

PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO BIÊNIO 2026-2027





Sumário

1. Apresentação	3
2. Objetivos do PDTI	3
3. Metodologia	4
4. Diagnóstico da Situação Atual.....	4
5. Inventário de Tecnologia da Informação.....	5
6. Levantamento de Necessidades	6
7. Diretrizes Estratégicas de TI	7
8. Plano de Ações e Metas.....	8
9. Gestão de Riscos.....	9
10. Setor de TI.....	10
11. Monitoramento e Avaliação	11
12. Indicadores para Monitoramento do PDTI 2026–2027	11
13. Referencial Legal e Normativo	11
14. Diagrama da Estrutura Ideal do CPD.....	15
• Switch Gerenciável de 24 Portas	16
• Switch TP-Link Omada de 48 Portas:	16
• Controladora de Rede Omada:	16
Observações Finais sobre a Estrutura Ideal	16
15. Cronograma Detalhado de Execução	16
16. Considerações Finais e Aprovação	18





1. Apresentação

O Plano Diretor de Tecnologia da Informação (PDTI) 2026–2027 é o instrumento de planejamento estratégico que orienta as ações, investimentos e decisões na área de Tecnologia da Informação da Prefeitura Municipal de Sarapuí. Seu principal objetivo é alinhar os recursos tecnológicos às necessidades da gestão pública e aos interesses da população.

A elaboração deste plano reflete o comprometimento da administração municipal com a modernização dos serviços públicos, a eficiência na utilização dos recursos, a segurança da informação e a integração entre os diversos setores da prefeitura.

Ao longo do biênio 2026–2027, o PDTI será a base para a priorização de projetos, aquisição de equipamentos, adoção de sistemas e definição de padrões tecnológicos que promovam maior produtividade, transparência e qualidade no atendimento aos cidadãos.

Este Plano Diretor de Tecnologia da Informação está alinhado às políticas de segurança da informação, privacidade e proteção de dados pessoais já instituídas pela Prefeitura, e busca consolidar a integração entre tecnologia, governança e proteção de dados, em conformidade com a Lei nº 13.709/2018 (LGPD).

2. Objetivos do PDTI

O presente PDTI reflete o comprometimento da Administração com a inovação tecnológica, a transparência pública e a proteção das informações institucionais e pessoais, assegurando a conformidade com os princípios da boa governança pública e da Lei Geral de Proteção de Dados.

O Plano Diretor de Tecnologia da Informação 2026–2027 da Prefeitura Municipal de Sarapuí tem como objetivos principais:

- **Alinhar a área de Tecnologia da Informação às estratégias e prioridades da gestão municipal**, garantindo que os recursos de TI contribuam efetivamente para os resultados institucionais.
- **Planejar de forma estruturada a aquisição, manutenção e modernização de recursos tecnológicos**, promovendo maior eficiência, economicidade e sustentabilidade.
- **Implantar e consolidar a infraestrutura de rede baseada em Active Directory**, promovendo a centralização da autenticação, o controle de acesso a recursos e a aplicação padronizada de políticas de segurança (GPOs) em todos os computadores da administração pública.
- **Estabelecer conexões seguras entre secretarias e prédios públicos por meio de rede VPN (Virtual Private Network)**, garantindo acesso remoto seguro, unificação de serviços e maior controle sobre os fluxos de dados institucionais.
- **Padronizar o uso de soluções de segurança, com a implantação de antivírus corporativo em todos os dispositivos institucionais**, assegurando a proteção contra ameaças digitais e reduzindo riscos operacionais.
- **Garantir o licenciamento regular de softwares utilizados pela administração pública**, respeitando a legislação vigente, promovendo conformidade e reduzindo riscos





jurídicos e operacionais.

- **Organizar e padronizar os processos internos de TI**, promovendo maior controle, rastreabilidade e transparência nas ações do setor.
- **Promover a capacitação dos servidores públicos no uso da tecnologia**, valorizando a formação contínua e a cultura digital no serviço público.
- **Estabelecer indicadores de desempenho e acompanhamento das ações de TI**, assegurando a mensuração de resultados e o cumprimento das metas estabelecidas.

3. Metodologia

A elaboração do Plano Diretor de Tecnologia da Informação (PDTI) da Prefeitura Municipal de Sarapuí para o período de 2026–2027 foi conduzida com base em práticas de planejamento estratégico e gestão pública, adaptadas à realidade administrativa e operacional do município. Foram utilizadas as seguintes etapas metodológicas:

- **Levantamento da situação atual da infraestrutura de TI**, incluindo redes, servidores, estações de trabalho, conectividade entre prédios públicos, sistemas utilizados, licenças de software e ferramentas de segurança.
- **Realização de diagnóstico junto aos Diretores Municipais**, obtendo suas avaliações, sugestões e apontamentos sobre a situação tecnológica atual em seus respectivos setores, a fim de subsidiar a elaboração do plano.
- **Diagnóstico de necessidades junto às secretarias e setores administrativos**, considerando as demandas atuais e futuras relacionadas a sistemas, rede, atendimento técnico, acessos e digitalização de processos.
- **Mapeamento dos principais problemas, riscos e gargalos operacionais**, com base na experiência prática do Setor de Tecnologia da Informação e no histórico de ocorrências recorrentes.
- **Definição de objetivos estratégicos e diretrizes prioritárias**, considerando as metas da gestão municipal, as limitações orçamentárias e a necessidade de modernização tecnológica.
- **Elaboração de um plano de ações e metas mensuráveis**, com previsão de prazos, responsáveis e custos estimados, buscando garantir a execução realista das iniciativas propostas.

O plano foi elaborado de forma interna, sob coordenação do Setor de Tecnologia da Informação, com validação institucional junto à Administração Municipal.

4. Diagnóstico da Situação Atual

A Prefeitura Municipal de Sarapuí atualmente dispõe de uma infraestrutura tecnológica que apresenta limitações significativas para atender às demandas administrativas e de segurança da informação.

- **Equipamentos e sistemas operacionais:** Grande parte dos computadores utilizados em algumas áreas são equipamentos antigos, com sistemas operacionais obsoletos que não recebem mais atualizações de segurança, comprometendo a estabilidade e a proteção contra vulnerabilidades.
 - De acordo com os formulários, setores como **Obras** relataram que os





computadores “funcionam, mas são lentos ou limitados”.

- Já a **Educação** reconhece a necessidade imediata de **mais 4 computadores** para suprir a demanda existente.
- Outros setores (Assistência Social, Saúde e Agricultura) informaram possuir quantidade suficiente de máquinas, em bom estado, mas sem padronização de modelos e capacidades.
- **Ausência de Active Directory e Intranet:** A administração não conta com uma solução de Active Directory (AD) para centralização e controle de usuários e políticas de segurança, tampouco dispõe de uma intranet própria para comunicação interna e compartilhamento seguro de informações. Isso foi percebido indiretamente nas respostas, pois vários setores declararam que os computadores não estão em rede entre si (Agricultura, Educação e Obras, por exemplo).
- **Problemas técnicos em equipamentos antigos:** Computadores utilizados por alguns Diretores apresentam falhas recorrentes, muitas vezes sem possibilidade de reparo devido à idade avançada dos equipamentos, prejudicando a produtividade dos servidores.
 - Em **Obras**, foi relatado que não há rede integrada e que impressoras só funcionam cabeadas, o que demonstra limitações de infraestrutura.
 - A **Diretoria de Finanças** também mencionou que o sistema JLSoft “sai fora do ar constantemente”, impactando diretamente os trabalhos.
- **Falta de conectividade segura entre setores:** Não existe atualmente uma rede VPN para interligar os diferentes setores e prédios da Prefeitura, o que impossibilita a autenticação integrada via AD e o acesso seguro aos servidores e recursos compartilhados.
 - Os formulários confirmam que a maioria dos setores **não possui acesso remoto seguro** a servidores ou arquivos da Prefeitura (casos de Obras, Agricultura e Segurança Pública).
 - Em contrapartida, **Educação, Finanças e Saúde** afirmaram ter algum tipo de acesso remoto, porém sem padrões claros de VPN.
- **Segurança da informação limitada:** A Prefeitura não dispõe de uma solução robusta de segurança de rede, como um firewall avançado configurado (exemplo: pfSense), o que deixa a infraestrutura vulnerável a ataques e dificulta o controle de acessos e o monitoramento do tráfego de dados.
 - Em relação a antivírus, alguns setores declararam não possuir solução instalada ou atualizada (**Assistência Social, Agricultura, Segurança Pública e Obras**).
 - Setores como **Saúde e Educação** utilizam apenas soluções básicas, como Windows Defender, sem padronização ou centralização.
 - Também foi observado que muitos arquivos ainda são salvos apenas em computadores locais, sem backup ou armazenamento em nuvem adequado (casos de Obras e Educação).

Essas condições limitam a eficiência operacional, aumentam os riscos de segurança da informação e dificultam a implantação de soluções tecnológicas modernas necessárias para a melhoria dos serviços públicos prestados à população.

Além disso, deverá ser elaborado inventário detalhado de ativos tecnológicos e informacionais, contendo fabricante, modelo, responsável, criticidade e classificação da informação (pública, interna, sigilosa, sensível), conforme Política de Segurança da Informação.





4.1. Ações de Conformidade com a Lei Geral de Proteção de Dados (LGPD)

A Prefeitura já implantou mecanismos de conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), incluindo:

- Nomeação do Encarregado de Dados (DPO);
- Registro das Operações de Tratamento (RoPA);
- Elaboração do Relatório de Impacto à Proteção de Dados (RIPD);
- Publicação da Política de Privacidade e Avisos de Tratamento de Dados;
- Criação de canal do titular para solicitações de acesso, correção e exclusão;
- Regulamentação interna da LGPD e Política de Segurança da Informação;
- Plano de Resposta a Incidentes.

Essas ações estão integradas ao planejamento tecnológico e serão continuamente revisadas e monitoradas pelo Comitê de Governança de Dados e pelo T.I.

5. Inventário de Tecnologia da Informação

O levantamento realizado junto às Diretorias e Secretarias da Prefeitura Municipal de Sarapuí (formulários anexos ao PDTI) permitiu identificar de forma preliminar a quantidade aproximada de equipamentos disponíveis em cada setor. Ressalta-se que tais informações **não devem ser consideradas como inventário estatístico definitivo**, mas sim como **referência diagnóstica complementar**.

Quantidade de computadores por setor:

- **Assistência Social:** mais de 10 computadores, em bom estado geral.
- **Agricultura, Abastecimento, Meio Ambiente e Turismo:** entre 6 e 10 computadores, atendendo às necessidades.
- **Segurança Pública:** 1 a 2 computadores, em bom estado.
- **Obras, Viação e Urbanismo:** entre 6 e 10 computadores, porém com relatos de lentidão.
- **Finanças, Planejamento e Tributação:** entre 3 e 5 computadores, atendendo adequadamente.
- **Educação:** mais de 10 computadores, em bom estado, mas com necessidade de acréscimo de ao menos 4 unidades.
- **Saúde:** mais de 10 computadores, em bom estado.

Equipamentos adicionais

- **Impressoras:** presentes em praticamente todos os setores, algumas de uso compartilhado (Agricultura, Obras, Educação e Saúde).
- **Notebooks:** relatados em setores como Assistência Social, Segurança Pública, Educação e Saúde.
- **Scanners:** encontrados em Assistência Social e Finanças.

Situação geral

De forma geral, a maioria dos setores declara possuir quantidade **minimamente suficiente** de computadores para suas atividades, ainda que haja relatos de **limitações de desempenho**





(lentidão) e **necessidade de reforço pontual**, especialmente na Educação e em Obras. O uso de equipamentos compartilhados (principalmente impressoras) é frequente, o que pode gerar gargalos em determinados fluxos de trabalho.

6. Levantamento de Necessidades

Com base no diagnóstico realizado e nas contribuições dos Diretores Municipais, foram identificadas as seguintes necessidades prioritárias para o período 2026–2027:

- **Renovação dos equipamentos de informática:** Substituição dos computadores antigos e obsoletos, especialmente nas áreas que apresentam maior índice de falhas e indisponibilidade, garantindo melhor desempenho e compatibilidade com sistemas atuais.
- **Implantação do Active Directory (AD):** Centralização da gestão de usuários, autenticação e políticas de segurança, possibilitando controle de acesso mais eficiente e padronizado.
- **Implementação de rede VPN entre secretarias e prédios públicos:** Estabelecer conexões seguras e integradas entre os setores, permitindo autenticação centralizada via AD e acesso remoto seguro aos servidores e sistemas administrativos.
- **Aquisição e implantação de solução robusta de segurança de rede:** Implementação de firewall avançado (como pfSense) para controle de tráfego, prevenção contra ameaças e monitoramento da rede.
- **Regularização e aquisição de licenças de software:** Garantir o uso legalizado e atualizado dos softwares utilizados pela administração pública, atendendo à legislação vigente e reduzindo riscos jurídicos.
- **Capacitação técnica dos servidores:** Promover treinamentos para os servidores públicos no uso das novas ferramentas, segurança da informação e melhores práticas de TI.
- **Melhoria na infraestrutura de rede:** Atualização dos equipamentos de rede (switches, cabling, roteadores) para suportar as novas demandas e garantir maior estabilidade e velocidade.
- **Estabelecimento de procedimentos e políticas de TI:** Definição de normas para uso de recursos tecnológicos, segurança da informação, backup, e atendimento aos usuários.

7. Diretrizes Estratégicas de TI

Com base no diagnóstico realizado e nas contribuições dos Diretores Municipais, foram identificadas as seguintes necessidades prioritárias para o período 2026–2027:

- **Renovação dos equipamentos de informática:** Substituição dos computadores antigos e obsoletos, especialmente nas áreas que apresentam maior índice de falhas e indisponibilidade, garantindo melhor desempenho e compatibilidade com sistemas atuais.
 - O setor de **Obras** relatou lentidão generalizada nos equipamentos.
 - A **Educação** indicou necessidade imediata de pelo menos **4 computadores adicionais**.
 - Embora setores como **Assistência Social, Agricultura e Saúde** informem





possuir equipamentos em bom estado, há falta de padronização e manutenção preventiva.

- **Implantação do Active Directory (AD):** Centralização da gestão de usuários, autenticação e políticas de segurança, possibilitando controle de acesso mais eficiente e padronizado.
 - Diversos setores informaram que seus computadores **não estão em rede entre si**, como **Educação, Agricultura e Obras**, reforçando a necessidade do AD para integração e gerenciamento centralizado.
- **Implementação de rede VPN entre secretarias e prédios públicos:** Estabelecer conexões seguras e integradas entre os setores, permitindo autenticação centralizada via AD e acesso remoto seguro aos servidores e sistemas administrativos.
 - A maioria das Diretorias declarou **não possuir acesso remoto seguro** (Agricultura, Obras e Segurança Pública).
 - Em contrapartida, **Educação, Finanças e Saúde** relataram algum nível de acesso remoto, porém **sem padrões de VPN corporativa**.
- **Aquisição e implantação de solução robusta de segurança de rede:** Implementação de firewall avançado (como pfSense) para controle de tráfego, prevenção contra ameaças e monitoramento da rede.
 - Setores como **Assistência Social, Agricultura, Obras e Segurança Pública** informaram **não possuir antivírus instalado ou atualizado**.
 - **Saúde** utiliza apenas o **Windows Defender**, sem gestão centralizada.
 - Em **Educação**, os arquivos são armazenados apenas em computadores locais, sem backup adequado.
- **Regularização e aquisição de licenças de software:** Garantir o uso legalizado e atualizado dos softwares utilizados pela administração pública, atendendo à legislação vigente e reduzindo riscos jurídicos.
 - O setor de **Obras** relatou não possuir licença para softwares essenciais de engenharia, como **Métrica (topografia), Revit e AutoCAD**.
 - A **Educação** apontou a necessidade de um **sistema pedagógico** para apoio às atividades escolares.
 - A **Segurança Pública** sugeriu a aquisição de um sistema de **monitoramento (Defense ou similar)**.
- **Capacitação técnica dos servidores:** Promover treinamentos para os servidores públicos no uso das novas ferramentas, segurança da informação e melhores práticas de TI.
 - A maioria dos setores apontou interesse em capacitações, especialmente em **Segurança da Informação e Procedimentos de Backup** (Assistência Social, Agricultura, Segurança Pública, Educação e Saúde).
- **Melhoria na infraestrutura de rede:** Atualização dos equipamentos de rede (switches, cabeamento, roteadores) para suportar as novas demandas e garantir maior estabilidade e velocidade.
 - Setores como **Agricultura, Finanças e Saúde** relataram **instabilidades constantes na internet**, com quedas e lentidão.
 - Em **Obras**, impressoras só funcionam cabeadas devido a problemas de rede.
 - A **Educação** registrou paralisações por indisponibilidade da rede.
- **Estabelecimento de procedimentos e políticas de TI:** Definição de normas para uso





de recursos tecnológicos, segurança da informação, backup e atendimento aos usuários.

- Nos formulários, ficou claro que alguns setores **não adotam práticas formais de backup** e dependem de salvamento apenas em computadores locais (casos de Obras e Educação).
- Há também falta de padronização no uso de antivírus e soluções de segurança, reforçando a urgência de políticas claras de TI.

Deverão ser adotadas medidas de segurança da informação como autenticação multifator (MFA), controle de acessos por perfis, criptografia de discos em estações e servidores, backup estruturado (modelo 3-2-1), **plano de resposta a incidentes**, e campanhas permanentes de conscientização sobre segurança digital.

8. Plano de Ações e Metas

- **Implantação do Active Directory (AD):** Centralizar a gestão de usuários, autenticação e políticas de segurança. Prazo previsto: 1º semestre de 2026. Responsável: Setor de TI. Custo estimado: R\$ 9.000,00
- **Implantação de rede VPN entre secretarias:** Estabelecer conexão segura e integrada entre os prédios e setores públicos. Prazo previsto: 2º semestre de 2026. Responsável: Setor de TI. Custo estimado: Baixo custo.
- **Renovação de computadores antigos:** Substituir equipamentos obsoletos para melhorar desempenho e segurança. Prazo previsto: 2026–2027. Responsáveis: Setores envolvidos. Custo estimado: R\$ 60.000,00
- **Implantação de firewall:** Implementar solução robusta de segurança de rede para controle e monitoramento. Prazo previsto: 1º semestre de 2026. Responsável: Setor de TI. Custo estimado: Baixo custo.
- **Licenciamento de softwares:** Adquirir e regularizar licenças dos sistemas utilizados pela Prefeitura. Prazo previsto: 2026. Responsável: Setor de Compras e Setor de TI. Custo estimado: R\$ 22.000,00
- **Capacitação dos servidores:** Promover treinamentos para uso das novas ferramentas e segurança da informação. Prazo previsto: 2026–2027. Responsáveis: RH e Setor de TI. Custo estimado: Baixo custo.
- **Atualização da infraestrutura de rede:** Modernizar equipamentos de rede para suportar maior demanda. Prazo previsto: 2026. Responsável: Coordenação de TI. Custo estimado: R\$ 25.000,00
- **Definição de políticas e procedimentos de TI:** Estabelecer normas para uso, segurança e atendimento aos usuários. Prazo previsto: 1º semestre de 2026. Responsável: Coordenação de TI. Custo estimado: Baixo custo.

9. Gestão de Riscos

Durante a elaboração e implementação do Plano Diretor de Tecnologia da Informação 2026–2027 da Prefeitura Municipal de Sarapuí, foram identificados os seguintes riscos e suas respectivas estratégias de mitigação:

- **Falta de orçamento adequado:** Pode comprometer a aquisição de equipamentos, softwares e serviços essenciais.





- Setores como **Educação** apontaram necessidade imediata de novos computadores.
- A **Diretoria de Obras** relatou carência de softwares licenciados essenciais (Métrica, Revit e AutoCAD), evidenciando risco de despesas não previstas.
Mitigação: Planejamento orçamentário rigoroso, busca por parcerias, uso de soluções de baixo custo e priorização das ações essenciais.
- **Resistência à mudança por parte dos servidores:** Pode dificultar a adoção das novas tecnologias e processos.
 - Nos formulários, alguns setores destacaram que **nunca receberam capacitações formais em TI** (casos de Assistência Social e Agricultura), o que pode gerar resistência e insegurança no uso das novas ferramentas.
Mitigação: Realização de campanhas de sensibilização, treinamentos contínuos e suporte próximo aos usuários.
- **Equipe de TI reduzida ou insuficiente:** Pode impactar na capacidade de implantação e suporte dos projetos.
 - A **Assistência Social** destacou que “o reforço na equipe de TI é sempre útil para a melhoria dos trabalhos”.
 - Outras Diretorias (como Agricultura e Educação) também avaliaram que o suporte técnico precisa ser reforçado.
Mitigação: Reforço da equipe com contratações ou terceirização, além de capacitação técnica interna.
- **Falhas na segurança da informação:** Possibilidade de ataques cibernéticos, perda de dados ou acesso não autorizado.
 - Diversos setores informaram **não possuir antivírus instalado ou atualizado**, como Obras, Agricultura e Segurança Pública.
 - A **Educação** relatou que arquivos ainda são salvos apenas em computadores locais, e em Saúde há dependência do Windows Defender sem solução corporativa.
Mitigação: Implantação de firewall robusto (pfSense), antivírus corporativo, políticas de segurança, backups regulares e monitoramento constante.
- **Problemas na conectividade e infraestrutura:** Instabilidades na rede podem afetar a comunicação entre setores e o acesso a sistemas.
 - **Finanças** relataram que o sistema JLSOFT “sai fora do ar constantemente”.
 - **Saúde e Agricultura** registraram lentidão e instabilidade na internet.
 - Em **Obras**, impressoras só funcionam cabeadas devido a falhas na rede.
Mitigação: Investimento em equipamentos atualizados, manutenção preventiva e monitoramento da infraestrutura.
- **Não cumprimento dos prazos estabelecidos:** Pode atrasar a execução do PDTI e impactar negativamente os resultados esperados.
 - Alguns setores destacaram que problemas técnicos e quedas de sistema já impactam o andamento das atividades rotineiras, como no caso de **Finanças e Educação**, o que pode se refletir também no cumprimento dos cronogramas do PDTI.
Mitigação: Acompanhamento periódico, revisão de cronogramas e ajustes conforme necessidade.





10. Setor de TI

Para garantir a efetividade do Plano Diretor de Tecnologia da Informação 2026–2027, a Prefeitura Municipal de Sarapuí adota a seguinte estrutura de governança:

- **Setor de Tecnologia da Informação:** Responsável pela execução das ações do PDTI, gestão da infraestrutura, suporte técnico, implantação de soluções, controle dos recursos de TI e acompanhamento das metas.
- **Comitê de TI (opcional):** Grupo formado por representantes das principais secretarias e setores que possuem conhecimento básico, que se reúne periodicamente para discutir prioridades, avaliar resultados e propor ajustes no plano.
- **Gabinete do Prefeito:** Responsável pela aprovação final do PDTI, alocação de recursos e apoio institucional às ações de TI.
- **Setores administrativos:** Devem colaborar com o Setor de TI, informando demandas, participando de treinamentos e seguindo as políticas e normas definidas.
- **Gestão de contratos e fornecedores:** Setor de TI deve acompanhar e fiscalizar contratos relacionados a serviços, aquisição de equipamentos e licenciamento de softwares, garantindo conformidade e qualidade.
- **Monitoramento e comunicação:** Estabelecer canais para feedback, acompanhamento periódico do andamento das ações e divulgação dos resultados à administração municipal.

11. Monitoramento e Avaliação

O monitoramento do Plano Diretor de Tecnologia da Informação 2026–2027 da Prefeitura Municipal de Sarapuí será realizado por meio dos seguintes mecanismos:

- **Indicadores de desempenho:** Serão estabelecidos indicadores para medir o progresso das ações, tais como percentual de máquinas integradas ao Active Directory, número de setores com acesso via VPN, tempo médio de resolução de chamados, entre outros.
- **Relatórios periódicos:** O Setor de Tecnologia da Informação deverá elaborar relatórios trimestrais de acompanhamento, contendo o status das ações, eventuais dificuldades e propostas de correção.
- **Reuniões de acompanhamento:** Serão realizadas reuniões regulares com a equipe de TI e, quando necessário, com representantes dos setores envolvidos para avaliação dos resultados e alinhamento das próximas etapas.
- **Avaliação e revisão do plano:** Ao final de cada ano, será promovida uma avaliação geral do PDTI, com revisão dos objetivos e metas, considerando os resultados alcançados e as mudanças no cenário tecnológico ou institucional.
- **Feedback dos usuários:** A opinião dos servidores públicos será considerada para identificar melhorias nos processos, ferramentas e serviços de TI.

Esse acompanhamento contínuo visa assegurar a efetividade do PDTI, promovendo a melhoria contínua da infraestrutura tecnológica e dos serviços prestados à população.

12. Indicadores para Monitoramento do PDTI 2026–2027

- **Percentual de máquinas integradas ao Active Directory:**





Meta: 80% em 2026; 100% em 2027.

- **Número de setores com acesso via VPN:**

Meta: 5 setores em 2026; 10 setores em 2027.

- **Tempo médio de resolução de chamados de TI:**

Meta: Até 48 horas para 90% dos chamados.

- **Porcentagem de equipamentos com antivírus corporativo atualizado:**

Meta: 100% dos equipamentos.

- **Percentual de softwares licenciados regularmente:**

Meta: 100% até o final de 2026.

- **Número de treinamentos realizados com servidores:**

Meta: Mínimo de 4 treinamentos por ano.

- **Disponibilidade da rede e sistemas críticos:**

Meta: 99,5% uptime.

- **Quantidade de incidentes de segurança reportados:**

Meta: Redução anual em 20%.

13. Referencial Legal e Normativo

A elaboração e execução do Plano Diretor de Tecnologia da Informação (PDTI) da Prefeitura Municipal de Sarapuí estão alinhadas a um conjunto de leis, normas e diretrizes que regem a gestão pública, a transparência, a segurança da informação e a governança em tecnologia.

Leis e Decretos Federais

- **Lei nº 8.666/1993** – Lei de Licitações e Contratos (vigente até a completa substituição pela nova lei)
- **Lei nº 14.133/2021** – Nova Lei de Licitações e Contratos Administrativos
- **Lei nº 12.527/2011** – Lei de Acesso à Informação (LAI)
- **Lei nº 13.709/2018** – Lei Geral de Proteção de Dados Pessoais (LGPD)
- **Lei nº 10.520/2002** – Lei do Pregão
- **Decreto nº 10.332/2020** – Estratégia de Governo Digital 2020–2022

Normas Técnicas e Boas Práticas

- **Instrução Normativa nº 01/2019** – **SEGES/ME**
Dispõe sobre o PDTI no âmbito da Administração Pública Federal, podendo ser usada como modelo para governos municipais.
- **Modelos do SISP/ME** (Sistema de Administração dos Recursos de Tecnologia da Informação – Ministério da Economia)
- **Boas práticas da Governança de TI**, como:
 - COBIT (Governança de TI)
 - ITIL (Gestão de serviços de TI)
 - ISO/IEC 27001 (Segurança da Informação)
 - ISO/IEC 38500 (Governança corporativa de TI)

Legislação Municipal (quando aplicável)

- Leis municipais de estrutura administrativa e competência do Setor de TI.
- Normas internas sobre compras, patrimônio, contratos e segurança digital (inserir referência se houver).





PREFEITURA MUNICIPAL DE
SARAPUÍ

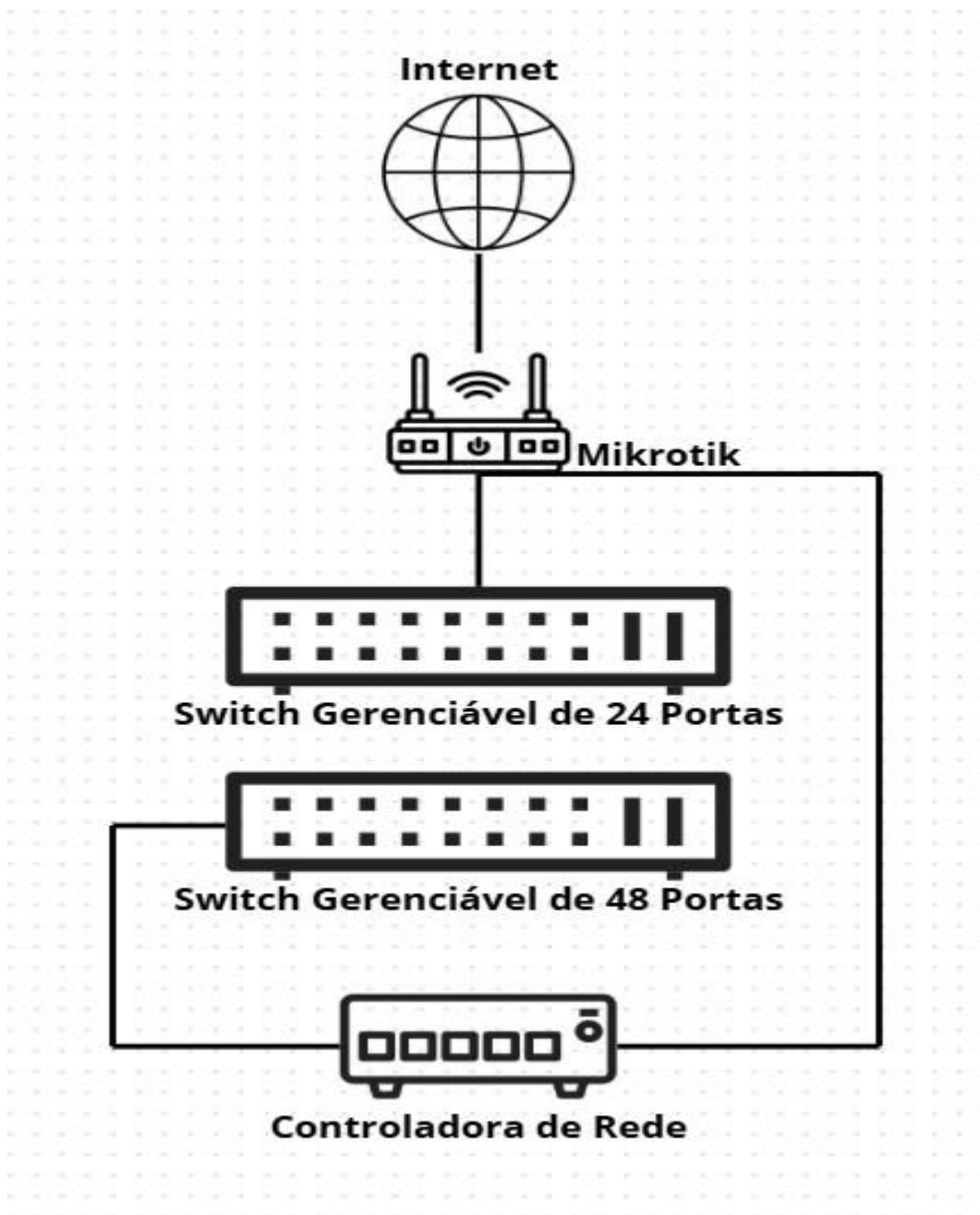
SETOR DE TECNOLOGIA
DA INFORMAÇÃO



Obs.: Este referencial legal serve de base para o planejamento, aquisição, execução e avaliação das ações previstas no PDTI, garantindo conformidade jurídica e alinhamento com boas práticas nacionais e internacionais.



14. Estrutura Atual do CPD – Centro de Processamento de Dados



A atual estrutura do CPD da Prefeitura Municipal de SarapuÍ encontra-se **defasada e carente de padronização**. O ambiente físico e lógico não foi originalmente concebido para atender às necessidades modernas de conectividade, segurança e desempenho exigidas pelas aplicações e demandas da administração pública municipal.





Situação Atual

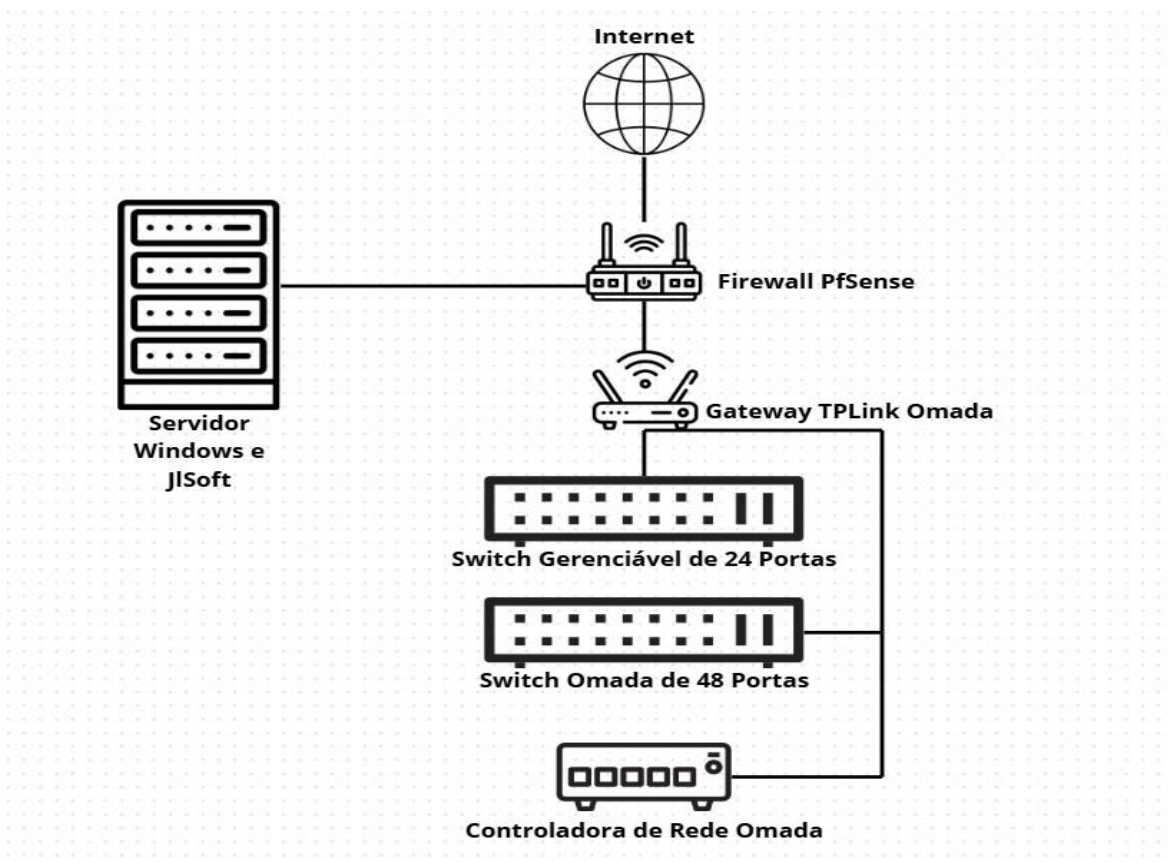
- **Ausência de documentação técnica da rede:** Não existe mapeamento atualizado da topologia da rede, IPs, switches, pontos de acesso ou organização lógica dos setores. Isso compromete tanto a manutenção quanto o crescimento da infraestrutura.
- **Equipamentos antigos e não gerenciáveis:** Parte significativa dos switches em operação não são gerenciáveis e alguns são de padrão residencial, inadequados para ambientes institucionais. O roteador principal também não possui recursos completos de segurança e gerenciamento.
- **Condições físicas do CPD:** O espaço destinado ao CPD não possui climatização adequada, organização de cabos (backbone), controle de acesso físico nem infraestrutura preparada para redundância ou crescimento futuro.
- **Riscos operacionais:** A falta de estrutura adequada compromete a confiabilidade dos serviços, com risco real de paralisações por sobrecarga, falhas de energia, falhas térmicas ou problemas de conectividade.

Necessidade de Reestruturação

- Será necessária a substituição gradual dos equipamentos obsoletos, especialmente switches não gerenciáveis, roteadores residenciais e dispositivos de rede com desempenho limitado.
- A nova estrutura deverá contar com equipamentos de padrão corporativo, gerenciáveis, com suporte a VLAN, QoS, agregação de links e monitoramento centralizado via controlador (como Omada Controller).
- A organização física do CPD deve ser revista, com instalação de rack padrão, sistema de identificação de cabos, ventilação adequada, nobreak, controle de temperatura e backup de energia.
- Deverá ser implementado um sistema de controle de acesso ao CPD, preferencialmente eletrônico e automatizado, com registro digital de entrada e saída de pessoas, seja por leitor de crachá RFID ou leitor biométrico (impressão digital), de forma a registrar de maneira precisa quem acessou o ambiente, a data e o horário do acesso, garantindo a rastreabilidade, segurança e integridade física dos equipamentos.
- Também será desenvolvida a documentação completa da infraestrutura de rede, com diagrama físico e lógico, tabelas de endereçamento IP, reserva de faixas para servidores, VLANs e dispositivos críticos.



15. Diagrama da Estrutura Ideal do CPD



A estrutura ideal do Centro de Processamento de Dados da Prefeitura Municipal de Sarapuí foi planejada para oferecer **maior segurança, desempenho, controle e escalabilidade**, de acordo com as boas práticas em gestão pública de TI. **Descrição Técnica da Topologia Ideal**

- **Firewall pfSense:**

Atua como **primeira camada de proteção da rede**, realizando inspeção de pacotes, controle de tráfego, criação de VLANs, acesso remoto via VPN, filtragem por IP e DNS, failover de internet, logs de auditoria e roteamento seguro. Todo o tráfego da rede passa obrigatoriamente por ele antes de acessar a internet.

- **Gateway TP-Link Omada (ER7206):**

Responsável por distribuir o tráfego interno com base nas VLANs configuradas e gerenciadas pela controladora Omada. Ele **interage com o pfSense**, porém não é o principal firewall da rede, funcionando como gateway de rede local compatível com o ecossistema Omada.

- **Servidor Windows com AD, DNS, DHCP e JLSOFT:**

Servidor centralizado que hospeda os principais serviços de infraestrutura, incluindo:\n

- Active Directory para autenticação e controle de usuários
- DNS e DHCP para resolução e distribuição de IPs internos
- Sistema JLSOFT, hospedado localmente, com acesso remoto via VPN





- Política de backup diário com redundância externa recomendada
- **Switch Gerenciável de 24 Portas:**
Equipamento legado em uso para atender setores menos exigentes ou com número reduzido de dispositivos. Permite configuração de VLANs básicas e monitoramento SNMP.
- **Switch TP-Link Omada de 48 Portas:**
Switch principal, com gerenciamento completo via Omada Controller, suportando VLANs, agregação de links, QoS, prioridade de tráfego, monitoramento em tempo real e integração total com o gateway e demais dispositivos do ecossistema.
- **Controladora de Rede Omada:**
Responsável pela gestão unificada dos dispositivos Omada (switches, gateway e pontos de acesso), permitindo:
 - Visualização gráfica da topologia da rede
 - Criação e controle de SSIDs Wi-Fi com regras separadas por VLAN
 - Agendamento de desligamento de portas e Wi-Fi
 - Monitoramento de tráfego, logs e geração de alertas

Observações Finais sobre a Estrutura Ideal

- Essa estrutura suporta perfeitamente a **criação de sub-redes segmentadas**, políticas específicas por setor e integração futura com prédios externos via VPN site-to-site.
- A **separação entre controle de tráfego (gateway) e segurança avançada (pfSense)** proporciona maior controle e flexibilidade.
- O uso de um **servidor dedicado com serviços de diretório e sistemas locais** permite melhor desempenho, autonomia e redução de dependência externa.
- A rede passa a ser **monitorada em tempo real**, com geração de logs e dados que permitem rápida atuação em falhas ou anomalias.

16. Cronograma Detalhado de Execução

O cronograma abaixo apresenta as etapas de implementação das ações previstas no Plano Diretor de Tecnologia da Informação da Prefeitura Municipal de Sarapuí para o biênio 2026–2027. Ele foi estruturado com base na **prioridade das ações**, na **capacidade técnica do Setor de TI**, e nas **possibilidades orçamentárias da administração municipal**.





PREFEITURA MUNICIPAL DE

SARAPUÍ

SETOR DE TECNOLOGIA
DA INFORMAÇÃO



Período	Ação
2º semestre de 2025	Elaboração e aprovação formal do PDTI
1º semestre de 2026	Requisição de equipamentos para substituição de máquinas obsoletas
1º semestre de 2026	Implantação inicial do firewall pfSense
1º semestre de 2026	Implantação de rede VPN entre setores prioritários
1º semestre de 2026	Estruturação lógica da nova topologia de rede
1º semestre de 2026	Estabelecimento das políticas de TI (uso, segurança, backups)
1º semestre de 2026	1º treinamento: boas práticas de segurança da informação
2º semestre de 2026	Implantação completa do Active Directory e GPOs
2º semestre de 2026	Integração dos computadores à autenticação centralizada
2º semestre de 2026	Configuração e distribuição das VLANs por setor
2º semestre de 2026	Substituição dos switches legados por switches Omada
2º semestre de 2026	Integração do sistema JLSOFT à nova estrutura via VPN
2º semestre de 2026	2º e 3º treinamentos: uso de sistemas e autenticação
2º semestre de 2026	Atualização da documentação da rede física e lógica
1º semestre de 2027	Conclusão da substituição de computadores restantes
1º semestre de 2027	Consolidação do CPD (racks, cabos, nobreaks, climatização)
1º semestre de 2027	Monitoramento ativo da rede com relatórios mensais
1º semestre de 2027	Acompanhamento dos indicadores do PDTI
1º semestre de 2027	4º treinamento: ferramentas colaborativas e produtividade
2º semestre de 2027	Avaliação e ajustes finais das políticas de TI
2º semestre de 2027	Relatório técnico final do PDTI com metas alcançadas





2º semestre de 2025 (final do ano)

- Elaboração e aprovação formal do PDTI.

1º semestre de 2026 (jan a jul)

- Requisição de equipamentos básicos para substituição de máquinas obsoletas.
- Início da implantação do firewall pfSense como camada de segurança primária.
- Implantação inicial da rede VPN entre setores prioritários (Gabinete, Contabilidade, Saúde).
- Estruturação lógica da nova topologia de rede (VLANs planejadas, reservas de IP, documentação).
- Estabelecimento das primeiras políticas de TI (uso, segurança, acesso, backups).
- Primeiro treinamento interno: boas práticas de segurança da informação.

2º semestre de 2026 (ago a dez)

- Implantação completa do Active Directory e GPOs.
- Integração de todos os computadores ativos à nova estrutura com autenticação centralizada.
- Configuração e distribuição definitiva das VLANs por setor.
- Conclusão da substituição dos switches legados por switches compatíveis Omada.
- Integração do sistema JLSOFT à nova estrutura (uso interno via IP fixo e acesso externo via VPN).
- Segundo e terceiro treinamentos: uso de sistemas, autenticação e atendimento básico.
- Atualização da documentação da rede física e lógica.

1º semestre de 2027 (jan a jul)

- Conclusão da substituição de computadores obsoletos restantes.





- Consolidação da estrutura do CPD (racks, organização de cabos, nobreaks e climatização).
- Monitoramento ativo da rede com relatórios mensais.
- Acompanhamento de indicadores de desempenho definidos no PDTI.
- Quarto treinamento: ferramentas colaborativas e produtividade.

2º semestre de 2027 (ago a dez)

- Avaliação e ajustes finais das políticas de TI.
- Relatório técnico final do PDTI com metas alcançadas, aprendizados e recomendações futuras.

Observações Importantes

- O cronograma poderá ser **revisto semestralmente**, de acordo com a evolução das etapas, mudanças orçamentárias ou novas demandas urgentes.
- Algumas ações poderão **ocorrer em paralelo**, desde que não interfiram na estabilidade dos serviços públicos.
- A execução está condicionada à **aprovação orçamentária, licitação e compra** dos equipamentos necessários.

17. Considerações Finais e Aprovação

O Plano Diretor de Tecnologia da Informação 2026–2027 da Prefeitura Municipal de Sarapuí representa o compromisso da gestão pública com a modernização, segurança e eficiência dos recursos tecnológicos, fundamentais para a melhoria dos serviços prestados à população.

A execução das ações previstas neste plano dependerá do esforço coordenado entre o Setor de Tecnologia da Informação, os setores administrativos, o Gabinete do Prefeito e demais órgãos envolvidos, bem como do apoio institucional e da adequada alocação de recursos.

Este documento deverá ser revisado periodicamente para garantir sua adequação às mudanças tecnológicas, às necessidades do município e às diretrizes da administração pública.

Assim, submetemos o presente Plano Diretor de Tecnologia da Informação para aprovação e implementação imediata.

Sarapuí, 23 de outubro de 2025.

Gustavo de Souza Barros Vieira
Prefeito Municipal

Marcos Vinicius Holtz
Diretor de Administração





PREFEITURA MUNICIPAL DE
SARAPUÍ

SETOR DE TECNOLOGIA
DA INFORMAÇÃO



Nicolas Henrique Machado Braz
Técnico em Informática

por Gustavo de Souza Barros Vieira (Senha), Marcos Vinicius Holtz (Senha), Nicolas Henrique Machado Braz (Senha) nos termos da lei 14.063/2020.
Validação de assinaturas: <https://sarapuiweb.jlsoft.com.br/assinador/verificacao.aspx?c11d6325-8541-4b4c-bec8-b9060ad46ec6>

