



Estância Turística de Pereira Barreto, 31 de março de 2026

PORTARIA Nº 001/2026 – SERVIÇO DE TECNOLOGIA DA INFORMAÇÃO - VERSÃO 1.0.0

Institui o Plano de Continuidade de Serviços de TIC e Resiliência Digital.

O CHEFE DO SERVIÇO DE TECNOLOGIA DA INFORMAÇÃO, no uso de suas atribuições, estabelece as diretrizes de continuidade para a infraestrutura tecnológica do Município de Pereira Barreto:

Art. 1º. Fica formalizado o Plano de Continuidade de Serviços, estruturado na redundância de ativos e na garantia de disponibilidade dos serviços ao cidadão.

1. ARQUITETURA DE ALTA DISPONIBILIDADE E SISTEMAS

A infraestrutura é segmentada para garantir que falhas locais não interrompam serviços externos críticos:

Serviços Externos (Cloud/VPS): O Portal Institucional, e o Diário Oficial Eletrônico, e gestão de ativos turísticos (Reservas via PIX) operam em ambiente VPS de Alta Disponibilidade externo, garantindo acesso mesmo em caso de indisponibilidade total do Data Center local.

Sistemas On-Premise (Locais): Hospedagem interna dos sistemas de gestão core (Fiorilli SCPI/SIP e RLZ Tributário e sistemas MV (Saúde), garantindo controle total sobre a soberania dos dados municipais.

2. RESILIÊNCIA DE ENERGIA E INFRAESTRUTURA (DATA CENTER)

Proteção Elétrica: O Data Center é suportado por sistemas de Nobreak de alta capacidade, garantindo autonomia mínima de 30 minutos em caso de queda de energia da concessionária.

Gestão Inteligente: Implementação de protocolos de desligamento (shutdown) e religamento (power-on) automatizados, preservando a integridade dos bancos de dados e do hardware em incidentes elétricos prolongados.

3. CONECTIVIDADE E REDUNDÂNCIA DE REDE

Link Principal: Conexão dedicada de 1Gbps para alta performance das secretarias e serviços internos.

Link de Contingência (Failover): Manutenção de link secundário de operadora distinta, garantindo rota de saída alternativa em caso de rompimento de fibra ou falha na operadora principal.

Serviços Públicos: Gestão de rede de Wi-Fi Público, com proteção de isolamento via Firewall da rede administrativa para garantir a segurança dos dados governamentais.



4. PROTOCOLO DE RECUPERAÇÃO E PRIORIDADES

Em cenários de contingência, a ordem de restabelecimento técnico será:

Sistemas de Saúde (MV): Pela natureza essencial do atendimento à vida.

Sistemas Financeiros e Tributários (Fiorilli/RLZ): Para manutenção da arrecadação e pagamentos municipais.

Recursos Humanos e Folha (SIP): Garantia dos proventos dos servidores.

Serviços de Turismo e Wi-Fi Público.

Prioridade de Restauração: Em caso de perda total, o Serviço de TI adotará o critério de Integridade Cronológica Reversa, iniciando a recuperação pelo ponto de restauração mais recente que esteja comprovadamente íntegro e livre de malwares/ransomwares.

5. POLÍTICA DE ESTOQUE CRÍTICO E SOBRESSALENTE (SPARE PARTS)

Fica estabelecida a manutenção de um Estoque de Contingência de Hardware, composto por ativos de rede e segurança essenciais, visando a substituição imediata (Hot Swap) em caso de falha física, descarga elétrica ou sinistro.

Dos Equipamentos de Pronta Reposição:

O Serviço de TI deverá manter em estoque, testados e pré-configurados, os seguintes itens mínimos:

Segurança de Borda (Firewalls/Gateways): No mínimo 01 (uma) unidade de reserva para o firewall principal da prefeitura, garantindo que o bloqueio de invasões e o controle de tráfego não sejam interrompidos.

Roteadores e Concentradores (RBs): Unidades de reserva para substituição de concentradores de link e roteadores de distribuição interna.

Infraestrutura de Rádio e Antenas: Manutenção de kits de antenas e rádios de backup para os pontos de conexão de secretarias externas e distritos que dependem de rádio-enlace.

Ativos de Rede (Switches): Switch Core e Switches de distribuição para garantir o fluxo de dados entre os departamentos.



6. POLÍTICA DE BACKUP E SALVAGUARDA DE DADOS (DATA PROTECTION)

A preservação da memória digital e da continuidade administrativa do Município de Pereira Barreto fundamenta-se na execução rigorosa de rotinas de cópias de segurança (backups), protegendo os sistemas Fiorilli (SCPI/SIP), RLZ (Tributário), MV (Saúde) e demais bases de dados críticas.

Da Periodicidade e Janelas de Backup:

As rotinas de salvaguarda devem seguir o cronograma de disponibilidade:

Backup Diário (Incremental): Deverá ser executado obrigatoriamente a cada 24 horas (janela noturna), capturando todas as alterações de dados realizadas durante o expediente bancário e administrativo.

2º Backup Semanal (Full/Completo): Realização de uma cópia integral de todos os sistemas e arquivos aos finais de semana, servindo como base de restauração para desastres de maior escala.

Cópia em Nuvem (Off-site Storage): Além do armazenamento local, é obrigatória a replicação dos dados para ambiente de nuvem (Cloud Backup) em servidor seguro e criptografado.



ANEXO I - MATRIZ DE IMPACTO E OBJETIVOS DE RECUPERAÇÃO

Serviço / Sistema	Criticidade	RPO (Backup)	RTO (Retorno)	Impacto Operacional	Impacto Legal / Financeiro
Sistema de Saúde (MV)	Crítica	24h	4h a 6h	Muito Alto	Alto (Risco à Vida)
Tributos e Arrecadação (RLZ)	Alta	24h	12h	Médio	Muito Alto (Receita)
Contabilidade/RH (Fiorilli)	Alta	24h	24h	Médio	Alto (Folha/Contas)
Site e Diário Oficial	Média	12h	2h	Médio	Médio (Transparência)
Wi-Fi Público / Turismo	Baixa	48h	72h	Médio	Médio

Art. 2º. Este plano entra em vigor na data de sua publicação.

Pereira Barreto - SP, 31 de Março de 2026.

Documento assinado digitalmente
gov.br RAFAEL NONATO BASSORA
Data: 31/03/2026 14:42:14-0300
Verifique em <https://validar.iti.gov.br>

RAFAEL NONATO BASSORA
Chefe do Serviço de Tecnologia da Informação