	Política	Código	POL-07
PREFEITURA DE SÃO JOSÉ DO RIO PARDO	Política de Backup	Classificação	Pública
		Revisão	0

1. Introdução

Esta política define os conceitos e diretrizes de segurança e backup de dados para as aplicações da PREFEITURA DE SÃO JOSÉ DO RIO PARDO, visando garantir um ambiente seguro e eficiente.

2. Objetivo

A Política de Backup objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pelo setor de tecnologia da informação formalmente definidos como de necessária salvaguarda na PREFEITURA DE SÃO JOSÉ DO RIO PARDO, 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.

3. Escopo

Esta política se aplica a todos os dados sob a jurisdição da Prefeitura de São José do Rio Pardo, incluindo aqueles armazenados em serviços de nuvem pública ou privada, mesmo que fora de suas instalações.

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 sob a responsabilidade do indivíduo que usa o(s) dispositivo(s).

A salvaguarda dos dados em formato digital pertencentes a serviços de TI da PREFEITURA DE SÃO JOSÉ DO RIO PARDO, 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.

4. Público Alvo

Esta política se aplica a colaboradores que podem ser criadores e/ou usuários de tais dados.

Esta política também se aplica a terceiros que acessam ou utilizam os sistemas e equipamentos de TI da **Prefeitura de São José do Rio Pardo**, bem como àqueles que criam, processam ou armazenam dados de sua propriedade.

5. 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;
- **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, ou à segurança da informação;

6. Referências

- ISO/IEC 27001:2022 - Segurança da Informação, Cibersegurança e Proteção da Privacidade - Requisitos para Sistemas de Gestão de Segurança da Informação.
- ITIL (Information Technology Infrastructure Library) - Conjunto de práticas para o gerenciamento de serviços de TI.

- COBIT (Control Objectives for Information and Related Technology) - Framework de boas práticas para o gerenciamento de TI.

7. Diretrizes

7.1. Dos princípios gerais

- 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 salvaguardado, dando prioridade aos serviços de TI críticos da organização.
- O armazenamento de backup, se possível, deve ser realizado em um local distinto da infraestrutura crítica.
- A infraestrutura de rede de backup deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização.
- Deve-se manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup.
- Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de criptografia.

7.2. Da frequência e retenção dos dados

Os backups dos serviços de TI críticos da PREFEITURA DE SÃO JOSÉ DO RIO PARDO devem ser realizados utilizando-se as seguintes frequências temporais:

I – Diária;
II – Semanal;
III – Mensal;
IV – Anual.

Especificidades 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 solicitação de salvaguarda dos dados referentes aos serviços de TI críticos e aos serviços de TI não críticos deve ser realizada pelo Coordenador de Infraestrutura, com a anuência prévia e formal Supervisor de Sistemas , 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 – Local de armazenamento;

A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas ao Coordenador de Infraestrutura. A aprovação para execução da alteração depende da anuência do Supervisor de Sistemas.

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.

7.3. Tipos de Backups:

I – Completo (full);
II – Incremental;
III – Diferencial.

7.4. Rotinas de Backups

Backups realizados pelo Free File Sync :

SEVERBKP:

BKP-FTP-OBRAS:

- **Tipo de Backup:** Primeiro Full e seguintes Incremental;
- **Frequência:** diário;
- **Horário de Backup:** 11:30 e 18:30.
- **Tempo de retenção:** Indefinido.
- **Local de armazenamento:** On premise.

BKP-LICITAÇÃO::

- **Tipo de Backup:** Primeiro Full e seguintes Incremental;
- **Frequência:** diário;
- **Horário de Backup:** 17:55.
- **Tempo de retenção:** Indefinido.
- **Local de armazenamento:** On premise.

BKP-JURÍDICO:

- **Tipo de Backup:** Primeiro Full e seguintes Incremental;
- **Frequência:** diário;
- **Horário de Backup:** 17:25.
- **Tempo de retenção:** Indefinido.
- **Local de armazenamento:** On premise.

BKP-CONTABILIDADE:

- **Tipo de Backup:** Primeiro Full e seguintes Incremental;
- **Frequência:** diário;
- **Horário de Backup:** 17:40.
- **Tempo de retenção:** Indefinido.
- **Local de armazenamento:** On premise.

BKP-TRIBUTAÇÃO:

- **Tipo de Backup:** Primeiro Full e seguintes Incremental;
- **Frequência:** diário;
- **Horário de Backup:** 12:15.
- **Tempo de retenção:** Indefinido.
- **Local de armazenamento:** On premise.

BKP-TRIBUTAÇÃO:

- **Tipo de Backup:** Primeiro Full e seguintes Incremental;
- **Frequência:** diário;
- **Horário de Backup:** 12:00.
- **Tempo de retenção:** Indefinido.
- **Local de armazenamento:** On premise.

DELL 90.0.0.21:

BKP-Alto_Custo:

- **Tipo de Backup:** Primeiro Full e seguintes Incremental;
- **Frequência:** diário;
- **Horário de Backup:** 17:45.
- **Tempo de retenção:** Indefinido.
- **Local de armazenamento:** On premise.

BKP-Docs_Storage:

- **Tipo de Backup:** Primeiro Full e seguintes Incremental;
- **Frequência:** diário;
- **Horário de Backup:** 18:15.
- **Tempo de retenção:** Indefinido.
- **Local de armazenamento:** Google Drive e On premise.

BKP-Siscam_Sismama:

- **Tipo de Backup:** Primeiro Full e seguintes Incremental;
- **Frequência:** diário;
- **Horário de Backup:** 17:30.
- **Tempo de retenção:** Indefinido.
- **Local de armazenamento:** On premise.

Backups realizados por Script e crontab:

DELL 90.0.0.17:

BKP-Convenio_Medico:

- **Tipo de Backup:** Full;
- **Frequência:** diário;
- **Horário de Backup:** 17:55.
- **Tempo de retenção:** 30 Dias.
- **Local de armazenamento:** On premise.

7.5. Do uso da rede

O administrador de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados da PREFEITURA DE SÃO JOSÉ DO RIO PARDO, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI da PREFEITURA DE SÃO JOSÉ DO RIO PARDO.

A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup.

O período de janela de backup deve ser determinado pelo administrador de backup em conjunto com o setor de tecnologia da informação PREFEITURA DE SÃO JOSÉ DO RIO PARDO.

7.6. Do transporte e armazenamento

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.

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.

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.

A execução das rotinas de backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.

No caso de desligamento do usuário (de forma permanente ou temporária), o backup do e-mail em nuvem deverá ser mantido por, no mínimo, 7 dias. Após esse período, os arquivos poderão ser excluídos a qualquer tempo.

7.7. Dos testes de backup

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.
- O setor de tecnologia da informação 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.

Os testes de restauração dos backups devem ser realizados, por amostragem trimestralmente, 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

Verificar se foi atendido os níveis de serviço pactuados, tais como os Recovery Time Objective – RTOs.

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

Quaisquer exceções a esta política serão totalmente documentadas e aprovadas pelo setor de tecnologia da informação.

7.8. Procedimento de restauração de backup

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 abertura de chamado.

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.

7.8.1. O cronograma de restauração de dados:

A. O tempo de restauração, preferencialmente definido em Acordo de Nível de Serviço entre as áreas de negócio e de TIC, é proporcional ao volume de dados necessários para o restore. Para serviços de e-mail o tempo de restauração estimado é de 2 dias após o incidente. Esta estimativa é do tempo de atendimento do setor de tecnologia da informação, não contemplando o tempo antes ou após o pedido à equipe.

B. Backups externos serão disponibilizados em aproximadamente 7 dias de uma falha catastrófica do sistema, observando a prioridade para restauração de acordo com a criticidade de cada um;

8. Papéis e Responsabilidades

8.1. Área de Tecnologia da Informação

É responsabilidade da Área de Tecnologia da Informação:

- Propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pela organização;
- Providenciar a criação e manutenção dos backups;
- Configurar as soluções de backup;
- Manter as unidades de armazenamento de backups preservadas, funcionais e seguras;
- Definir os procedimentos de restauração e neles auxiliar;
- Implementar e cumprir o especificado nesta política

9. Penalizações

Sanções e punições serão aplicadas conforme previsto na Política Geral de Segurança da Informação.

10. Documentos correlatos.

POL-SI-01 - Política Geral de Segurança da Informação.

11. Natureza das Alterações.

Revisão	Data	Histórico de Revisões
0	02/04/2025	Emissão Inicial

	Política	**Código**	**POL-07**
	Política de Backup	**Classificação**	**Pública**
		Revisão	**0**

EqPDTIC

Libércio Donizete Martins
Cooordenador do Setor de Tecnologia da Informação