Manual de

Controle de Cópia de Segurança da Informação

MTPrev

GOVERNO DO ESTADO DE MATO GROSSO

Mauro Mendes – Governador

MATO GROSSO PREVIDÊNCIA - MTPREV

Elliton Oliveira de Souza – Diretor Presidente

DIRETORIA DE ADMINISTRAÇÃO SISTÊMICA

Paola Correia Sanches – Diretora Administrativa

COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO

Flávio Lopes da Silva – Coordenador

Cuiabá-MT

SUMÁRIO

APRESENTAÇÃO

O presente documento tem como escopo atender os objetivos estratégicos do Plano de Desenvolvimento Institucional – PDI, determinar o uso responsável de conteúdos disponíveis na internet pelas unidades administrativas do MTPrev, estabelecer controles de segurança e agregar valor às unidades administrativas devido a disponibilidade, confiabilidade e a segurança na internet.

A Coordenadoria de Tecnologia da Informação (CTI) é parte integrante da estrutura organizacional do Mato Grosso Previdência - MTPrev, instituído pela Lei Complementar nº 560, de 31/12/2014 que ao dispor sobre a estrutura organizacional desta Autarquia estabeleceu ao Setor de Tecnologia da Informação compete:

I. Realizar estudos e pesquisas, emitir pareceres e laudos técnicos e consolidar informações na área de Tecnologia da Informação;
II. Garantir o funcionamento dos sistemas de informática;
III. Desenvolver e atualizar programas e sistemas em conjunto com o órgão competente do Poder Executivo, visando ao atendimento das necessidades da Autarquia;
IV. Analisar a viabilidade técnica e funcional para a elaboração de projetos referentes à contratação de serviços de informática e aquisição de equipamentos tecnológicos;
V. Gerenciar a manutenção e a segurança das informações, de servidores e de equipamentos da rede de computadores;
VI. Assessorar e treinar usuários de programas;
VII. Elaborar as diretrizes e ações relacionadas com a informatização dos processos, análise dos negócios, organização das informações, gestão de contratos e

recursos de informática, assim como pela normatização das políticas de informática;

VIII. Gerir o acesso aos usuários dos sistemas;

IX. Viabilizar a manutenção do ambiente operacional, prestando atendimento e orientação técnica aos usuários e corpo técnico, assim como a implementação da infraestrutura, especificação e manutenção do parque tecnológico e da padronização de softwares

X. Prover ampla divulgação da Política e das Normas de Segurança da Informação para todos os servidores e prestadores de serviços;

XI. Promover ações de conscientização sobre Segurança da Informação para os servidores e prestadores de serviços;

XII. Propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação;

XIII. Elaborar e manter política de classificação da informação, com temporalidade para guarda;

XIV. Adotar os procedimentos que garantam a segurança das informações por meio de rotinas de backups;

XV. Desenvolver outras atividades correlatas ou que lhe forem atribuídas.

No ambiente de Tecnologia da Informação, o backup e a proteção dos dados são utilizados para prover continuidade de negócios, replicação de dados, recuperação de desastres e redução nos custos de infraestrutura tecnológica. Porém, a melhor maneira para assegurar os dados, seja local ou remotamente, pode ser um desafio desanimador, se não forem estabelecidas normas estratégicas para este fim.

Para a proteção das informações e para atenderem a padrões de segurança e regulamentações governamentais, as organizações estabelecem um conjunto de Políticas de Segurança da Informação. Para auxiliar na elaboração de Políticas de Segurança da Informação existe a norma NBR ISO/IEC 27001:2006 homologada pela Associação Brasileira de Normas Técnicas, que é um conjunto de normas e padrões,

baseados em melhores práticas.

Mesmo estabelecendo políticas de segurança, as organizações não estão livres de erros humanos, ataques de vírus, catástrofes naturais, e outras ameaças. E caso ocorram perdas de informações é preciso recuperá-las, e isto se torna possível se o processo de backup e recuperação de dados for seguro.

DEFINIÇÕES

I. **Agente Público:** Toda e qualquer pessoa que exerce uma atribuição pública em sentido lato, seja estagiário, ocupante de função, cargo ou de emprego público.

II. **Prestador de Serviço:** Toda e qualquer pessoa que possui uma relação contratual com o MTPrev em período determinado.

III. **Usuário de TIC:** agente público ou prestador de serviço que fazem uso de serviço de TIC.

IV. **Dado:** Qualquer registro de conteúdo armazenado em meio magnético. Pode compreender software, dados propriamente ditos (arquivos, bancos de dados), conteúdo multimídia ou qualquer outro passível de armazenamento em meio magnético.

V. **Dado estruturado:** dado que passou por processo de modelagem; geralmente residente em tabelas componentes de bancos de dados ou arquivos acessados por aplicações.

VI. **Dado não estruturado:** documento, mensagens de correio eletrônico, conteúdo multimídia (imagem, vídeo, áudio) armazenado em formato digital. Em conjunto, têm como características grande volume, rápido crescimento e dificuldade de manipulação pelas ferramentas de gerenciamento de bancos de dados ou aplicações que processam arquivos de dados. Devido a estas características, são também conhecidos pela denominação de “Big Data”.

VII. **Backup:** Cópia de segurança gerada para possibilitar o acesso ou recuperação futura de dados existentes no Data Center contratado pelo MTPrev. O termo também pode ser associado ao processo de geração da cópia de segurança, acepção que tem no restore seu complemento (vide restore).

VIII. **Janela de Backup:** Período de tempo requerido para a geração do backup (total, diferencial ou incremental).

IX. **Mídia de Backup**: Suporte magnético ou óptico utilizado para armazenamento de dados. Dentre as mídias de backup destacam-se as fitas e cartuchos magnéticos e os discos ópticos.

X. **Restore**: Cópia eventual de dados armazenados em backup para um disco ou outra mídia através da qual podem ser acessados pelos usuários ou aplicações.

XI. **Servidor:** Computador responsável por gerenciar e oferecer serviços para uma rede de computadores clientes.

XII. **Storage**: Equipamento composto por conjuntos de discos magnéticos, especializado no armazenamento e disponibilização de grandes volumes de dados.

XIII. **Virtual Tape Library (VTL)**: Equipamento que simula uma tape library através da utilização de discos rígidos em lugar de mídias de backup convencionais, possibilitando otimização dos processos de backup e restore.

XIV. **Software de backup:** Conjunto de programas especializados no planejamento, identificação do backup, processamento e controle do backup de servidores, storage e demais dispositivos que armazenam dados.

OBJETIVO

Este documento tem por objetivo estabelecer uma política de backup de dados estruturados e não estruturados a fim de evitar que os arquivos sejam permanentemente perdidos ou danificados em caso de algum incidente, seja ele físico, lógico, ambiental, ou como na maioria dos casos, uma falha humana. Os arquivos de backup ajudam a evitar ou minimizar as perdas de trabalho executado caso algo indesejado aconteça, e por isso deve-se gerá-los regularmente.

Para que isto ocorra, utilizamos os recursos adequados para a geração de cópias de segurança para garantir que toda informação e sistemas essenciais possam ser recuperados após a perda de dados devida a desastres, erros, falhas de mídias ou outros fatores além de registrar informações completas e exatas das cópias de segurança em documentação apropriada.

Todas as aplicações corporativas ou setoriais devem armazenar os dados nos servidores de arquivos e nos servidores de bancos de dados, para os quais será assegurada a execução de rotina de backup, de acordo com esta política, entretanto, esta norma não se aplica aos backups de dados de dados locais, cabendo essa responsabilidade ao seu usuário de TIC.

A Empresa Mato-grossense de Tecnologia da Informação – MTI é a empresa responsável por assegurar a execução das rotinas de backup no âmbito do MT Prev através da determinação da Coordenadoria de Tecnologia da Informação – CTI do MT Prev.

PROCEDIMENTOS

A rotina de backup de dados estruturados compreende:

I. **Backup diário:** Processado de segunda a sexta-feira, com retenção dos últimos sete dias de backups;

II. **Backup semanal:** Backup diário processado às sextas-feiras, incluindo o backup diário com retenção de um mês;

III. **Backup mensal:** backup semanal processado na primeira sexta-feira do mês subsequente com retenção dos últimos doze meses;

IV. **Backup anual:** backup mensal processado na primeira sexta-feira do ano subsequente, com retenção dos últimos seis anos.

A rotina de backup de dados não estruturados compreende:

I. **Backup diário:** processado de segunda a sexta-feira, com retenção dos últimos trinta dias (dias corridos).

Ambiente de processamento de backup:

I. O backup deve ser processado em equipamento específico (Mídia de Backup / storage / servidor de backup / cloud datacenter), sob controle do software de backup homologado pela MTI.

II. Qualquer solicitação de serviços que envolva outros equipamentos, software de backup, local de armazenamento de mídias, alteração na frequência de geração ou no tempo de retenção do backup deverá ser analisada previamente pela CTI, quanto à sua viabilidade, em prazo negociado entre as partes.

III. O backup deverá ser processado, preferencialmente, durante a noite, em horário que gere menor impacto nas demais rotinas e serviços do Data Center do MTPrev.

IV. Os procedimentos de backup de servidores e storage hospedados na Empresa Mato-grossense de Tecnologia da Informação – MTI ou em outros sites serão de responsabilidade dessas entidades.

DISPOSIÇÕES FINAIS

Casos omissos a este documento devem ser tratados pelo setor responsável pela segurança da informação Coordenadoria de Tecnologia da Informação – CTI do Mato Grosso Previdência – MTPrev.

Não é dado ao Agente Público ou Prestador de Serviço o direito de alegar desconhecimento da presente norma.

O não cumprimento da presente norma acarretará ao Agente Público e Prestador de Serviço as penalidades cabíveis, previstas no âmbito administrativo, cível e criminal.

REFERÊNCIAS

I. Resolução Nº 003/2010 – Políticas e Diretrizes de Segurança da Informação Estadual.
II. Norma ABNT NBR ISO/IEC 27001: 2006 Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos.
III. Norma ABNT NBR ISO/IEC 17799: 2005 Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação.
IV. Resolução 001/2005-COSINT – Políticas e Diretrizes do Sistema Estadual de Informação.
V. Código Penal Brasileiro.