# ANEXO III

## POLÍTICA DE BACKUP E RESTAURAÇÃO DE DADOS

Regulamenta a política de cópia de segurança (backup) e restauração de dados no âmbito da Prefeitura do Município de Bertioga.

### Disposição Preliminares

A Política de Backup e Restauração de Dados objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados custodiados pela Diretoria de Tecnologia da Informação (DTI) para manter a continuidade das atividades institucionais da Prefeitura do Município de Bertioga.

A implantação desta política busca assegurar sua missão, sendo necessário estabelecer mecanismos que permitam a guarda de dados e sua eventual restauração em casos de indisponibilidade ou perda por erro humano, ataques cibernéticos ou outras ameaças. Busca estabelecer o modo e a periodicidade da cópia de dados armazenados pelos sistemas computacionais.

Considera-se como “dados críticos” pastas armazenadas no servidor de dados, banco de dados dos sistemas de informações corporativas, de folha de pagamento, tramitação de documentos e e-mails devendo ser revisado anualmente a definição de dados críticos e o escopo desta política de backup.

Esta política se aplica aos servidores da DTI que armazenam tais dados. A política também se aplica a terceiros que processam e armazenam dados de propriedade da Prefeitura.

### Dos Conceitos

Para fins desta política considera-se:

**- Backup ou Cópia de Segurança:** conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo a guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Deve ser identificado a mídia em que a cópia é realizada;

**- Custodiante da Informação:** qualquer indivíduo ou estrutura da Prefeitura que tenha a responsabilidade formal de proteger a informação e aplicar os níveis de controle 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 os dados podem ser armazenados;

**- Infraestrutura Crítica:** Instalações, serviços, bens e sistemas, virtuais ou físicos, que se forem incapacitados ou tiverem desempenho degradado, provocarão forte impacto na rotina de trabalho da Prefeitura;

**- Recovery Point Objective (RPO):** ponto no tempo em que os dados dos serviços de TI devem ser recuperados após uma situação de parada ou perda, correspondendo ao prazo máximo em que se admite perder dados no caso de um incidente;

**- Recovery Time Objective (RTO):** tempo estimado para restaurar os dados e tornar os serviços de TI novamente operacionais, correspondendo ao prazo máximo em que se admite manter os serviços de TI inoperante até a restauração de seus dados, após um incidente.

## Dos Princípios Gerais

A Política de Backup e Restauração de Dados deve estar alinhada com a Politica de Segurança da Informação, bem como com a gestão de continuidade das atividades.

As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.

As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.

As rotinas de backup devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TI ou dado armazenado, dando prioridade aos serviços de TI críticos da Prefeitura.

O armazenamento de backup, se possível, deve ser realizado em um local distinto da infraestrutura crítica.

A infraestrutura de rede de backup deve ser separada dos sistemas críticos da Prefeitura.

Nos casos em que a confidencialidade for importante, convém que as cópias de segurança sejam protegidas através de criptografia apropriada.

Os backups críticos devem ser realizados diariamente.

Os serviços críticos de TI, armazenados em nuvem, devem ser resguardados sob um padrão de segurança, devendo observar a frequência da retenção de dados estabelecida abaixo:

I – Diária: 1 mês;

II – Mensal: 1 ano;

III – Anual: 5 anos.

Os serviços não críticos de TI, armazenados em nuvem ou infraestrutura local, devem ser resguardados sob um padrão de segurança, devendo observar a frequência da retenção de dados estabelecidas abaixo:

I – Diária: 1 mês;

II – Mensal: 1 ano;

III – Anual: 1 ano.

Especificações dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenção diferenciados.

Os ativos envolvidos no processo de backup são considerados ativos críticos para a organização.

A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas à DTI para análise e aprovação.

Os responsáveis pelos dados deverão ter ciência dos tempos de retenção estabelecidos para cada tipo de informação e os administradores de backup deverão zelar pelo cumprimento das regras estabelecidas.

**Do Tipo de Backup**

Para fins de realização de backup serão utilizados os seguintes modelos:

I – Completo (Full);

II – Incremental.

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

I – Backup incremental diário;

II – Backup completo semanal.

Os backups serão armazenados na infraestrutura de rede de backup. Os backups deverão ser realizados no período noturno para permitir mais tempo para realizar o backup e o baixo processamento dos servidores de dados.

**Do Uso da Rede e Recurso de Armazenamento**

Deve ser considerado o impacto da execução das rotinas de backup sobre o desempenho da rede de dados da Prefeitura, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI da instituição.

As unidades de armazenamento utilizadas no armazenamento dos dados devem considerar as características de cada dado armazenado, tais como:

I – A criticidade do dado armazenado;

II – O tempo necessário de retenção do dado;

III – A probabilidade de necessidade de restauração;

IV – O tempo previsto de restauração;

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

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

A Diretoria de Tecnologia da Informação deve identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso.

A execução das rotinas de backup deve considerar a previsão de ampliação da capacidade dos dispositivos envolvidos para o armazenamento local e em nuvem.

As unidades de armazenamento de backup devem estar instaladas em locais apropriados, com controle de temperatura, umidade,

poeira e de acesso restrito a pessoas de acordo com as normas técnicas que tratam de segurança física e lógica destes equipamentos.

Quando ocorrer a 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 conforme normas ambientais para equipamentos de TI.

**Dos Testes de Backup**

Os backups deverão ser verificados periodicamente:

I – Diariamente, deverão ser revisados os logs em busca de erros, durações anormais e quando possível a oportunidade para melhoria do desempenho do backup;

II – Ações corretivas serão tomadas quando forem identificados os problemas de backup, a fim de reduzir os riscos associados a falhas de backup;

III – Deverá ser mantido registro de backups e de testes de restauração para demonstrar a conformidade com esta política.

Os testes de restauração de backups devem ser realizados por amostragem, uma vez por mês, em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, a fim de verificar backups bem-sucedidos.

Será necessário verificar se foram atendidos os níveis de serviço de Recovery Time Objective – RTOs.

Os registros deverão conter, no mínimo, o tipo de sistema que teve seu restabelecimento testado, a data da realização do teste, o tempo gasto para o retorno de backup e se o procedimento foi realizado com sucesso.

**Do Procedimento de Restauração de Backup**

O atendimento de solicitações de restauração de backup de arquivos, banco de dados e demais formas de dado deverá obedecer aos seguintes procedimentos:

I – A solicitação de restauração deverá sempre partir do responsável pelo dado, através de chamado técnico;

II – A restauração somente será possível nos casos em que este tenha sido atingido pela estratégia de backup;

III – A restauração poderá ser negada nos casos cujo conteúdo não seja condizente com a atividade da área solicitante, cabendo recurso da negativa solicitado pelo secretário da pasta solicitante com as justificativas da solicitação;

IV – O tempo de restauração é proporcional ao volume de dados necessários para o restore de dados, devendo ser estabelecido por meio de acordo de nível de serviço o tempo para atendimento estas solicitações.

**Do Descarte de Dados e da Mídia**

Nos casos de desligamento do usuário (de forma permanente ou temporária), o backup de seus arquivos respeitará as diretrizes de política de descarte. Após o período determinado, os arquivos poderão ser excluídos a qualquer momento.

A mídia de backup será retirada e descartada conforme descrito nesta política de backup;

Deverá ser garantido 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.

A Diretoria de Tecnologia da Informação deverá garantir a destruição física da mídia antes do descarte.

**Considerações Finais**

Não serão salvaguardados, nem recuperados dados armazenados localmente em microcomputadores dos usuários ou em qualquer outro dispositivo que seja de desconhecimento da Diretoria de Tecnologia da Informação, ficando sob a responsabilidade do usuário/ departamento que utilizar o dispositivo.