Política de Backup

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Versão 1.0

Tupã, Dezembro de 2022

POLÍTICA DE CONTROLE DE BACKUP

PREFEITURA MUNICIPAL DA ESTÂNCIA TURÍSTICA DE TUPÃ

CAIO AOQUI

Prefeito

SECRETARIA DE ADMINISTRAÇÃO

Everton Nakashima

Secretário de Administração

DEPARTAMENTO DE TECNOLOGIA E PROCESSOS

Flávio Fagoti Pelim

Diretor do Departamento de Tecnologia e Processos

Equipe Técnica de Elaboração

Flávio Fagoti Pelim

Equipe Revisora

Aguinaldo Redi dos Reis

Carlos Henrique Ghiraldeli Saes Lopes

Ricardo Barbosa

Sumário

Histórico de Versões

Data	Versão	Descrição	Autor
08/11/2022	1.0	Modelo de Política de Backup	Equipe Técnica de Elaboração

Histórico de Revisão

ID da versão	Data da Mudança	Autor

Esclarecimentos

O objetivo deste documento é fornecer ao Departamento de Tecnologia e Processos e à Secretaria de Administração, orientações para mitigação de possíveis riscos ligados às temáticas de privacidade e segurança da informação, relativos aos seus sistemas informatizados, contratos administrativos e processos de trabalho da instituição.

O documento foi construído a partir de análises de pontos relevantes dos sistemas informatizados críticos de Tecnologia da Informação, realizadas pelo Departamento de Tecnologia e Processos.

Introdução

No contexto da transformação digital do Estado brasileiro, o Governo Federal publicou em 29 de abril de 2020, por meio do Decreto nº 10.332, a Estratégia de Governo Digital, iniciativa que se encontra em plena execução. Ela norteia as ações de todos os órgãos federais, com o objetivo de transformar o governo pelo Digital, oferecendo políticas públicas e serviços de melhor qualidade, mais simples, acessíveis de qualquer lugar e a um custo menor para o cidadão.

Hoje, mais do que em qualquer outro momento da história, o Governo utiliza a tecnologia para melhorar e expandir a oferta de serviços públicos para o cidadão apoiado em sistemas informatizados

Nesse contexto, os órgãos federais, com infraestrutura própria ou contratada de terceiros, coletam, recebem, acessam, processam, modificam, produzem, extraem, validam, armazenam, distribuem e transmitem informações confidenciais e públicas para apoiar a entrega de produtos e serviços essenciais (por exemplo, fornecimento de serviços financeiros; fornecimento de serviços de emissões guias, certificados e carteiras; processamento de autorizações de segurança ou dados de saúde; fornecimento de serviços em nuvem; desenvolvendo comunicações via cabo, wireless e/ou satélites; sistemas militares de defesa). As informações federais são frequentemente fornecidas ou compartilhadas, obedecidos os requisitos legais, com entidades como governos estaduais e municipais, empresas públicas e privadas, faculdades e universidades, organizações de pesquisa independentes ou públicas e organizações do terceiro setor.

A proteção dessas informações pelo Governo enquanto agente de tratamento está designada no **Art.46. da Lei Geral de Proteção de Dados**, sancionada em 14 de agosto de 2018 – “Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.”

A sua não observância pode impactar diretamente a capacidade do governo federal de cumprir suas missões precípuas de promover uma gestão pública eficiente, ampliar o acesso à cidadania, estimular uma economia brasileira crescentemente digitalizada, dinâmica, produtiva e competitiva, e em última instancia, impedir a geração de valor público para o cidadão.

Política de Backup e Restauração de Dados Digitais

Responsável	Departamento de Tecnologia e Processos.
Aprovado por:	Secretaria de Administração
Políticas Relacionadas	Gestão de riscos.
Localização de armazenamento	Tupa.sp.gov.br
Data da Aprovação	
Data de revisão	01/12/2024

Propósito

A Política de Backup e Restauração de Dados Digitais objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pelo Departamento de Tecnologia e Processos e formalmente definidos como de necessária salvaguarda na Prefeitura Municipal, 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 a todos os dados no âmbito da Prefeitura Municipal da Estância Turística de Tupã, incluindo dados fora dela, armazenados em um serviço de nuvem Pública ou Privada. “Dados críticos”, neste contexto, incluem bancos de dados de diversos sistemas, códigos fonte, arquivos compartilhados específicos e emails. A definição de dados críticos e o escopo desta política de backup serão revisados bienalmente.
- Os serviços de TI críticos da PMETT devem ser formalmente elencados pelo Comitê de gestão de políticas de TI.
- Já ficam previamente estabelecidos os bancos de dados de todos os sistemas como serviços críticos da PMETT.
- Esta política se aplica aos agentes públicos que podem ser criadores e/ou usuários de tais dados. A política também se aplica a terceiros que acessam e usam na PMETT sistemas e equipamentos de TI ou que criam, processam ou armazenam dados de propriedade da PMETT.
- 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, ficando sobre a responsabilidade do indivíduo que usa o(s) dispositivo(s).
- A salvaguarda dos dados em formato digital pertencentes a serviços de TI da PMETT 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 Federal, 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;

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 inoperantes até a restauração de seus dados, após um incidente;

Referência legal e de boas práticas

Orientação	**Secção**
Acórdão 1.889/2020-TCU-Plenário	Relatório de Levantamento de Auditoria Páginas 30-32
Decreto 10.332/2020 - Estratégia de Governo Digital 2020-2022	Em sua íntegra
Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2, XXIII
Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER)	Anexo, Item 2.3.4 e 2.3.5
Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	Anexo Art.3, Inciso I, II e V
Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	CAPÍTULO I - Art.2, Incisos III e IV CAPÍTULO II - Art.3, Inciso III, IV, VIII XI CAPÍTULO VI - Seção IV – Art.15
Framework Control Objectives for Information and Related Technology – Cobit, conjunto de boas práticas a serem aplicadas à governança da TI;	v4.1: DS11: Gerenciar Dados v5: DSS01.01, DSS04.08; DSS06.04, DSS04.08, DSS05.06; DSS06.05-06, DSS04.08, DSS001.01; DSS05.02-05; DSS06.03; DSS06.06
Framework de segurança cibernética do CIS 8	Salvaguardas do controle 11 (Data Recovery Capabilities)
Framework Information Technology Infrastructure Library – ITIL, v. 4, conjunto de boas práticas a serem aplicadas na infraestrutura, operação e gerenciamento de serviços de TI;	Gestão da Segurança da Informação

Guias Operacionais SGD	Todos
Instrução Normativa 01/GSI/PR	Art.12, Inciso IV, alínea g, h
Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021	Capítulo IV
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – Art. 46, Seção II Art. 50
Lei Nº 12.527/2011 – Lei de Acesso à Informação (LAI)	Em sua íntegra
Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança - Sistemasde gestão de segurança da informação - Requisitos;	A.12.3 Cópias de segurança
Norma ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;	12.3 Cópias de segurança
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra

Declarações da política

Dos princípios gerais

1. A Política de Backup e Restauração de Dados deve estar alinhada com a Política de Segurança da Informação da PMETT.
2. A Política de Backup e Restauração de Dados deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.
3. As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.
4. As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.
5. 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.
6. 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.
7. A infraestrutura de rede de backup deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização.
8. Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup.
9. Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.

Da frequência e retenção dos dados

10. Os backups dos serviços de TI críticos da PMETT devem ser realizados utilizando-se as seguintes frequências temporais:

    I – Diária;

    II – Anual;

11. Os serviços de TI críticos da PMETT devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

    I – Diária: 1 mês;

    II – Anual: 3 anos.

12. Os serviços de TI NÃO críticos da PMETT devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

    I – Diária: 1 mes;

    II – Anual: 2 anos.

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

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

15. A solicitação de salvaguarda dos dados referentes aos serviços de TI críticos e aos serviços de TI não críticos deve ser realizada por funcionários do Departamento de Tecnologia e Processos com a anuência prévia e formal do Diretor do Departamento de Tecnologia e Processos, refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação e proteção de dados envolvidos e a criticidade da informação para a continuidade da operação da organização, e deve explicitar, no mínimo, os seguintes requisitos técnicos:

    I – Escopo (dados digitais a serem salvaguardados);

    II – Tipo de *backup* (completo, incremental, diferencial);

    III – Frequência temporal de realização do backup (diária, semanal, mensal, anual);

    IV – Retenção;

    V – RPO (ponto em uma linha de tempo em que o s dados devem ser recuperados após a ocorrência de uma ruptura);

    VI – RTO (período de tempo dentro do qual os níveis mínimos dos serviços e/ou sistemas devem ser recuperados após a ocorrência de uma interrupção).

16. A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas ao funcionário responsável pela manutenção dos backups. A aprovação para execução da alteração depende da anuência do Diretor do Departamento de Tecnologia e Processos.

17. 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 diretrizes estabelecidas.

Tipo de backup

I – Completo (*full*);

II – Incremental;

III – Diferencial.

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

18. Backup incremental diário (segunda a sábado), armazenado no local e em nuvem.
19. Os backups devem ser programados para uma faixa de horário que não afete o horário comercial de funcionamento da PMETT.

Do uso da rede

20. O administrador de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados da PMETT, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI da PMETT.
21. A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup.
22. O período de janela de backup deve ser determinado pelo administrador de backup em conjunto com a área técnica responsável pela administração da rede de dados da PMETT.

Do transporte e armazenamento

23. 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.
24. 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.
25. Podem ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de restauração dos dados seja considerado aceitável pelos gestores das informações.
26. A execução das rotinas de backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.
27. No caso de desligamento do usuário (de forma permanente ou temporária), o backup de seus arquivos em nuvem deverá ser mantido por, no mínimo, 30 dias. Após esse período os arquivos poderão ser excluídos a qualquer tempo.
28. 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. Além disso, as condições de temperatura, umidade e pressão devem ser aquelas descritas pelo fabricante das unidades de armazenamento.

29. 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.

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

- Todos os backups serão gravados em mídias reutilizáveis, SSDS OU HDDS.
- A mídia será claramente identificada e armazenada em uma área segura acessível apenas para pessoa(s) autorizada(s) ou o fornecedor de armazenamento seguro de mídia externo, contratado pela PMETT.
- A mídia não será deixada sem supervisão durante o transporte.
- Backups diários completos dos bancos de dados e incrementais de arquivamentos, serão mantidos por 1 semana e armazenado no local e na nuvem.
- Backups completos anuais dos dados arquivados serão mantidos por 3 anos. Após esse período, as midias serão reutilizadas ou destruídas.

Dos testes de backup

30. Os backups serão verificados periodicamente:
    - Diariamente os logs de backup serão revisados 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.
    - A TI manterá registros de backups e testes de restauração para demonstrar conformidade com esta política.
    - Os testes devem ser realizados em todos os backups produzidos independente do ambiente.
31. Os testes de restauração dos backups devem ser realizados, por amostragem uma vez ao mës, em equipamentos 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.
32. Verificar se foi atendido os níveis de serviço pactuados, tais como os Recovery Time Objective – RTOs.
33. Os registros deverão conter, no mínimo, o tipo de sistema/serviço que teve o seu reestabelecimento testado, a data da realização do teste, o tempo gasto para o retorno do backup e se o procedimento foi concluído com sucesso
34. Quaisquer exceções a esta política serão totalmente documentadas e aprovadas pelo comitê de gestão de políticas de TI.

Procedimento de restauração de backup

35. O atendimento de solicitações de restauração de arquivos, e-mails 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 chamado técnico utilizando a ferramenta/sistema que for o padrão de aberturas do tipo na PMETT naquele momento.

    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.

36. O cronograma de restauração de dados:

    a. O tempo de restauração é proporcional ao volume de dados necessários para a restauração. As estimativas a seguir são do tempo de atendimento do Departamento de Tecnologia e Processos, não contemplando o tempo antes ou após o pedido a equipe:

        - A cada 1 GB de dados de arquivos compartilhados não criptografados, o tempo de restauração é de 30 minutos.
        - A cada 1GB de dados de bancos de dados de sistemas, o tempo de restauração é de 1 hora.
        - A cada 1GB de dados de arquivos compartilhados criptografados, o tempo de restauração é de 90 minutos.

    b. Backups externos serão disponibilizados em aproximadamente 1 dia de uma falha catastrófica do sistema, observando a prioridade para restauração de acordo com a criticidade de cada um;

    c. Backups externos serão disponibilizados em aproximadamente 4 horas de uma falha não catastrófica do sistema, observando a prioridade para restauração de acordo com a criticidade de cada um.

37. A restauração de dados seguirá as seguintes diretrizes:

    a) Será realizada em uma estação dedicada a essa tarefa.

    b) Restaurações não críticas serão realizadas fora de horário de expediente.

    c) O processo deverá ser documentado quanto a seu inicio, termino e ocorrências quando houver.

Do Descarte da Mídia

38. 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. Uma vez destruída a mídia, esta será encaminhada para o setor responsável por descarte de lixo eletrônico.

Das Responsabilidades

39. O administrador de backup e o operador de backup devem ser capacitados para as tecnologias, procedimentos e soluções utilizadas nas rotinas de backup.

São atribuições do administrador de backup:

I – Propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pela organização;
II – Providenciar a criação e manutenção dos backups;
III – Configurar as soluções de backup;
IV – Manter as unidades de armazenamento de backups preservadas, funcionais e seguras;
V – Definir os procedimentos de restauração e neles auxiliar;

Não conformidade

Em caso de violação desta política poderão ser aplicadas sanções previstas na Lei 8.112/1990 e outras legislações cabíveis.

As sanções por descumprimento podem incluir, mas não se limitam a um ou mais dos seguintes:

1. Processo Administrativo Disciplinar de acordo com a legislação aplicável
2. Exoneração.
3. Ação judicial de acordo com as leis aplicáveis e acordos contratuais.
4. Rescisão contratual ao bem do serviço público.

Concordância

Eu li e entendi a Política de Backup e Restauração de Dados Digitais do PMETT. Entendo que se eu violar as diretrizes estabelecidas nesta Política, posso enfrentar ações legais e/ou disciplinares de acordo com as leis aplicáveis e as normas internas da PMETT.

_____
Nome do Servidor/Empregado

_____
Assinatura do funcionário Data