Política de Backup

PREFEITURA DO MUNICÍPIO DE MAUÁ

Sumário

Esclarecimentos

O presente documento estabelece uma política de cópias de segurança (backup) e restauração de arquivos digitais armazenados no parque tecnológico da Prefeitura do Município de Mauá.

Política de Backup e Restauração de Dados Digitais

Propósito

A Política de Backup e Restauração de Dados Digitais objetiva instituir diretrizes que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pelo GTI e formalmente definidos como de necessária salvaguarda na Prefeitura do Município de Mauá, para se manter a continuidade do negócio. No sentido de assegurar sua missão é fundamental estabelecer mecanismos que permitam a guarda dos dados e sua eventual restauração em casos de indisponibilidades ou perdas por erro humano, ataques, catástrofes naturais ou outras ameaças. O presente documento apresenta a Política de Backup e Restauração de Dados Digitais, onde se estabelece o modo e a periodicidade de cópia dos dados armazenados pelos sistemas computacionais.

Escopo

- Esta política se aplica aos seguintes dados da Prefeitura do Município de Mauá:
  Bancos de Dados;
  Servidor de Arquivos;
  Máquinas Virtuais (imagem).

Cada tópico acima citado tem suas características próprias de backup, que serão expostas neste documento.

- A política também se aplica a terceiros que acessam e usam na Prefeitura do Município de Mauá sistemas e equipamentos de TI ou que criam, processam ou armazenam dados de propriedade da Prefeitura do Município de Mauá.
- Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos fora dos centros de processamento de dados mantidos pelas unidades de TI do Paço, ficando sob a responsabilidade do indivíduo que usa o(s) dispositivo(s).
- Não serão salvaguardados nem recuperados dados de cunho pessoal, armazenados indevidamente na rede.
- A salvaguarda dos dados em formato digital pertencentes a serviços de TI da Prefeitura do Município de Mauá mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, deve estar garantida nos acordos ou contratos que formalizam a relação entre os envolvidos.

Termos e Definições

BACKUP OU CÓPIA DE SEGURANÇA - Conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

CUSTODIANTE DA INFORMAÇÃO - Qualquer indivíduo ou estrutura de órgão ou entidade da Administração Pública, direta e indireta, que tenha responsabilidade formal de proteger a informação e aplicar os níveis de controles de segurança em conformidade com as exigências de Segurança da Informação comunicadas pelo proprietário da informação;

ELIMINAÇÃO - Exclusão de dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

MÍDIA - Mecanismos em que dados podem ser armazenados. Além da forma e da tecnologia utilizada para a comunicação - inclui discos ópticos, magnéticos, CDs, fitas e papel, entre outros. Um recurso multimídia combina sons, imagens e vídeos;

INFRAESTRUTURA CRÍTICA – instalações, serviços, bens e sistemas, virtuais ou físicos, que se forem incapacitados, destruídos ou tiverem desempenho extremamente degradado, provocarão sério impacto social, econômico, político, internacional ou à segurança;

Declarações da política

Dos princípios gerais

1. As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.
2. As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.
3. As rotinas de backup devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado, dando prioridade aos serviços de TI críticos da organização.
4. O armazenamento de backup, se possível, deve ser realizado em um local distinto da infraestrutura crítica. É desejável que se tenha um sítio de backup em um local remoto ao da sede da organização para armazenar cópias extras dos principais backups, a exemplo dos backups de dados de serviços críticos.
5. Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup.
6. Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.

DA FREQUÊNCIA E RETENÇÃO DOS DADOS

7. Os backups dos serviços de TI da Prefeitura do Município de Mauá devem ser realizados utilizando-se as seguintes frequências temporais:

   I - Diária;

   II - Mensal;

   III - Anual.

8. Os serviços de T Ida Prefeitura do Município a retenção de dados estabelecida a seguir:

   I – Diária: 5 dias;

   II – Mensal: 12 meses;

   III – Anual: 5 anos.

9. A Salvaguarda dos dados referentes aos serviços de TI deve explicitar, no mínimo, os seguintes requisitos técnicos:

   I – Tipo de *backup*;

   II – Frequência temporal de realização do backup;

   III – Retenção;

TIPOS DE BACKUP

I – Completo (*full*);

II – Incremental;

Salvo indicação em contrário, o backup dos dados do sistema será feito de acordo com a seguinte programação padrão:

10. Backup full (aos sábados), armazenado no local e em fita magnética.
11. Backup incremental diário (segunda a quinta), armazenamento no local e em fita magnética.
12. Backup completo Mensal, armazenado externo.
13. Backup completo Anual, armazenado localmente.

CONFIGURAÇÃO DOS BACKUPS

Backup de Servidores (Máquinas Virtuais)

Tipo	Frequência	Período	Retenção
FULL	Semanalmente	Fim de Semana	6 dias
INCREMENTAL	uma vez ao dia, depois do horário de expediente.	Diariamente	5 dias
FULL	1 vez ao mês	Mensal	12 meses
FULL	1 vez ao ano	Anual	1 ano

Backup de Banco de Dados de Produção

Tipo	Frequência	Período	Retenção
FULL	1 vez ao dia	Diariamente	5 dias
FULL	1 vez ao mês	Mensal	12 meses
FULL	1 vez ao ano	Anual	1 ano

Servidor de Arquivos

Tipo	Frequência	Período	Retenção
FULL	Semanalmente	Fim de Semana	5 dias
INCREMENTAL	uma vez ao dia, depois do horário de expediente.	Diariamente	5 dias
FULL	1 vez ao mês	Mensal	12 meses
FULL	1 vez ao ano	Anual	1 ano

Do transporte e armazenamento

14. As unidades de armazenamento utilizadas na salvaguarda dos dados digitais devem considerar as seguintes características dos dados resguardados:

    I – A criticidade do dado salvaguardado;

    II – O tempo de retenção do dado;

    III – A probabilidade de necessidade de restauração;

    IV – O tempo esperado para restauração;

    V – O custo de aquisição da unidade de armazenamento de backup;

    VI – A vida útil da unidade de armazenamento de backup.

15. A equipe técnica deve identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso.
16. A execução das rotinas de backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.
17. As unidades de armazenamento dos backups devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade, temperatura, poeira e pressão, e com acesso restrito a pessoas autorizadas. Além disso, as condições de temperatura, umidade e pressão devem ser aquelas descritas pelo fabricante das unidades de armazenamento.
18. As fitas de backup devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência com etiquetas não manuscritas, dando uma conotação mais organizada e profissional.
19. Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.
20. Quando da necessidade de descarte de unidades de armazenamento de backups, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los.

As fitas de backup serão transportadas e armazenadas conforme descrito neste documento:

- A mídia será claramente identificada e armazenada em uma área segura, acessível apenas para pessoas autorizadas.
- A mídia não será deixada sem supervisão durante o transporte.
- Backups completos diários serão mantidos por 5 dias e armazenados no local em um cofre à prova de fogo fisicamente protegido.
- Backups completos semanais serão mantidos por um período de 5 dias, e guardado no cofre de armazenamento de mídia fisicamente protegido. Depois de 5 dias, as fitas serão reutilizadas ou destruídas.
- Backups completos mensais dos dados arquivados serão mantidos por 1 ano. Depois deste período, as fitas serão reutilizadas ou destruídas.
- Backups completos anuais dos dados arquivados serão mantidos por 5 anos. Após esse período, as fitas serão reutilizadas ou destruídas.

Dos testes de backup

21. Os backups serão verificados periodicamente:
    - Os logs de backup serão revisados semanalmente em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho do backup.
    - Ações corretivas serão tomadas quando os problemas de backup forem identificados, a fim de reduzir os riscos associados a backups com falha.
22. Os testes de restauração dos backups devem ser realizados, por amostragem uma vez ao mês, em servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos de TI e tecnologias disponíveis, a fim de verificar backups bem-sucedidos.
23. Quaisquer exceções a esta política serão totalmente documentadas e aprovadas pela equipe técnica.

Procedimento de restauração de backup

24. O atendimento de solicitações de restauração de arquivos e demais formas de dados deverá obedecer às seguintes orientações:

    a. A solicitação de restauração de objetos deverá sempre partir do responsável pelo recurso, através de abertura de chamado técnico.

    b. A restauração de objetos somente será possível nos casos em que este tenha sido atingido pela estratégia de backup.

    c. A solicitação de restauração de dados que tenham sido salvaguardados depende de prévia e formal autorização dos respectivos gestores das informações.

    d. O operador de backup terá a prerrogativa de negar a restauração de dados cujo conteúdo não seja condizente com a atividade institucional, cabendo recurso da negativa ao gestor da unidade do demandante.

Do Descarte da Mídia

25. A mídia de backup será retirada e descartada conforme descrito neste documento:

    a. A TI garantirá que a mídia não contenha mais imagens de backup ativas e que o conteúdo atual ou anterior não possa ser lido ou recuperado por terceiros não autorizados.

    b. A TI garantirá a destruição física da mídia antes do descarte.

    c. A fita magnética será encaminhada para sobrescrita ou para descarte, caso já tenha excedido 2/3 da sua vida útil ou apresente sinais de degradação. A fita magnética só será considerada confiável durante os dois primeiros terços da vida útil estabelecida pelo fabricante. Após expirado este prazo, as informações nela contidas deverão ser transcritas para uma nova mídia, a fim de zelar pela integridade dos dados. O descarte das mídias de backup não confiáveis deverá ser feito mediante proposta apresentada pela Equipe de Backup e dirigida à Superintendência de Tecnologia da Informação. As fitas a serem descartadas deverão ser destruídas fisicamente, seguindo orientações do fabricante quanto a vida útil, de forma a impedir a sua reutilização ou acesso indevido às informações por pessoas não autorizadas.