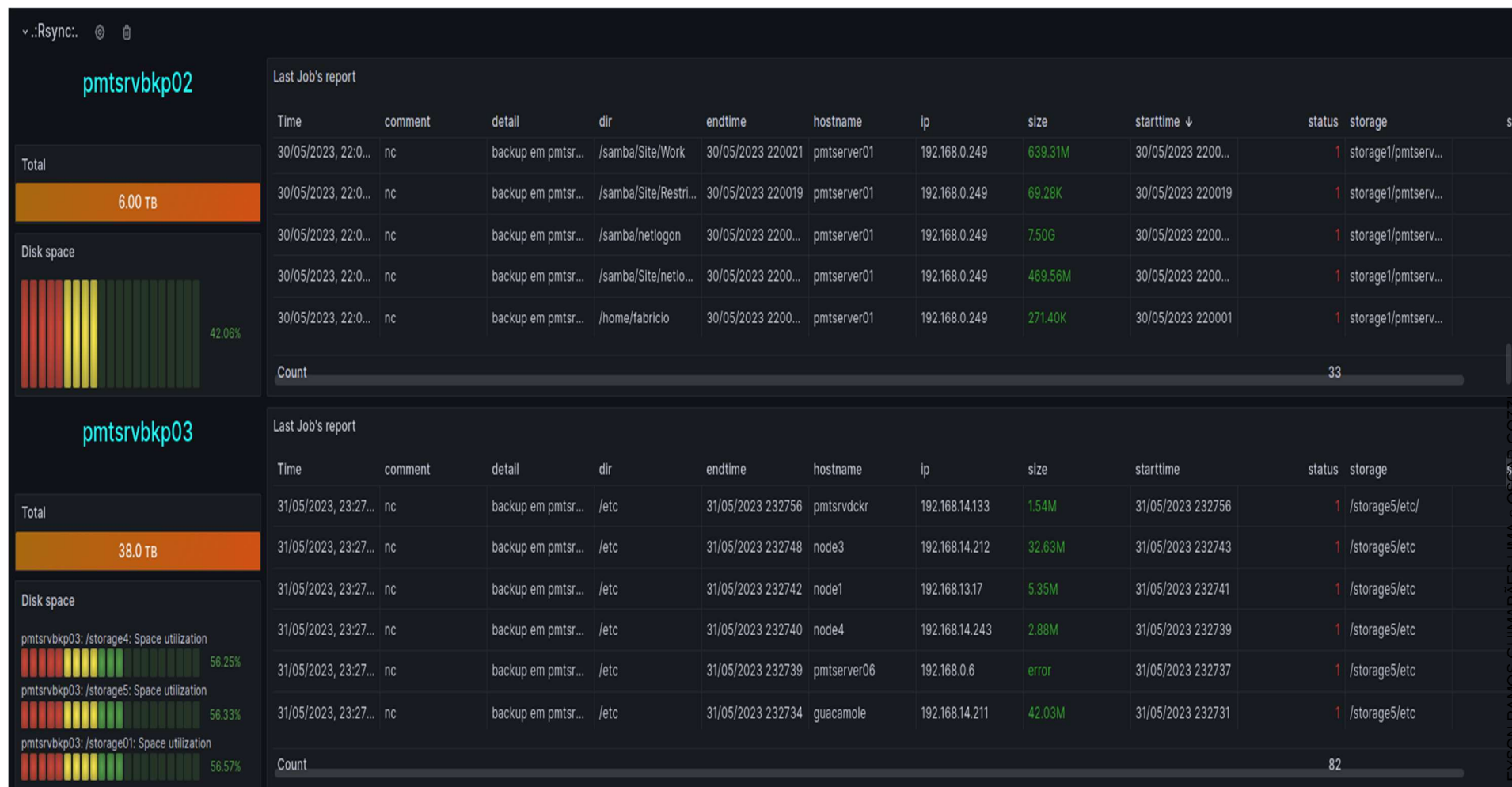


Figura 5: Dashboard de estatísticas do Backup Principal.

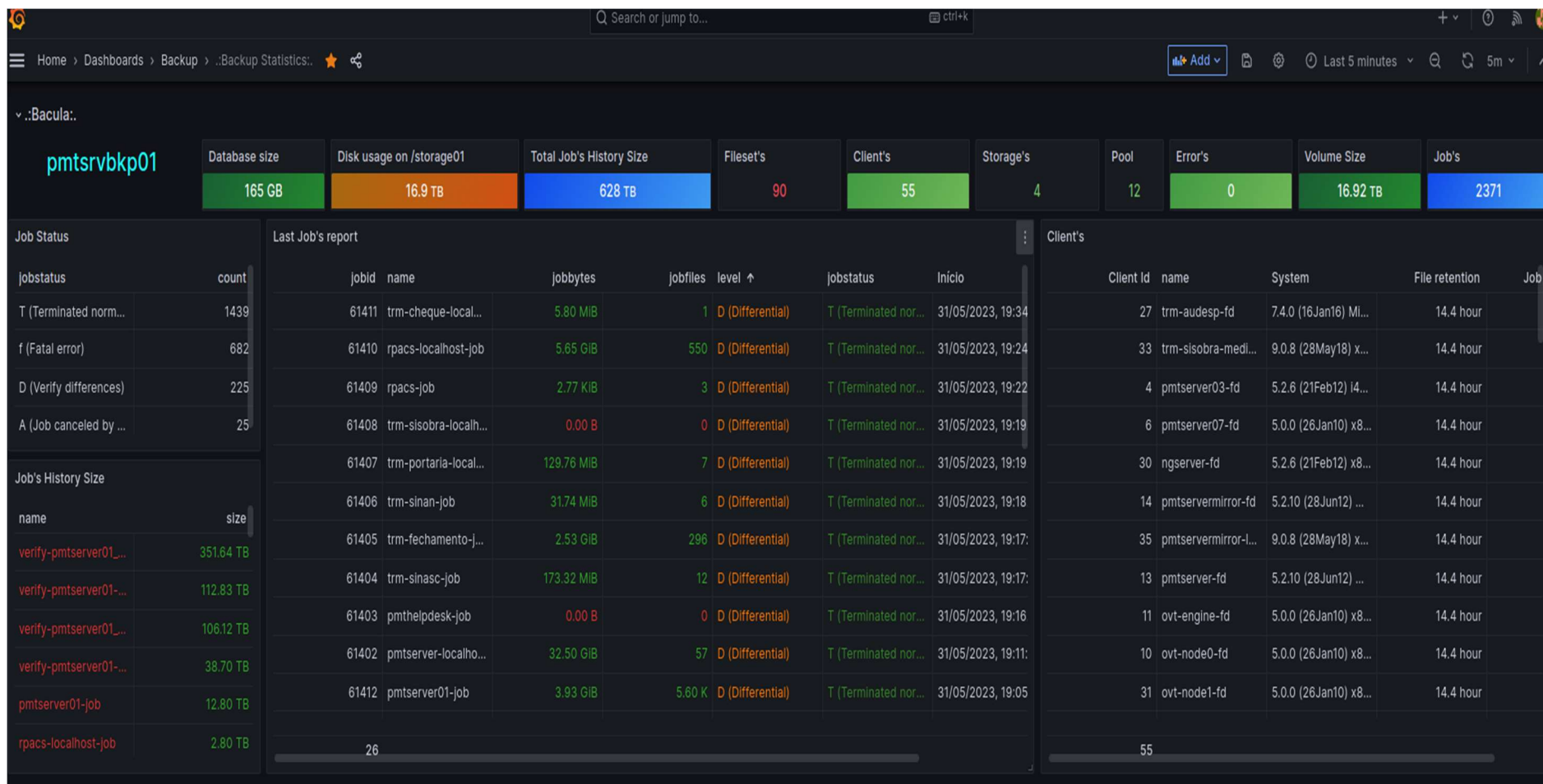


Figura 6: Dashboard backup espelhos, com informações do programa Rsync



VERIFICAÇÃO DAS ASSINATURAS



Código para verificação: E271-9D22-CCDD-D01A

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:



GLEYSON RAMOS GUIMARÃES LIMA (CPF 320.XXX.XXX-06) em 03/07/2023 11:37:59 (GMT-03:00)

Papel: Parte

Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)



OSCAR GOZZI (CPF 403.XXX.XXX-72) em 03/07/2023 19:28:46 (GMT-03:00)

Papel: Parte

Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

Para verificar a validade das assinaturas, acesse a Central de Verificação por meio do link:

<https://taruma.1doc.com.br/verificacao/E271-9D22-CCDD-D01A>