

POLÍTICAS GERAIS PARA GESTÃO DO BACKUP DE DADOS INSTITUCIONAL

(versão 1.2)

NOVEMBRO DE 2016



E-MAIL: drinfo@mpto.mp.br

TELEFONES: Chefia: (63) 3216 7630, Redes: (63) 3216 7561, Manutenção: (63) 3216 7681

Nós utilizamos sistema operacional Linux e suíte de escritório Libreoffice.org

Pág. 1/6

Sumário

1. RESUMO.....	3
2. INTRODUÇÃO.....	3
3. CONSIDERAÇÕES INICIAIS.....	3
4. ORIENTAÇÕES GERAIS.....	4
5. ESTRATÉGIA GERAL DE BACKUP.....	5
6. NECESSIDADES ESPECIAIS DE BACKUP (EXCEÇÃO).....	5
6.1. MÁQUINAS VIRTUAIS (IMAGEM).....	5
7. INFORMAÇÕES GERAIS.....	6



O Departamento de Modernização e Tecnologia da Informação (DMTI), departamento responsável pela normatização e padronização de procedimentos referentes à área de informática, define as políticas gerais para gestão do BACKUP de dados Institucionais.

1. RESUMO

Este documento estabelece normas, regras e procedimentos gerais quanto a política do BACKUP de dados Institucionais do MPETO.

2. INTRODUÇÃO

O presente documento estabelece uma política de cópias de segurança (backup) e restauração de arquivos digitais armazenados no parque tecnológico do Ministério Público do Tocantins, onde existir servidores de redes para centralização de dados, ou storages (unidade de armazenamento) ou unidades de fitas.

Os donos dos dados (servidores e membros) deverão ter ciência dos tempos de retenção aqui estabelecidos para cada tipo de informação e os administradores/operadores de backup (são todos os servidores da RTSI – Área de redes, telecomunicações e segurança da informação) deverão zelar pelo cumprimento das diretrizes aqui estabelecidas.

3. CONSIDERAÇÕES INICIAIS

O serviço de backup deve ser orientado para a restauração das informações no menor tempo possível, principalmente havendo indisponibilidade de serviços que dependam da operação de restore (restauração dos arquivos).

O Assessor Técnico de Tecnologia da Informação – Atuação em Redes e Segurança, é responsável por acompanhar e executar o cumprimento da Política de Backup, bem como sugerir melhorias ao mesmo, respondendo por omissão, caso descumpra as normas aqui relacionadas.



4. ORIENTAÇÕES GERAIS

Cabem aos administradores (todos os servidores da RTSI – Área de redes, telecomunicações e segurança da informação) prever a realização de testes periódicos de restauração, no intuito de averiguar os processos de backup e estabelecer melhorias, devendo este não ultrapassar o prazo máximo de seis meses.

Os administradores dos backups deverão respeitar as janelas para execução, inclusive realizando previsão para a ampliação da capacidade dos dispositivos envolvidos no armazenamento.

As mídias, quando for o caso, (ou dispositivos de armazenamento) deverão ser armazenados em cofre corta-fogo, ou em localidade diversa da origem dos dados (backup off-site).

As mídias/discos rígidos defeituosos ou inservíveis serão encaminhadas para picotamento, incineração, procedimentos de sobrescrita de dados remanescentes (disco rígido) ou outro procedimento que impossibilite a recuperação dos dados por terceiros.

As solicitações de restauração de arquivos deverão ser abertas formalmente através do sistema de abertura de chamados que se encontra na Intranet e deverá conter os nomes dos arquivos e pastas que deverão ser recuperados e, principalmente, a data do arquivo que se pretende ter acesso. As restaurações poderão ocorrer em horários diferenciados do expediente para que não comprometa a rede interna, e os arquivos deverão ser disponibilizado ao usuário final em até 4 dias úteis.

Os backups no prédio sede, será realizado em STORAGE, com redundância em outro equipamento, sendo de responsabilidade do Assessor Técnico de Tecnologia da Informação – Atuação em Redes e Segurança, fazer o dimensionamento adequado e as solicitações formais necessárias para a sua ampliação.



5. ESTRATÉGIA GERAL DE BACKUP

De acordo com a natureza dos dados trazemos a seguinte classificação:

1. Servidores de Arquivos;
2. Bancos de Dados;
3. Máquinas Virtuais (imagem);
4. Servidores de E-mail.

Por padrão será adotada o seguinte esquema de realização de backups, baseado no esquema GFS (Grandfather-Father-Son), onde deverá ser realizada uma política de backups full (**COMPLETO**) mensalmente e incremental diariamente. Sendo que os backups full terão seu período de retenção de 1 ano e os backups incrementais 30 dias:

	Backup Full	Qt. de retenções	Backup Incremental	Qt. de retenções
Serv. Arquivos	500 G	12	40 G	2
Serv. Arquivos CAOMA	155 G	12	5 G	2
BD	90 G	12	200 G	2
E-Mail	80 G	17	Ñ se aplica	-

No caso do servidor de e-mail, que não é possível a realização de backups incrementais, deverá ser mantido os 5 últimos backups full diários, mais um mensal, sendo que o mensal deverá ter a retenção de 1 ano.

6. NECESSIDADES ESPECIAIS DE BACKUP (EXCEÇÃO)

6.1. MÁQUINAS VIRTUAIS (IMAGEM)

O backup das máquinas virtuais como imagem (adequado para fins de



disaster recovery – ou seja: restauração da máquina como um todo), será feito apenas na seguinte periodicidade:

1. Backups completos (full – denominados semestral) na primeira sexta-feira do mês, realizados a partir das 20:00h., com um ano de retenção.

No mais, as Máquinas Virtuais serão tratadas como outras máquinas físicas, devendo o cliente de backup ser instalado em cada uma delas.

7. INFORMAÇÕES GERAIS

Não deverá ser realizado backup de arquivos ou documentos que não sejam de interesse da administração, ou que sejam de cunho pessoal do membro ou servidor, como: músicas; vídeos e fotos pessoais e familiares; apostilas, vídeos e áudios de concursos; jogos; pornografias; contas pessoais; dentre outros do gênero. Caso seja identificado qualquer um desses itens, o Chefe do DMTI deverá ser informado formalmente para tomar as medidas necessárias, junto ao chefe imediato do servidor ou junto a Diretoria-Geral ou Chefe de Gabinete.

As informações aqui contidas serão complementadas pelo ATO nº 72/2011, ou o que o substituí-lo ou vier a complementá-lo, no que se refere a backup e segurança da informação.

Huan Carlos Borges Tavares

Chefe do Departamento de Modernização e Tecnologia da Informação

