

# PREFEITURA DE MAIRIPORÃ

## SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO RECURSOS HUMANOS E MODERNIZAÇÃO

### DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

#### NORMAS DE BACKUPS E RECUPERAÇÃO DE DADOS

Normas para estabelecer um processo sistemático para a realização de backups regulares e a recuperação de dados, garantindo a integridade, disponibilidade e segurança das informações da Prefeitura Municipal de Mairiporã:

- I. A política de Backup e Restauração de Dados deve estar alinhada com a Política de Segurança da Informação da Prefeitura.
- II. A Política de Backup e Restauração de Dados deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.
- III. As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.
- IV. As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.
- V. A solução utilizada para realização das cópias de segurança deve gerar logs das rotinas de backup, incluindo as etapas bem-sucedidas e erros do processo de backup, além de permitir integração com um servidor operador de serviço de Syslog.
- VI. 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 Prefeitura.
- VII. 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 local remoto ao da sede da organização para armazenar cópias extras dos principais backups, a exemplo de dados de serviços críticos.
- VIII. A infraestrutura de rede de backup deve ser apartada logicamente dos sistemas críticos da organização.
- IX. Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup.
- X. Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.
- XI. Os backups dos serviços de TI críticos da Prefeitura devem ser realizados utilizando-se as seguintes frequências temporais: a. Diária; b. Semanal; c. Mensal; d. Anual.
- XII. Os ativos envolvidos no processo de backup são considerados ativos críticos para a Prefeitura.
- XIII. A solicitação de salvaguarda dos dados referentes aos serviços de TI críticos e aos serviços de TI não críticos deve ser realizada pelo (s) responsável (s) dos dados, com a anuência prévia e formal do superior hierárquico, refletindo os requisitos de negócio da organização da informação para a continuidade da operação, e deve explicitar, no mínimo, os seguintes requisitos: a. Escopo (dados digitais a serem salvaguardados); b. Tipo de backup (completo, incremental, diferencial); c. Frequência temporal de realização do backup (diária, semanal, mensal, anual);
- XIV. A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas ao Administrador de Backup.



# PREFEITURA DE MAIRIPORÃ

## SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO RECURSOS HUMANOS E MODERNIZAÇÃO

### DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

- XV. O administrador de backup deve identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso.
- XVI. Podem ser utilizadas técnicas de compressão de dados, contando que o acréscimo no tempo de restauração dos dados seja considerado aceitável pelos gestores das informações.
- XVII. No caso de desligamento do usuário (de forma permanente ou temporária), o backup de seus arquivos na Rede de Comunicação Interna (RCI) deverá ser mantido por, no mínimo, 90 dias.
- XVIII. 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 pelo administrador de backup.
- XIX. Quando da necessidade de descarte de unidades de armazenamento de backups, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los, atentando-se ao descarte sustentável e ambientalmente correto.
- XX. Quaisquer exceções a esta política serão totalmente documentadas e aprovadas pela Comissão de Segurança da Informação.
- XXI. O processo de restauração deve ser iniciado imediatamente após a identificação de um problema pela Prefeitura
- XXII. O administrador de backup e o operador de backup devem ser capacitados para as tecnologias, procedimentos e soluções utilizadas nas rotinas de backup.
- XXIII. 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.
- XXIV. Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.

