PDTIC

PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

2026 - 2029

VERSÃO 1.11 - 09/12/2025

PREFEITURA DE ARRAIAL DO CABO

SECRETARIA DE EDUCAÇÃO
CULTURA, CIÊNCIA, TECNOLOGIA, ESPORTE E LAZER

Poder Executivo

Marcelo Magno Félix dos Santos - Prefeito Municipal

Comitê Gestor da Tecnologia da Informação e Comunicação

Victor Hugo Ferreira Fontes
Wellington Rodrigues de Mendonça
Francisco Carlos Lourenço de Mattos
Michelli Fernanda Tito Ferreira Alves
Diogo Sanchez Florentino Santos
Izabela Rocha Macedo Vieira
Débora Viana Barbosa Oliveira
Felipe da Cruz do Amaral

Grupo de Tecnologia e Estratégia Digital

Francisco Carlos Lourenço de Mattos
Lúcio Mauro da Silva
Mário Gonçalves Cardoso Júnior
Luiz Otávio Batista de Paiva

1. APRESENTAÇÃO E FUNDAMENTAÇÃO LEGAL

1.1 - INTRODUÇÃO

O Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) da Prefeitura Municipal de Arraial do Cabo constitui-se como um instrumento estratégico e operacional, coordenado pela Subsecretaria de Ciência e Tecnologia, destinado a orientar os investimentos, a gestão e a utilização dos recursos de TIC em toda a Administração Pública Municipal. Seu propósito é alinhar as iniciativas tecnológicas às diretrizes de governo e às necessidades de todas as secretarias e órgãos municipais, promovendo uma gestão pública mais inclusiva, eficiente, transparente e inovadora.

O plano foi elaborado de forma integrada, contemplando as demandas apresentadas nos Planos de Contratações Anuais (PCA) de TI das secretarias municipais, assegurando que as ações previstas atendam às necessidades específicas de cada área, em consonância com os objetivos institucionais da Prefeitura.

Entre as diretrizes do PDTIC estão a modernização da infraestrutura tecnológica, a ampliação da conectividade, a implantação de sistemas de gestão integrados, a padronização de serviços de suporte, bem como a adoção de soluções que fortaleçam a atividade administrativa e a execução de políticas públicas. Além disso, contempla medidas para aprimorar a segurança da informação, a certificação digital, o controle de acesso e a gestão de dados, assegurando maior confiabilidade e agilidade nos processos internos.

O plano dedica atenção especial à área da educação, prevendo investimentos em equipamentos multimídia, televisores para salas de aula de inglês, serviços de produção audiovisual para os projetos de TV-Educação, cabeamento estruturado para unidades escolares e locação de impressoras. Também estão previstas iniciativas voltadas ao desenvolvimento de competências, como cursos de capacitação, além da aquisição de softwares e ferramentas de pesquisa para apoiar o trabalho técnico e pedagógico.

Com um investimento total estimado em R$ 74.026.351,81 (conforme demonstrado no Anexo II), o PDTIC 2026-2029 consolida-se como um marco para a transformação digital da Prefeitura de Arraial do Cabo. Ao integrar secretarias, otimizar recursos, estimular a cultura digital e fomentar a inovação, o plano assegura que a gestão pública esteja preparada para responder de forma ágil, moderna e segura às demandas da sociedade, colocando a tecnologia como uma aliada estratégica na melhoria da qualidade dos serviços prestados à população.

1.2 - OBJETIVO DO PDTIC

O Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) tem como objetivo principal estabelecer diretrizes estratégicas para o uso eficiente dos recursos tecnológicos, alinhando-os às estratégias e aos objetivos institucionais. Ele atua como um instrumento fundamental de diagnóstico, planejamento e gestão dos recursos e processos de TIC, promovendo a transparência, a governança eficiente e o alinhamento das soluções tecnológicas às metas organizacionais. O PDTIC visa otimizar o uso da tecnologia para aprimorar a qualidade dos serviços públicos, garantir a eficiência operacional e assegurar que os investimentos em TIC contribuam efetivamente para o sucesso institucional. Além disso, orienta a alocação de recursos, o acompanhamento de projetos e a mitigação de riscos relacionados à tecnologia da informação, sempre com foco na melhoria contínua durante o período de vigência do plano. Dessa forma, o PDTIC apoia a governança digital e a entrega de soluções alinhadas às necessidades estratégicas do órgão ou entidade, promovendo a sustentabilidade e o aprimoramento contínuo dos negócios e serviços oferecidos.

1.3 - FUNDAMENTAÇÃO LEGAL

A elaboração do plano, baseia-se em leis federais e decretos municipais, relatórios técnicos, documentação interna, a saber:

- **Lei Municipal 2.623/2025** – Criação do CGTIC (Comitê Gestor de Tecnologia da Informação e Comunicação).
- **Decreto Municipal 4.354/2025** – Dispõe sobre as competências, atribuições e regulamentação do Comitê Gestor de Tecnologia da Informação e Comunicação (CGTIC) e dos Conselhos Deliberativos e Consultivos do Município de Arraial do Cabo, em conformidade com a Lei Municipal nº 2.623/2025, que instituiu o referido Comitê no âmbito do Município de Arraial do Cabo.
- **Lei Federal nº 14.129/2021** - Lei do Governo Digital.
- **Decreto Municipal 4.367/2025** - Dispõe sobre a regulamentação da aplicação da Lei Federal nº 14.129/2021, de 29 de março de 2021, no âmbito da Administração Municipal.
- **Lei Municipal 2.641/2025** – Institucionaliza a Política de Tecnologia da Informação no âmbito do Município de Arraial do Cabo, e dá outras providências.
- **Lei Federal nº 13.460/2017** - Dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública.
- **Decreto Municipal 4.370/2025** – Regulamenta na Administração Pública Municipal nos termos da Lei Federal nº 13.460 de 26 de junho de 2017 que dispõe sobre a proteção e defesa dos direitos dos usuários dos serviços públicos do Poder Executivo Municipal de Arraial do Cabo e dá outras providências.

- **Decreto Municipal 4.368/2025** – Regulamenta o uso de assinaturas eletrônicas na Administração Pública Municipal, nos termos da Lei Federal nº 14.063, de 23 de setembro de 2020, quanto ao nível mínimo exigido para a assinatura eletrônica em interações com o ente público.
- **Lei Federal nº 13.709/2018** - Lei Geral de Proteção de Dados Pessoais (LGPD).
- **Lei Federal nº 12.965/2014** - Marco Civil da Internet.
- **Lei Federal nº 12.527/2011** – Lei de Acesso à Informação.
- **Decreto Municipal 4.369/2025** - Institui a Política de Dados Abertos do Poder Executivo Municipal de Arraial do Cabo e dá outras providências.
- **Decreto Municipal 4.458/2025** - Institui a Estratégia de Governo Digital para o município de Arraial do Cabo no período de 2025 a 2035.
- **Decreto Municipal 3.900/2022** – Seção VI – Art. 58 a Art. 77 – Regulamenta o desfazimento de bens móveis.

1.4 - VIGÊNCIA DO PLANO

Este Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) terá vigência estabelecida por um período de quatro anos, abrangendo o intervalo temporal compreendido entre os anos de 2026 e 2029. Durante esse ciclo de vigência, o PDTIC servirá como um instrumento estratégico fundamental para orientar o planejamento, a implementação e a gestão dos recursos e ações relacionados à tecnologia da informação e comunicação na organização. Além disso, para garantir que o plano permaneça alinhado às necessidades reais e atuais da instituição, ele poderá ser objeto de revisões periódicas sempre que forem identificadas demandas emergentes, mudanças no ambiente tecnológico ou avanços significativos que justifiquem ajustes. Essas revisões visam assegurar que o PDTIC mantenha sua relevância, eficácia e adequação, acompanhando a evolução tecnológica e as transformações estratégicas da entidade ao longo do período estabelecido. Dessa forma, o PDTIC não apenas definirá uma direção clara para a gestão de TIC nos próximos quatro anos, como também permitirá a flexibilidade necessária para adaptações tempestivas face a novos desafios e oportunidades.

1.5 - JUSTIFICATIVA E IMPORTÂNCIA DO PLANO

O Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) é fundamental para garantir uma gestão eficiente, transparente e alinhada dos recursos e processos de TIC em qualquer organização, especialmente na esfera pública, onde os recursos são limitados e a responsabilidade social é evidente. A justificativa para sua elaboração reside na necessidade de articular as estratégias tecnológicas com os objetivos institucionais, otimizando os investimentos e minimizando desperdícios. Além disso, o PDTIC propicia um planejamento claro e orientado, que permite priorizar ações, mitigar riscos e acompanhar resultados, contribuindo para a melhoria contínua da qualidade dos serviços oferecidos à sociedade.

A importância do PDTIC está justamente em sua capacidade de suportar a governança digital, promover a transparência na alocação e uso dos recursos tecnológicos e assegurar que as ações de TIC estejam diretamente alinhadas às demandas e metas estratégicas da organização. Isso possibilita não só a eficiência operacional e a sustentabilidade dos investimentos, mas também a entrega de valor público por meio da inovação, agilidade e confiabilidade nos serviços. Dessa forma, o PDTIC é um instrumento essencial para fortalecer a gestão de TIC e garantir que as tecnologias da informação sejam um diferencial no cumprimento da missão institucional.

1.6 - METODOLOGIA

PROCESSO DE ELABORAÇÃO

O PDTIC foi elaborado por meio de um processo participativo que envolveu reuniões e questionários, com os principais stakeholders dos setores de TIC e áreas-fim, garantindo o alinhamento com a estratégia institucional.

PARTICIPAÇÃO DAS ÁREAS ENVOLVIDAS

Todas as áreas da Prefeitura Municipal de Arraial do Cabo que possuem interface tecnológica estiveram diretamente e de forma ativa envolvidas nas etapas fundamentais de diagnóstico e validação das propostas apresentadas. Essa participação ativa foi crucial para garantir que todas as ações planejadas estivessem devidamente alinhadas e aderentes às necessidades concretas e específicas da administração municipal, considerando suas particularidades e demandas institucionais. A colaboração efetiva entre essas áreas assegurou que as soluções desenvolvidas fossem adequadas, factíveis e voltadas para o atendimento das reais prioridades da gestão pública, promovendo, assim, maior eficiência e eficácia na execução das iniciativas tecnológicas contempladas.

1.7 - ALINHAMENTO ESTRATÉGICO: AGENDA ONU 2030, PLANO DE GOVERNO E PLANO PLURIANUAL (PPA)

O Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2026–2029 da Prefeitura Municipal de Arraial do Cabo está alinhado à Agenda 2030 da ONU, especialmente aos Objetivos de Desenvolvimento Sustentável (ODS 4, 9, 11 e 16), que tratam de educação de qualidade, inovação, infraestrutura e instituições eficazes.

Esse alinhamento assegura que os investimentos em tecnologia fortaleçam a governança pública, promovam a inclusão digital e impulsionem o desenvolvimento sustentável do município.

O PDTIC também está integrado ao Plano de Governo 2025–2028, que prioriza a transformação digital, a transparência e a eficiência administrativa, consolidando as ações de TIC como ferramentas estratégicas para modernizar os serviços públicos.

De forma transversal, o plano conecta-se ao Plano Plurianual (PPA), garantindo que os projetos tecnológicos estejam vinculados às metas orçamentárias e estratégicas, promovendo sinergia entre os compromissos da Agenda 2030, as diretrizes locais e a inovação centrada no cidadão.

Relacionamento dos 17 ODS com Atividades no PDTIC

ODS	Atividades TIC Relacionadas	Tipo de Impacto
ODS 1 – Erradicação da pobreza	• Sistemas de benefícios sociais com base em dados; • Internet gratuita em áreas de baixa renda; • Investir em plataformas de capacitação digital; • Sites de oportunidades de emprego.	Social / Econômico / Ambiental
ODS 2 – Fome zero e agricultura sustentável	Apps para ajudar na redução do desperdício de alimentos, como por exemplo: Too Good To Go e Food to Save.	Social / Econômico / Ambiental
ODS 3 – Saúde e bem-estar	• **Prontuários Eletrônicos e Bases de Dados Médicas:** O uso de dispositivos móveis com acesso à internet integra sistemas e prontuários eletrônicos, permitindo que profissionais de saúde acessem informações essenciais sobre pacientes em tempo real, favorecendo diagnósticos mais rápidos e tratamentos eficazes. • **Monitoramento e Diagnóstico Remoto (Internet das Coisas):** Dispositivos conectados permitem o acompanhamento de pacientes à distância (telemedicina), facilitando o monitoramento de condições	Social / Econômico / Ambiental

crônicas e o acompanhamento domiciliar, o que é fundamental para regiões remotas e populações vulneráveis.

- **Acesso a Informações e Educação para Saúde:**

Plataformas digitais permitem a disseminação de campanhas educativas, orientação sobre prevenção de doenças e promoção do autocuidado, potencializando o alcance das políticas públicas de saúde.

- **Cobertura Universal de Saúde:**

TICs auxiliam na gestão de recursos e indicadores em saúde, apoiando a ampliação do acesso e da qualidade dos serviços, mecanismos relevantes para alcançar a cobertura universal de saúde prevista no ODS 3.

- **Resposta Rápida a Epidemias e Situações de Emergência:**

Sistemas digitais integrados promovem o alerta precoce, a vigilância epidemiológica e a resposta coordenada em situações de risco sanitário, contribuindo para controlar epidemias e outras emergências.

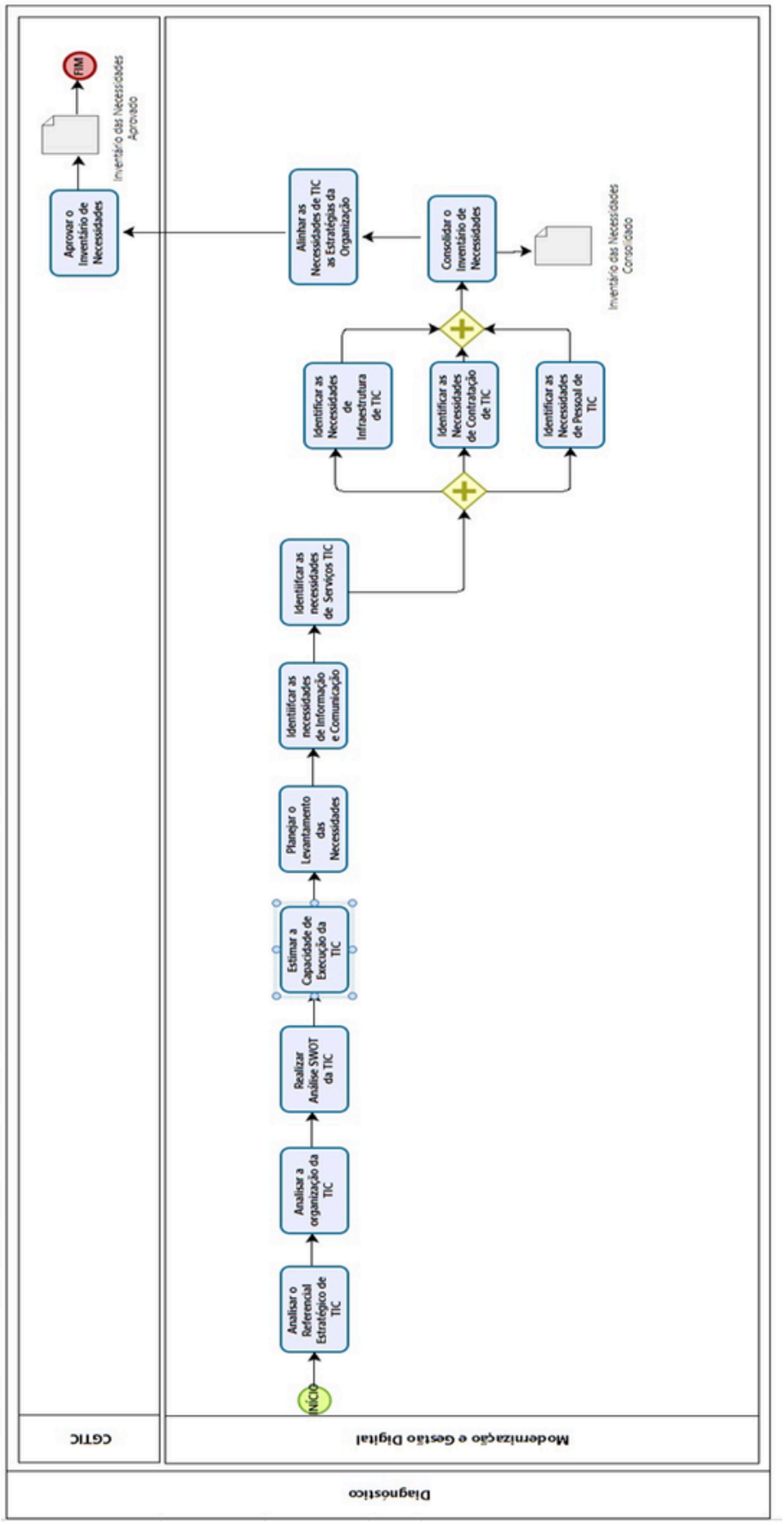
- **Pesquisa e Desenvolvimento:**

TICs facilitam o compartilhamento de dados para pesquisa médica, viabilizando o desenvolvimento de medicamentos, vacinas e tratamentos inovadores contra doenças transmissíveis e não transmissíveis.

ODS 4 – Educação de qualidade	• Expandir ambientes virtuais de aprendizagem; • Gestão escolar digital; • Inclusão digital nas escolas	Social / Econômico / Ambiental
ODS 5 – Igualdade de gênero	• Indicadores de igualdade; • Canais de denúncia online; • Capacitação de mulheres em TIC	Social / Econômico / Ambiental
ODS 6 – Água potável e saneamento	• Monitoramento hídrico por sensores; • Alerta de qualidade da água	Social / Econômico / Ambiental
ODS 7 – Energia limpa e acessível	• Monitoramento de consumo energético; • Data centers verdes	Social / Econômico / Ambiental
ODS 8 – Trabalho decente e crescimento econômico	• Automatização de processos; • Plataformas de empregabilidade e capacitação; • Fomentar startups de tecnologia com impacto social	Social / Econômico / Ambiental
ODS 9 – Indústria, inovação e infraestrutura	• Parcerias com Instituições de Ensino; • Ambientes de inovação aberta	Social / Econômico / Ambiental
ODS 10 – Redução das desigualdades	• Portais inclusivos; • Dados abertos; • Projetos de inclusão digital • Democratizar o acesso à internet em áreas remotas (distritos)	Social / Econômico / Ambiental

ODS 11 – Cidades e comunidades sustentáveis	• Desenvolver soluções de Cidades inteligentes (smart cities); • Transporte inteligente; • Gestão de resíduos	Social / Econômico / Ambiental
ODS 12 – Consumo e produção responsáveis	• Controle sustentável de compras públicas; • Implementar políticas de descarte sustentável de equipamentos; • Monitorar o ciclo de vida dos ativos de TI	Social / Econômico / Ambiental
ODS 13 – Ação contra a mudança global do clima	• Monitoramento de emissões; • Soluções em nuvem; • Incentivo ao teletrabalho	Social / Econômico / Ambiental
ODS 14 – Vida na água	• Sensores para qualidade da água; • Alertas de contaminação	Social / Econômico / Ambiental
ODS 15 – Vida terrestre	• Geoprocessamento; • Monitoramento de queimadas e áreas protegidas	Social / Econômico / Ambiental
ODS 16 – Paz, justiça e instituições eficazes	• Portais de transparência; • Sistemas de ouvidoria; • Segurança da informação; • Automação de processos administrativos	Social / Econômico / Ambiental
ODS 17 – Parcerias e meios de implementação	• Interoperabilidade; • Parcerias com academia e setor privado; • Estabelecer cooperação com universidades e ONGs	Social / Econômico / Ambiental

2. ANÁLISE DO REFERENCIAL ESTRATÉGICO DE TIC



2.1 - MISSÃO

Promover um ambiente inovador no município de Arraial do Cabo, tornando os serviços públicos mais sustentáveis, integrados e centrados no cidadão.

2.2 - VISÃO

Transformar Arraial do Cabo em uma cidade mais conectada, integrada e eficiente, por meio de políticas inclusivas e serviços de qualidade, acessíveis e focados nas necessidades das pessoas.

2.3 - VALORES

- Inovação contínua;
- Transparência e ética;
- Foco no usuário/cliente;
- Segurança da informação;
- Sustentabilidade digital

2.4 – OBJETIVOS ESTRATÉGICOS DE TIC

- Garantir infraestrutura tecnológica segura, escalável e disponível;
- Promover a transformação digital dos serviços públicos;
- Assegurar governança e gestão eficiente dos recursos de TIC;
- Estimular a inovação e a integração entre sistemas e secretarias;
- Garantir a proteção de dados e a conformidade legal;
- Ampliar a transparência, a participação social e a acessibilidade digital.

Médio prazo (2 a 3 anos)

- Modernização da infraestrutura de redes e sistemas;
- Padronização de processos de TIC nas secretarias;
- Implantação de serviços digitais acessíveis ao cidadão;
- Melhoria na segurança da informação e no controle de acessos;
- Criação de painéis de monitoramento para apoio à decisão;

Longo prazo (4 a 10 anos)

- Consolidação do Governo Digital no município;
- Integração total dos sistemas de gestão pública;
- Cultura organizacional orientada a dados e inovação;
- Sustentabilidade tecnológica com custos otimizados;
- Reconhecimento de Arraial do Cabo como referência em gestão pública digital na região.

3. ANÁLISE DA ORGANIZAÇÃO DA TIC

3.1 - ESTRUTURA ORGANIZACIONAL

A TIC está centralizada na Subsecretaria de Ciência e Tecnologia favorecendo padronização e governança. A organização da TIC deve ser vista como eixo estratégico da administração municipal. Quando bem estruturada, possibilita eficiência administrativa, serviços digitais acessíveis ao cidadão e maior transparência.
Quanto à capacitação dos servidores, é imperioso destacar a necessidade de investimentos em cursos de capacitação (infraestrutura, sistemas, suporte, segurança e inovação), visto à constatação que em quase sua totalidade a organização possui autodidatas.

3.2 - GOVERNANÇA E GESTÃO

- Políticas e Normas: atualmente inexistem normativos voltados a definir diretrizes para aquisição, uso e gestão de TIC;
- Planejamento Estratégico de TIC: os objetivos da TIC estão alinhados aos objetivos estratégicos da prefeitura;
- Gestão de Projetos: as iniciativas digitais são planejadas em ondas (fases), onde prioridades, metas e objetivos são definidos e estimados de forma estruturada.

3.3 - INFRAESTRUTURA TECNOLÓGICA

O mapeamento da infraestrutura tecnológica da Prefeitura Municipal de Arraial do Cabo evidenciou diversas fragilidades que impactam diretamente a eficiência, segurança e continuidade dos serviços públicos.

Redes e Conectividade:
A avaliação da infraestrutura de redes revelou problemas críticos que afetam disponibilidade, desempenho e segurança:

- Oscilações de velocidade e interrupções frequentes no tráfego de internet;
- Ausência de redundância de link, com dependência de infraestrutura terceirizada;
- Topologia interna de rede inadequada e mal configurada pelo provedor;
- Equipamentos residenciais (switches e roteadores) utilizados em rede de grande porte;
- Ausência de nobreaks em pontos estratégicos da rede;
- Cabeamento de rede não homologado e fora dos padrões;
- Equipamentos de rede expostos a acesso não autorizado;
- Infraestrutura interna não atende às normas técnicas vigentes.

Essas vulnerabilidades aumentam o risco de interrupções nos serviços e comprometem a segurança da informação. Recomenda-se:

- Revisão completa da topologia e padronização do cabeamento;
- Substituição de equipamentos inapropriados por soluções corporativas;
- Implantação de redundância de links e nobreaks estratégicos;
- Restrição física e lógica de acesso aos equipamentos;
- Monitoramento contínuo e manutenção preventiva da rede.

Servidores e Armazenamento:

Atualmente, a prefeitura dispõe de cinco servidores próprios, sendo apenas dois atualizados com hardware recente, e três VPS contratados em ambiente de nuvem. O ambiente apresenta fragilidades relevantes, tais como:

- Uso de um computador adaptado como servidor de pastas, sem configuração adequada;
- Ausência de espaço em disco suficiente para suportar as demandas atuais;
- Utilização de HDs antigos e fora dos padrões recomendados para armazenamento corporativo;
- Armazenamento de dados realizado localmente em algumas secretarias, de forma descentralizada, sem uso de datacenter ou ambiente centralizado.

Equipamentos e Suporte:

O mapeamento do parque tecnológico municipal evidenciou que parte significativa dos equipamentos encontra-se em estado de obsolescência ou inadequada às demandas atuais, o que compromete a eficiência e a continuidade dos serviços. Constatou-se a necessidade de investimentos imediatos em renovação e padronização do parque tecnológico, além da estruturação de um plano de suporte técnico capaz de garantir maior disponibilidade e desempenho. Recomenda-se investimento imediato em renovação do parque tecnológico, padronização de equipamentos e estruturação de um suporte técnico centralizado e eficiente.

3.4 - SISTEMAS E APLICAÇÕES

3.4.1 - Situação Atual:

- Há sistemas administrativos e de gestão em uso, alguns desenvolvidos internamente e outros adquiridos de fornecedores externos;
- Convivem aplicações modernas com outras já defasadas, que dificultam a integração de dados;
- Ausência de catálogo oficial de sistemas em produção, o que dificulta controle e governança.

3.4.2 - Pontos Positivos:

- Sistemas essenciais para o funcionamento administrativo estão operacionais;

Adoção parcial de soluções em nuvem (VPS).

3.4.3 - Fragilidades:

- Falta de integração entre sistemas;
- Dependência de soluções isoladas e não padronizadas;
- Uso de planilhas e registros manuais em algumas áreas, com risco de duplicidade e inconsistência.

3.4.3 - Recomendações:

- Elaborar um inventário e catálogo de sistemas;
- Priorizar a integração entre aplicações para eliminar redundâncias;
- Avaliar a migração gradual para soluções centralizadas ou em nuvem com maior escalabilidade.

3.5 - SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS

3.5.1 - Situação Atual:

- Não há política formalizada de segurança da informação;
- Backups são feitos, mas de forma descentralizada e sem rotinas claras de auditoria;
- Falhas de controle de acesso e de uso de equipamentos pessoais para atividades institucionais.

3.5.2 - Pontos Positivos:

- Existe consciência inicial da necessidade de segurança;
- Alguns setores já adotam práticas de senhas e restrição de acessos básicos.

3.5.3 - Fragilidades:

- Risco elevado de perda de dados ou vazamento de informações sensíveis;
- Ausência de Plano de Recuperação de Desastres (PRD) e de continuidade de serviços críticos;
- Falta de treinamento da equipe e dos usuários quanto à proteção de dados.

3.5.4 - Recomendações:

- Criar e implantar uma Política de Segurança da Informação alinhada às normas ISO/IEC 27001 e à LGPD;
- Estruturar rotinas de backup centralizado, com testes regulares de restauração;
- Implantar controle de acessos, autenticação forte e segregação de funções;
- Desenvolver plano de contingência e recuperação de desastres.

3.6 - CULTURA DIGITAL E CAPACITAÇÃO

3.6.1 - Situação Atual:

- O uso de TIC ainda é visto por muitos servidores apenas como suporte operacional, e não como ferramenta estratégica;

- Baixo índice de capacitação contínua em sistemas, governança e boas práticas digitais;
- Resistência cultural a mudanças e adoção de novas tecnologias em alguns setores.

3.6.2 - Pontos Positivos:
- Há disposição de parte da equipe em participar de cursos e treinamentos;
- Projetos digitais recentes geraram maior aceitação do uso de tecnologia.

3.6.3 - Fragilidades:
- Ausência de programa formal de capacitação;
- Desigualdade no domínio das ferramentas digitais entre os usuários;
- Baixa cultura de inovação.

3.6.4 - Recomendações:
- Implantar um programa permanente de capacitação digital, contemplando tanto a equipe de TIC quanto os usuários finais;
- Promover campanhas de alfabetização digital e sensibilização sobre uso seguro da tecnologia e da informação;
- Estimular a cultura de inovação por meio de oficinas, laboratórios de tecnologia e incentivo à automação de processos.

3.6.5 – Alinhamento Estratégico
Integração com o plano Plurianual (PPA), Lei de Diretrizes Orçamentárias (LDO), Plano de Governo, Auditorias – TCE-RJ e demais políticas públicas municipais.

3.6.5.1 – Princípios
Transparência, inovação, eficiência, ética, sustentabilidade, segurança da informação, gestão de riscos e qualidade, foco no atendimento aos usuários, acessibilidade, capacitação e desenvolvimento e governança e transparência inclusão digital.

3.6.5.2 – Contexto Organizacional e Tecnológico
O presente plano considera a estrutura interna da organização, suas unidades gestoras, além dos recursos tecnológicos disponíveis atualmente, analisando o cenário local e as tendências tecnológicas aplicáveis ao serviço público.

3.6.5.3 – Diagnóstico Situacional de Tecnologia da Informação
3.6.5.3.1 – Inventário de Recursos Tecnológicos
Hardware: levantamento dos equipamentos em uso como servidores, estações de trabalho, notebooks, periféricos e dispositivos móveis.

INVENTÁRIO DE RECURSOS TECNOLÓGICOS - SUBSECRETARIAS / AUTARQUIAS – CENÁRIO ATUAL

	TOTAL GERAL		
	773	196	63
SETOR	Funcionários	Computadores C/Patrimônio	Impressoras C/Patrimônio
Controladoria Geral do Município	25	3	2
Gabinete do Prefeito	30	6	2
Gabinete do Vice-Prefeito	8	0	0
Procuradoria Geral do Município	28	4	1
Secretaria de Compras e Licitação	18	0	0
Secretaria de Desenvolvimento Social, Trabalho, Renda e Direitos Humanos	94	39	18
Secretaria de Educação – Subsecretaria de Ciência e Tecnologia	60	22	6
Secretaria de Governo	8	1	2
Secretaria de Habitação e Regularização Fundiária	27	2	0
Secretaria de Mobilidade Urbana	30	0	0
Secretaria de Obras e Urbanismo	51	17	2
Secretaria de Postura	15	2	0
Secretaria de Proteção e Defesa do Consumidor – PROCON	5	4	1
Secretaria Municipal de Administração	60	22	6
Secretaria Municipal de Administração Tributária	30	9	4
Secretaria Municipal de Finanças e Orçamento	22	5	1
Secretaria Municipal de Saúde	98	18	7
Secretaria Municipal de Segurança Pública	39	7	0
Secretaria Municipal de Serviços Públicos	21	0	0
Secretaria Municipal de Turismo	56	7	2
Secretaria Municipal do Ambiente e Saneamento	48	28	9

INVENTÁRIO DE RECURSOS TECNOLÓGICOS - SUBSECRETARIAS / AUTARQUIAS – CENÁRIO DESEJADO

	TOTAL GERAL									
	781	781	71	20	1	1	781	4	1	2
SETOR	Funcionários	Computadores	Impressoras Monocromáticas	Impressoras Coloridas	Impressoras Tam. A0	Impressoras Tam.A3	Nobreaks p/ PC's	Nobreaks p/ Servidores	Geradores de Energia	Datacenter
Controladoria Geral do Município	33	33	3	1			33			
Gabinete do Prefeito	30	30	3	2			30			
Gabinete do Vice-Prefeito	8	8	1	1			8			
Procuradoria Geral do Município	28	28	2				28			
Sec. Mun. de Compras e Licitação	18	18	1	1			18			
Sec. Mun. de Desenvolvimento Social, Trabalho, Renda e Direitos Humanos	94	94	10	2			94			
Sec. Mun. de Educação – Subsecretaria de Ciência e Tecnologia	60	60	4	1			60	4	1	2
Sec. Mun. de Governo	8	8	1	1			8			
Sec. Mun. de Habitação e Regularização Fundiária	27	27	1	1	1		27			
Sec. Mun. de Mobilidade Urbana	30	30	2	1			30			
Sec. Mun. de Obras e Urbanismo	51	51	4	1		1	51			
Sec. Mun. de Postura	15	15	2				15			
Sec. Mun. De Proteção e Defesa do Consumidor – PROCON	5	5	1	1			5			
Sec. Mun. de Administração	60	60	4	1			60			
Sec. Mun. de Administração Tributária	30	30	3				30			
Sec. Mun. de Finanças e Orçamento	22	22	3	1			22			
Sec. Mun. de Saúde	98	98	13	1			98			
Sec. Mun. de Segurança Pública	39	39	5	1			39			
Sec. Mun. de Serviços Públicos	21	21	2	1			21			
Sec. Mun. de Turismo	56	56	2	1			56			
Sec. Mun. do Ambiente e Saneamento	48	48	4	1			48			

3.6.5.3.2 – Softwares – inventário das aplicações instaladas, incluindo sistemas corporativos, utilitários e softwares livres.

SECRETARIAS / AUTARQUIAS	SISTEMAS, UTILITÁRIOS E SOFTWARES UTILIZADOS
CONTROLADORIA GERAL	• ADOBE ACROBAT • PJE OFFICE • SHODO • ASSINADOR LIVRE MOBILE ID • GOOGLE CHROME • FIREFOX • SIOPE • NOVO ASSINADOR DIGITAL TCE/RJ • ANYDESK • MICROSOFT OFFICE • MICROSOFT EDGE • MICROSOFT WINDOWS • SISTEMA DE GESTÃO PÚBLICA – MODERNIZAÇÃO PÚBLICA o CONTABILIDADE o FOLHA DE PAGAMENTO o LICITAÇÕES o LEIS E DIRETRIZES ORÇAMENTARIAS o PROTOCOLO o ALMOXARIFADO
FIPAC – FUNDAÇÃO INSTITUTO DE PESCA DE ARRAIAL DO CABO	• SISTEMA DE BILHETERIA – CONTROLE DE INGRESSOS / RECEITA – SOLUÇÃO DESENVOLVIDA PELA PRÓPRIA FIPAC. • SISTEMA WEB PRÓPRIO – GESTÃO OPERACIONAL • SISTEMA DE GESTÃO PÚBLICA – MODERNIZAÇÃO o PROTOCOLO • MICROSOFT EDGE • MICROSOFT OFFICE • MICROSOFT WINDOWS • ADOBE ACROBAT (READER/STANDARD) • WINRAR • CORELDRAW • AUTOCAD • SOLIDWORKS • MS PROJECT

FUNTEC – FUNDAÇÃO DO MEIO-AMBIENTE	• QGIS • ANACONDA • R • OCEAN DATA VIEW • ADOBE PHOTOSHOP • COREL DRAW • AUTOCAD • SISTEMA DE GESTÃO PÚBLICA MODERNIZAÇÃO o PROTOCOLO o ALMOXARIFADO o PATRIMÔNIO • MICROSOFT OFFICE • MICROSOFT WINDOWS
GABINETE DO PREFEITO	• ADOBE ILUSTRATOR • ADOBE PHOTOSHOP • ADOBE INDESIGN • ADOBE AFTER EFFECTS • ADOBE PREMIERE PRO • CAPCUT • CANVA • CLIPSTUDIO • CORELDRAW • SISTEMA DE GESTÃO PÚBLICA – MODERNIZAÇÃO o PROTOCOLO • MICROSOFT EDGE • MICROSOFT OFFICE • MICROSOFT WINDOWS • VEGAS PRO
IPC - INSTITUTO DE PREVIDÊNCIA CABISTA	• SISTEMA DE GESTÃO PÚBLICA – MODERNIZAÇÃO o PROTOCOLO o PATRIMÔNIO o ALMOXARIFADO o TRANSPARÊNCIA - IPC o FOLHA DE PAGAMENTO o CONTABILIDADE • GERPEV – PLATAFORMA DE GESTÃO PREVIDENCIÁRIA – SAAS

	• SISTEMA DE GESTÃO SUPERNOVA (LEGADO) o FOLHA DE PAGAMENTO • MICROSOFT EDGE • MICROSOFT OFFICE • MICROSOFT WINDOWS
PROCURADORIA GERAL	• DROPBOX – (DRIVE EM NUVEM) • ADOBE READER • SISTEMA DE GESTÃO PÚBLICA – MODERNIZAÇÃO o PROTOCOLO • PJE OFFICE • SHODO • ASSINADOR LIVRE MOBILE ID • MICROSOFT EDGE • MICROSOFT OFFICE • MICROSOFT WINDOWS
SECRETARIA DE CULTURA E ECONOMIA CRIATIVA	• ADOBE LIGHTROOM • ADOBE PHOTOSHOP • ARCGIS • ARGUS • AUTOCAD • CANVA • CAPCUT • CORELDRAW • FOTOR • GIMP • INKSCAPE • INPATRIMONIUM • KOHA • MICROSOFT EDGE • MICROSOFT OFFICE • MICROSOFT WINDOWS • PICSART • PERGAMUM • SISTEMA DE GESTÃO PÚBLICA – MODERNIZAÇÃO o PROTOCOLO • PHOTOGRID • POLLAR • PAINT.NET

	• PHOTOSCAPE • PIXIR • QGIS • SKETCHUP • SOFIA • SNAPSEED • VSCO • V-RAY • REVIT
SECRETARIA DE DEFESA DO CONSUMIDOR - PROCON	• PROCONSUMIDOR • MICROSOFT EDGE • MICROSOFT OFFICE • MICROSOFT WINDOWS
SUBSECRETARIA DE ESPORTE E LAZER	• SISTEMA DE GESTÃO PÚBLICA – MODERNIZAÇÃO o PROTOCOLO • MICROSOFT EDGE • MICROSOFT OFFICE • MICROSOFT WINDOWS
SECRETARIA DE FINANÇAS E ORÇAMENTO	• SISTEMA DE GESTÃO PÚBLICA – MODERNIZAÇÃO o PROTOCOLO o CONTABILIDADE o TESOURARIA o TRANSPARÊNCIA o COMPRAS E LICITAÇÃO • SERPRO – RECEITA FEDERAL – GOV.BR • ANYDESK • CANVA PRO • TEAMVIEWER • APLICATIVOS BANCÁRIOS • MICROSOFT EDGE • MICROSOFT OFFICE • MICROSOFT WINDOWS
SECRETARIA DE HABITAÇÃO E REGULARIZAÇÃO FUNDIÁRIA	• AUTOCAD • SKETCHUP • SISTEMA DE GESTÃO PÚBLICA – MODERNIZAÇÃO o PROTOCOLO

	• MICROSOFT EDGE • MICROSOFT OFFICE • MICROSOFT WINDOWS
SECRETARIA DE SEGURANÇA PÚBLICA	• MICROSOFT EDGE • MICROSOFT OFFICE • MICROSOFT WINDOWS • SISTEMA DE GESTÃO PÚBLICA – MODERNIZAÇÃO o PROTOCOLO • SISTEMA GAIDE (DETRAN) • PRODEC – PROGRAMA DE REGISTRO DE OCORRÊNCIAS EM DEFESA CIVIL • S2ID – SISTEMA INTEGRADO DE INFORMAÇÕES SOBRE DESASTRES
SECRETARIA DE SERVIÇOS PÚBLICOS	• GOOGLE WORKSPACE • SISTEMA DE CADASTRO DE REQUERENTES – SAC – PROPRIETÁRIO CRUD • WINRAR • DROPBOX • MICROSOFT EDGE • MICROSOFT OFFICE • MICROSOFT WINDOWS
SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO TRIBUTÁRIA	• SISTEMA DE GESTÃO PÚBLICA – MODERNIZAÇÃO o PROTOCOLO o CADASTRO IMOBILIÁRIO E ARRECADAÇÃO DE IPTU o ISS o DIVIDA ATIVA o ARRECADAÇÃO DE TRIBUTOS o EMISSÃO E FISCALIZAÇÃO DE ALVARÁS • MICROSOFT EDGE • MICROSOFT OFFICE • MICROSOFT WINDOWS
SECRETARIA MUNICIPAL DE COMPRAS E LICITAÇÃO	• ADOBE ACROBAT READER • BANCO DE PREÇOS • PNCP – PORTAL NACIONAL DE CONTRATAÇÕES PÚBLICAS

	• PORTAL DE COMPRAS DO GOVERNO FEDERAL • SIGFIS – SISTEMA INTEGRADO DE GESTÃO FISCAL DO TCE/RJ • GOOGLE WORKSPACE • SISTEMA DE GESTÃO PÚBLICA – MODERNIZAÇÃO o PROTOCOLO o TRANSPARÊNCIA o COMPRAS E LICITAÇÃO • MICROSOFT OFFICE • MICROSOFT WINDOWS
SECRETARIA MUNICIPAL DE MOBILIDADE URBANA	• AUTOCAD • SISTEMA DE GESTÃO PÚBLICA – MODERNIZAÇÃO o PROTOCOLO • MICROSOFT EDGE • MICROSOFT OFFICE • MICROSOFT WINDOWS • MICROSOFT ONEDRIVE (DRIVE EM NUVEM) • QGIS
SECRETARIA MUNICIPAL DE SAÚDE	• SISTEMA DE GESTÃO PÚBLICA – MODERNIZAÇÃO o PROTOCOLO • MICROSOFT EDGE • MICROSOFT OFFICE • MICROSOFT WINDOWS **SETOR DO CENES** • https://pecsus.arraial.rj.gov.br • https://egetoraps.saude.gov.br/ • https://cadastro.saúde.gov.br • https://siscan.saude.gov.br/login.jsf **SETOR DO TFD (TRATAMENTO FORA DO DOMCÍLIO)** • http://www.regulacao.niteroi.rj.gov.br:8080/ser/login • http://www.sisregiii.saude.gov.br/cgi´bin/index# • https://cabofrio.ecosistemas.com.br/ser/login.xhtml • https://ser.saude.rj.gov.br/ser/home?cid=5187 • https://ser.saude.rj.gov.br/trs/ • https://cadastro.saude.gov.br

SECRETARIA MUNICIPAL DE ORDEM PÚBLICA, POSTURAS E FISCALIZAÇÃO	• SISTEMA DE GESTÃO PÚBLICA – MODERNIZAÇÃO o PROTOCOLO o ALMOXARIFADO o FOLHA DE PAGAMENTO o SISTEMA DE ARRECADAÇÃO MUNICIPAL • MICROSOFT EDGE • MICROSOFT OFFICE • MICROSOFT WINDOWS • SISTEMA DE POSTURAS: https://postura.arraial.rj.gov.br/login
SECRETARIA MUNICIPAL DO AMBIENTE E SANEAMENTO	• SISTEMA DE GESTÃO PÚBLICA – MODERNIZAÇÃO o PROTOCOLO o CONTABILIDADE o ALMOXARIFADO o PATRIMÔNIO • MICROSOFT EDGE • MICROSOFT OFFICE • MICROSOFT WINDOWS • SISTEMA PARA CLÍNICA VETERINÁRIA – NUVEM VET – SISTEMA TERCEIRIZADO; • GOOGLE DRIVE; • GOOGLE EARTH PRO; • AUTO CAD; • ADOBE PDF; • APLICATIVO DO BANCO ITAÚ
SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO	• SISTEMA DE GESTÃO PÚBLICA – MODERNIZAÇÃO o PROTOCOLO o FOLHA DE PAGAMENTO o GESTÃO DE PESSOAS o TRAMITAÇÃO DE PROCESSOS o ARQUIVAMENTO DE PROCESSOS
IDAC	• SISTEMA DE GESTÃO PÚBLICA – MODERNIZAÇÃO o PROTOCOLO o CONTABILIDADE o GESTÃO DE PESSOAS o TRAMITAÇÃO DE PROCESSOS o GESTÃO DO PORTAL DA TRANSPARÊNCIA

	o MIGRAÇÃO DE DADOS DE SISTEMAS LEGADOS o PLANEJAMENTO • ARQUIVAMENTO DE PROCESSOS

3.6.5.3.3 - Redes, comunicação / infraestrutura física e lógica

Diagnóstico Detalhado – Problemas Identificados:

Apuração realizada junto à infraestrutura atual demonstrou vulnerabilidades, carências e não conformidades em diversas frentes técnicas e organizacionais. Cada item a seguir elenca os principais gargalos para funcionamento pleno dos serviços digitais municipais.

Equipamentos de Informática

- Ausência total de licenciamento de softwares, gerando riscos jurídicos e operacionais;

Impressoras

- Uso de impressoras de utilização residencial sendo utilizado em alguns setores com grande demanda de trabalho, impactando o fluxo de trabalho.
- Falta de padronização e multiplicidade de marcas/modelos tornando insumos e suporte ineficientes;
- Falta de sistema para controle de custos e rastreio de uso.

Switches e Roteadores

- Predominância de switches Layer 1 sem recursos gerenciáveis, dificultando administração da rede;
- Uso de roteadores residenciais nos links críticos afetando largura de banda e estabilidade;
- Falta de redundância de links e hardware;
- Riscos de segurança pela impossibilidade de controle granular de acessos, monitoramento e atualizações. Ausência de Firewall de alta escalabilidade e gerência.

Servidores

- Hardware crítico e obsoleto, fora de garantia e com altas possibilidades de falhas.
- Limitação severa do espaço em disco e impossibilidade de expansão planejada;
- Falta de peças de reposição para eventos críticos;
- Uso de software de virtualização sem licenciamento;
- Falta de políticas claras de backup (cronograma, testes, retenção, restauração);
- Elevado risco de perda definitiva de dados por falha e falta de redundância adequada;

Nobreaks

- Proteção elétrica insuficiente: menos de 10% do parque coberto;
- Nobreaks antigos, sem revisões preventivas e com baterias degradadas;
- Risco de shutdown abrupto e perda de equipamentos/sistemas por instabilidade da rede elétrica;
- Ausência de monitoramento centralizado e de política de manutenção preventiva;
- Falta de redundância nas proteções de energia;

Data Center

- Instalações não atendem normas técnicas de infraestrutura NBR ISO/IEC 22237, TIER III;
- Falta de controle ambiental, climatização e sensores adequados;
- Ausência de mecanismos de segurança física eficazes, monitoramento de acesso e CFTV;
- Inexistência de sistema de detecção e combate a incêndios específico;
- Infraestrutura improvisada sem piso elevado, redundância ou isolamento adequado aos equipamentos críticos;

Segurança da Informação

- Falta de profissionais especializados para implementar e manter políticas de segurança;
- Ausência de firewall e regras de proteção para o ambiente governamental;
- Ausência de políticas de segurança documentadas e disseminadas;
- Não implementação de controles de acesso por criticidade, nem de mecanismos de resposta e mitigação a incidentes;

Topologia de Rede

- Falhas recorrentes nas conexões entre secretarias devido a instabilidades do serviço prestado pelo ISP/falta de nobreaks funcionais para mitigar quedas de energia, topologia de anel contratada instável;
- Inexistência de links de internet de backup, causando interrupções periódicas;
- Cabeamento antigo, mal dimensionado, exposto e misturado à rede elétrica, não seguindo as devidas normas técnicas, causando instabilidade e limitação da largura de banda. Gerando instabilidade lentidão e as vezes perda de comunicação;
- Poluição visual, risco de acidentes e dificuldade de manutenção;

Time Técnico

Número insuficiente de profissionais especializados para atendimento de demandas rotineiras e de projetos estruturantes;
Falta de um programa sistemático de capacitação, desenvolvimento e retenção de talentos;

- Ausência de plano de carreira, incentivos à certificação e política de treinamento continuado;
- Dependência excessiva de fornecedores externos e risco de perda de conhecimento institucional

3.6.5.3.4 - Cenário Ideal – Soluções Técnicas Propostas

A seguir, delineiam-se soluções modernas e aderentes às normas técnicas, visando responder de forma efetiva a cada fragilidade apontada no diagnóstico.

Equipamentos de Informática

- Renovação completa do parque de computadores, com estações de trabalho padronizadas e especificação adequada por função;
- Aquisição apenas de equipamentos novos com garantia mínima, ciclo de vida planejado e sistemas de gestão de ativos;
- Licenciamento formal e inventariado de todos os softwares essenciais;
- Implantação de softwares de proteção (antivírus centralizado, firewall de endpoint) e sistemas de atualização automática;
- Controle de inventário e auditoria digital do parque computacional.

Impressoras

- Implantação de parque de impressoras corporativas com recursos multifuncionais (impressão, digitalização, cópia);
- Padronização de marca/modelo e contratação de fornecedores por acordo de nível de serviço SLA.
- Sistema de cotas e monitoramento centralizado de impressões, contabilizando uso por setor/usuário;
- Contrato de manutenção com visitas preventivas;
- Sistema de insumos centralizado para otimização de compras.

Switches e Roteadores

- Substituição de switches e roteadores domésticos por modelos corporativos, Layer 2/3 plenamente gerenciáveis;
- Topologia planejada com suporte a VLANs, QoS, LACP, port security e monitoração SNMP;
- Roteadores/finalizadores de link com alta capacidade, firewall integrado, suporte a VPNs e failover automático;
- Estrutura de monitoramento em tempo real, geração de alertas e logs para análise forense;
- Implementação de redundância de backbone e segmentação lógica da rede;

Servidores

- Instalação de servidores modernos em rack padrão, com fontes redundantes e storage escalável RAID 10/RAID 6;
- Aquisição de insumos/hardware backup em caso de falhas;

- Virtualização com soluções licenciadas e/ou de código aberto como Hyper-V, RHV ou Proxmox, priorizando alta disponibilidade, migração dinâmica e backup de VMs;
- Implementação de rotinas rigorosas de backup com múltiplas cópias locais, remotas e off- site (regra 3- 2- 1);
- Monitoramento ativo da saúde dos servidores (discos, memórias, energia, temperaturas);
- Contratação/Treinamento de equipe técnica especializada para administração, upgrade e recuperação de desastres;

Nobreaks

- Planejamento e instalação de nobreaks em topologia online de dupla conversão para servidores e switches críticos;
- Dimensionamento de autonomia mínima para desligamento seguro após falha da concessionária;
- Monitoramento remoto do status dos equipamentos e baterias, com alertas;
- Plano preventivo para manutenção, trocas programadas de baterias e testes periódicos de funcionamento;
- Redundância de proteção em nodes/links críticos.

Data Center

- Projeto estrutural atualizado conforme NBR ISO/IEC 22237, buscando ao menos aderência a requisitos TIER III;
- Instalação de piso elevado, climatização redundante N1, sensores ambientais, isolamento e proteção contra fogo;
- Sala-cofre conforme ABNT NBR 15247 para banco de dados essenciais;
- Controle de acesso físico por biometria/cartão, registros detalhados de entrada e CFTV permanente;
- Sistemas de detecção precoce e combate a incêndio sem água, apropriados a eletrônicos sensíveis

Segurança da Informação

- Mapeamento e inventário detalhado dos dados pessoais tratados e fluxo de dados em TI.
- Firewalls NGFW, sistema IDS/IPS, anti-malware e SIEM para defesa em múltiplas camadas;
- Políticas de segurança documentadas, treinamentos anuais obrigatórios e plano de resposta a incidentes;
- Treinamentos anuais obrigatórios e plano de resposta a incidentes;
- Adoção de criptografia, autenticação forte MFA, controles por perfil e trilha de auditoria detalhada;

Topologia de Rede

- Redesenho da topologia para garantir redundância (anéis duplos/ligações paralelas em pontos críticos);
- Contratação de links de backup de internet e configuração de failover automático;
- Substituição de todo o cabeamento por categoria 6A blindada, passagem em dutos próprios longe da rede elétrica;
- Identificação, documentação e organização completa para evitar riscos operacionais e facilitar manutenções.

Recursos Humanos

- Dimensionamento do quadro mínimo recomendado de TI para porte da prefeitura (analistas e técnicos devidamente qualificados).
- Elaboração e execução anual de plano de capacitação, trilhas de certificação CompTIA, Cisco, Microsoft, LGPD, ITIL, etc.);
- Estímulo à formação continuada, política de retenção de talentos e contratação de especialistas se necessário;
- Programa de acompanhamento individual do desenvolvimento técnico e comunicação interna efetiva.
- Redução progressiva da dependência de terceiros em áreas núcleo, preservando o conhecimento institucional.

Avaliação dos sistemas e aplicações

Inexiste qualquer análise da maturidade, integração, desempenho e segurança dos sistemas corporativos, verificando os processos suportados e a interoperabilidade entre eles.

4. ANÁLISE DE MATRIZ SWOT

FORÇAS	
Engajamento da liderança com temas de transformação digital e segurança	Presença de infraestrutura básica de TI que pode ser modernizada
Existência de parcerias institucionais ou convênios com universidades e órgãos públicos	Capacitação, Treinamento Contínuo e Inclusão Digital
Promoção da Inovação tecnológica	Aprimoramento da Segurança da Informação
Tomada de Decisões mais eficientes	Aprimoramento na Gestão de Recursos
Integração entre Áreas	Maior Conformidade Regulatória

FORÇAS	
Melhoria na Governança de TIC	Padronização de Processos
Melhoria na Governança e Planejamento Estratégico	Eficiência Operacional e Gestão de Recursos
Desburocratização e Eficiência Administrativa	Fortalecimento da Governança e Melhoria no Atendimento ao Cidadão
Fortalecimento da Cultura de Inovação no Setor Público	Eficiência e Agilidade com Processos Administrativos Eletrônicos
Melhoria na Qualidade do Atendimento ao Cidadão	Redução de Custos Operacionais
Fortalecimento da Imagem Institucional	Garantia de proteção a dados críticos
Capacidade de resposta rápida e eficiente a incidentes de segurança	Processos estruturados e bem definidos para lidar com incidentes de segurança
Maior alinhamento estratégico entre TI e os objetivos do município	Resposta rápida a incidentes e otimização da performance dos sistemas
Melhoria da performance geral dos sistemas e maior segurança	Aumento da eficiência operacional e segurança dos sistemas
Redução de riscos legais e de segurança com suporte e atualizações regulares	Acompanhamento constante da qualidade do atendimento e eficiência dos serviços

FORÇAS	
Correção rápida de falhas ou melhorias necessárias	Engajamento contínuo da população para melhoria dos serviços
Melhoria da Eficiência Operacional com Automação de Processos	Adoção de Ferramentas de Análise de Dados para Otimizar Serviços

FRAQUEZAS	
Ausência de Profissionais Especialistas em Segurança de TI (Segurança da Informação e Segurança Cibernética	Ausência de profissionais especialistas em Administração de Dados (DBA/AD)
Baixa Maturidade Digital Institucional e Governança Administrativa de TIC	Auditorias e penalidades legais por não conformidade
Vazamentos de dados sensíveis (servidores)	Perda de confiança dos usuários de serviços públicos
Atraso em processos de transformação digital	Não disponibilização de internet em locais públicos
Ausência de ferramentas de monitoramento de rede 24x7;	Ausência de política de manutenção preventiva e avaliação tecnológica e de serviços digitais
Ausência parcial de login em domínio de rede	Limitação de criação de emails com domínios e subdomínios

FRAQUEZAS	
Dependência de infraestrutura de TI antiga ou limitada	Capacitação não uniforme entre equipes
Falta de integração plena entre todos os setores ou sistemas	Risco de excesso de burocracia em processos que ainda não foram digitalizados
Possível resistência cultural à inovação em setores mais tradicionais	Capacidade reativa, mas ainda não plenamente preventiva na segurança da informação
Desalinhamento estratégico em unidades específicas	Dependência de poucos profissionais-chave ou alta rotatividade
Falta de métricas claras e padronizadas para medir desempenho e eficiência	Necessidade contínua de manutenção e atualização de sistemas legados
Capacidade limitada para escalar soluções digitais com rapidez	Baixo engajamento de parte da população nos canais digitais
Falta de uma estratégia unificada de transformação digital em todos os níveis	Baixa capacidade interna para acessar ou aproveitar editais e linhas de financiamento
Desconhecimento ou baixa adoção de frameworks como ISO 27001/NIST	Dependência excessiva de parcerias externas para consultoria e tecnologia
Infraestrutura digital insuficiente para suportar a automação de processos	Equipe pouco capacitada para utilizar tecnologias emergentes e análise de dados

FRAQUEZAS	
Governança fraca ou fragmentada para coordenação entre diferentes órgãos	Cultura institucional pouco voltada à inovação ou transformação digital
Comunicação limitada com o cidadão sobre os serviços digitais existentes	Senha sob domínio de uma só pessoa (Exemplo: Cloudflare)
Não possui ciclo de vida de software	Carência de políticas públicas municipais estruturadas baseadas em dados
Ausência de profissional com sólidas habilidades em mapeamento de processos	Ausência de ferramentas que facilitem a adoção de padrões de desenvolvimento de códigos de programação
Quantidade limitada de nobreak para previnir contra risco de queima de equipamentos.	Hardware defasado e obsoleto, fora da garantia e com alta probabilidade de falhas, comprometendo a produtividade e infraestrutura insuficiente para suportar a automação de processos
Ausência total de licenciamento de softwares, gerando riscos jurídicos e operacionais;	Incompatibilidade tecnológica com sistemas e padrões modernos;
Gastos excessivos com manutenção emergencial e aluguel de equipamentos inadequados;	Vulnerabilidades de segurança digital;
Uso de impressoras residenciais em setores com grande demanda;	Falta de padronização e multiplicidade de marcas/modelos tornando insumos e suporte ineficientes;

FRAQUEZAS	
Ausência de contratos ou programas de manutenção preventiva e corretiva;	Equipamentos incapazes de atender demandas setoriais, impactando fluxo de trabalho;
Falta de sistema para controle de custos e rastreio de uso;	Utilização de switches layer 1 sem recursos gerenciáveis;
Ausência de VLANS, Qos, port security e monitoramento SNMP;	Uso de roteadores residenciais nos links críticos afetando largura da banda e estabilidade;
Falta de redundância, monitoramento em tempo real e registro de eventos;	Risco de segurança pela impossibilidade de controle granular de acessos e atualizações;
Limitação severa do espaço em disco e impossibilidade de expansão planejada;	Uso de software de virtualização sem licenciamento formalizado;
Equipe em estágio de aprendizado para administração, monitoramento e backup;	Falta de políticas claras de backup (cronograma, testes, retenção, restauração);
Elevado risco de perda definitiva de dados por falha e falta de redundância adequada;	Proteção elétrica insuficiente: menos de 10% do parque coberto;
Nobreaks antigos, sem revisões preventivas e com baterias degradadas com risco de shutdown abrupto e perda de equipamentos/sistemas por instabilidade da rede elétrica;	Falta de redundância nas proteções de energia;

FRAQUEZAS	
Instalações não atendem normas técnicas de infraestrutura NBR ISO/IEC 22237, TIER III;	Falta de controle ambiental, climatização e sensores adequado;
Ausência de mecanismos de segurança física eficaz, monitoramento de acesso e CFTV;	Inexistência de sistema de detecção e combate a incêndios específico;
Infraestrutura improvisada sem piso elevado, redundância ou isolamento adequado aos equipamentos críticos;	Hardware de proteção (firewalls, IDS/IPS) inadequado para o ambiente governamental;
Ausência de políticas de segurança documentadas e disseminadas;	Falta de conformidade com a LGPD;
Ausência de inventário de dados pessoais;	Não implementação de controles de acesso por criticidade, nem de mecanismos de resposta e mitigação a incidentes;
Falhas recorrentes nas conexões entre secretarias por topologia de anel instável;	Inexistência de links de internet de backup, tornando o sistema vulnerável à indisponibilidade total;
Cabeamento antigo, mal dimensionado, sem certificação, exposto e misturado à rede elétrica;	Poluição visual, risco de acidentes e dificuldade de manutenção;
Limitação de largura de banda e instabilidade das conexões internas;	Número insuficiente de profissionais especializados para atendimento de demandas rotineiras e de projetos estruturantes;

FRAQUEZAS	
Falta de um programa sistemático de capacitação, desenvolvimento e retenção de talentos;	Ausência de plano de carreira, incentivos à certificação e política de treinamento continuado;
Dependência excessiva de fornecedores externos e risco de perda de conhecimento institucional	Ausência de governança sobre a Segurança da Informação
Ausência de papéis, responsabilidades e autoridades estabelecidas em Segurança da Informação	Ausência de gerência sobre os riscos de segurança da informação
Inexistência de uma Política de Segurança da Informação	Ausência de avaliação de desempenho e análise crítica sobre a segurança da informação
Inexistência de inventário detalhado de ativos corporativos	Ausência de tratamento dos ativos não autorizados encontrados na infraestrutura institucional
Inexistência de inventário detalhado de softwares	Ausência de seguridade para que todo software autorizado seja suportado pelo fabricante
Ausência de tratamento dos softwares não autorizados	Ausência de processos voltados a gestão de dados
Inexistência de inventário de dados	Ausência de lista de controle de acesso de dados institucional
Retenção apenas parcial dos dados adequadamente	Ausência de política institucional referente a descarte de dados com segurança

FRAQUEZAS	
Ausência de criptografia dos dados nos dispositivos dos usuários	Ausência de procedimento de hardening expondo fragilidades no processo de configuração segura
Ausência de bloqueio automático de sessão nos ativos corporativos	Ausência de implementação e gerencia de firewalls nos servidores e dispositivos de usuários finais.
Ausência de gerência de ativos e softwares de maneira segura	Ausência de tratamento das contas padrão dos ativos e softwares
Inexistência de inventário detalhado de contas	Não utilização de senhas exclusivas
Ausência de política institucional voltada a desabilitação de contas inativas após um tempo pré-definido	Ausência de política institucional voltada a restringir os privilégios de administrador às contas dedicadas para o perfil de administrador
Ausência de processo institucional para a concessão de acesso	Ausência de processo institucional para a revogação de acesso
Ausência de autenticação multifator para autorização dos usuários a seus ativos	

OPORTUNIDADES	
Programas de capacitação/treinamento gratuitos ou subsidiados (ex: cursos online, iniciativas governamentais)	Adoção de frameworks reconhecidos como ISO 27001 ou NIST para acelerar maturidade digital

OPORTUNIDADES	
Editais de fomento à transformação digital e segurança da informação	Parcerias com empresas de tecnologia para terceirização ou consultoria especializada
Digitalização e automação de processos	Acesso a linhas de financiamento e programas de apoio à transformação digital
Ampliação da oferta de serviços digitais através do site institucional	Adaptação dos marcos legislativos de outros órgãos
Atuação orientadora da ANPD (manuais, normativas etc.)	Fomento à Colaboração e Parcerias
Transformação Digital e Acesso ao Governo	Aumento da Transparência e Acessibilidade
Promoção de Cultura Digital e Capacitação Contínua	Criação e Implementação de Políticas Públicas de Governo Digital
Inovação na Gestão Pública e Melhoria na Qualidade dos Serviços	Integração de Ações e Colaboração Entre Diferentes Órgãos Governamentais
Aumento da Transparência e Engajamento Cidadão	Aumento da Transparência e Confiança do Cidadão
Adequação à LGPD e Proteção de Dados Pessoais	Adoção de Tecnologias Emergentes para Tomada de Decisões
Desenvolvimento de Políticas Públicas Baseadas em Dados	Agilidade, redução de custos e segurança jurídica nos processos eletrônicos

OPORTUNIDADES	
Redução da desigualdade digital	Inclusão social e maior participação cidadã
Acesso universal à informação e serviços públicos	Apoio ao desenvolvimento econômico local
Fortalecimento da educação digital	Expansão da Oferta de Serviços Digitais
Monitoramento em Tempo Real dos Índices de Satisfação dos Serviços Digitais	Criação de Canais de Participação Cidadã Digital
Expansão de Serviços de Identificação e Certificação Digital	Integração de Serviços Digitais com Diferentes Áreas da Administração Pública

AMEAÇAS	
Crescimento exponencial de ataques cibernéticos, como ransomware e phishing	Sanções legais e reputacionais por não conformidade com a LGPD e outras normas
Dificuldade de retenção de talentos, especialmente em áreas técnicas	Baixa notificação de incidentes, o que pode gerar riscos jurídicos e perda de confiança
Pressão regulatória crescente sem estrutura interna para resposta adequada	A baixa maturidade digital pode gerar multas e sanções

AMEAÇAS	
Incidentes de segurança ou falhas digitais impactam a imagem institucional	Perda e/ou vazamento de dados sensíveis
Sequestro do site institucional ou de sistemas institucionais	Perda de recursos por não aproveitamento de editais e financiamentos disponíveis
Atraso na adequação à LGPD e riscos legais associados	Desigualdade digital ampliada
Crescimento da desconfiança pública na gestão digital	Concorrência entre órgãos por atenção e recursos em vez de colaboração
Obsolescência tecnológica acelerada	Risco de vazamentos e ciberataques devido à falta de governança de dados e segurança
Baixo engajamento da população nas soluções digitais criadas	Dependência excessiva de fornecedores externos de tecnologia e risco de perda de conhecimento institucional
Pressão social e política por resultados rápidos	Desvalorização de profissionais capacitados pelo mercado privado
Corte de investimentos públicos em capacitação contínua	Dificuldade de retenção de conhecimento institucional
Rápido avanço tecnológico e obsolescência acelerada, exigindo investimentos constantes para manter a força em inovação	Crescimento do cibercrime e aumento da sofisticação de ataques cibernéticos, exigindo respostas cada vez mais complexas e especializadas

AMEAÇAS	
Falta de regulamentações claras ou mudança abrupta nas leis de segurança digital, criando insegurança jurídica	Mudanças frequentes em políticas públicas e instabilidade institucional, dificultando a consolidação de boas práticas de governança.
Resistência de lideranças políticas ou administrativas à continuidade de processos de transformação digital, especialmente em trocas de governo.	Aumento das exigências legais e regulatórias, sem correspondente suporte técnico ou orçamentário.
Desigualdade digital ou exclusão de populações vulneráveis, dificultando o acesso universal aos serviços públicos digitais.	Baixo engajamento da população nas ferramentas digitais disponíveis, por falta de confiança ou conhecimento.
Perda de credibilidade institucional em caso de falhas graves em serviços digitais ou vazamento de dados.	Dependência excessiva de fornecedores de software e automação, com riscos de descontinuidade contratual.
Mudanças tecnológicas que exigem novos investimentos imprevistos, pressionando o orçamento público.	Dificuldade de integração entre sistemas legados e novas plataformas, gerando ineficiência e retrabalho
Risco de decisões equivocadas por análise de dados incompletos ou enviesados, impactando negativamente políticas públicas.	Críticas públicas e legais sobre uso indevido de dados pessoais, mesmo com boa estrutura de segurança.

4.1. PLANO DE GERENCIAMENTO DE RISCOS

Nomenclatura:
R-**F**XX – Riscos identificados a partir das FRAQUEZAS constantes no modelo SWOT.
R-**A**XX - Riscos identificados a partir das AMEAÇAS constantes no modelo SWOT.

Código: R-F01
Nome do Risco: Ausência de Profissionais Especialistas em Segurança da Informação
Descrição: Falta de pessoal qualificado em segurança da informação, elevando a vulnerabilidade a ataques cibernéticos.
Impacto Potencial: Muito Alto — perdas financeiras e multas.
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Contratar e/ou capacitar especialistas, implantar políticas de segurança e monitorar continuamente os sistemas.

Código: R-F02
Nome do Risco: Ausência de Profissionais Especialistas em Segurança Cibernética
Descrição: Falta de capacidade para detectar e responder rapidamente a ataques e invasões.
Impacto Potencial: Alto — prejuízos financeiros e reputacionais.
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Criar equipe de resposta (CSIRT), estabelecer parcerias e promover treinamento contínuo.

Código: R-F03
Nome do Risco: Ausência de Profissionais Especialistas em Administração de Dados (DBA/AD)
Descrição: Problemas com integridade, disponibilidade e desempenho dos bancos de dados.
Impacto Potencial: Alto — perda ou corrupção de dados.
Probabilidade: Média
Nível de Risco: Médio
Plano de Resposta: Contratar/capacitar ADs e/ou DBAs e implantar monitoramento contínuo.

Código: R-F04
Nome do Risco: Baixíssima Maturidade Digital Institucional

Descrição: Retardo nas iniciativas de digitalização e inovação devido à baixa maturidade.
Impacto Potencial: Alto — perda de eficiência.
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Desenvolver plano estratégico, capacitação e fortalecer governança.

Código: R-F05
Nome do Risco: Auditorias e Penalidades Legais por Não Conformidade
Descrição: Multas e sanções devido a não conformidade com legislações como LGPD.
Impacto Potencial: Muito Alto — multas e prejuízo à imagem institucional.
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Implantar políticas de conformidade, realizar auditorias, designar DPO e promover treinamentos.

Código: R-F06
Nome do Risco: Vazamentos de Dados Sensíveis (Servidores)
Descrição: Vazamento de informações pessoais e críticas.
Impacto Potencial: Muito Alto — perda de confiança dos usuários e stakeholders.
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Controlar acessos, aplicar criptografia, monitorar sistemas 24x7 e realizar comunicação eficaz.

Código: R-F07
Nome do Risco: Perda de Confiança dos Usuários de Serviços Públicos
Descrição: Usuários perdem confiança nos serviços digitais institucionais.
Impacto Potencial: Muito Alto — redução no uso dos serviços.
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Assegurar transparência, comunicação eficaz, segurança reforçada e atendimento de qualidade.

Código: R-F08
Nome do Risco: Atraso em Processos de Transformação Digital
Descrição: Processos antigos e ineficientes atrasam a evolução organizacional.
Impacto Potencial: Alto — ineficiência e aumento de custos.

Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Definir prioridades, automatizar processos e promover capacitação da equipe.

Código: R-F09
Nome do Risco: Não Disponibilização de Internet em Locais Públicos
Descrição: População sem acesso à internet enfrenta barreiras para utilizar serviços digitais.
Impacto Potencial: Alto — exclusão social.
Probabilidade: Média
Nível de Risco: Médio
Plano de Resposta: Implantar pontos públicos de acesso à internet e estabelecer parcerias para conectividade.

Código: R-F10
Nome do Risco: Ausência de Ferramenta de Monitoramento de Rede 24x7
Descrição: Incapacidade de identificar ataques ou falhas rapidamente.
Impacto Potencial: Alto — aumento do impacto de incidentes.
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Implementar monitoramento contínuo e formar equipe SOC/NOC.

Código: R-F11
Nome do Risco: Ausência Parcial de Login em Domínio de Rede
Descrição: Dificuldade para controlar acessos e rastrear atividades na rede.
Impacto Potencial: Médio — risco de acessos indevidos.
Probabilidade: Média
Nível de Risco: Médio
Plano de Resposta: Implementar login centralizado e autenticação robusta.

Código: R-F12
Nome do Risco: Limitação na Criação de Emails com Domínios e Subdomínios
Descrição: Controle limitado sobre a comunicação institucional via email.
Impacto Potencial: Médio — falhas na comunicação.
Probabilidade: Média
Nível de Risco: Médio
Plano de Resposta: Expandir infraestrutura de email e estabelecer políticas claras.

Código: R-F13
Nome do Risco: Dependência de Infraestrutura de TI Antiga ou Limitada
Descrição: Infraestrutura obsoleta causa falhas e lentidão nos sistemas.
Impacto Potencial: Alto — aumento de falhas e insatisfação dos usuários.
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Planejar e executar modernização gradual da infraestrutura.

Código: R-F14
Nome do Risco: Capacitação Não Uniforme Entre Equipes
Descrição: Equipes com diferentes níveis de competência geram baixa eficiência operacional.
Impacto Potencial: Médio — erros operacionais.
Probabilidade: Média
Nível de Risco: Médio
Plano de Resposta: Estabelecer treinamentos padronizados e contínuos.

Código: R-F15
Nome do Risco: Governança de TIC em Amadurecimento em Algumas Unidades
Descrição: Decisões descentralizadas ou falhas nas políticas de TIC.
Impacto Potencial: Alto — riscos operacionais.
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Fortalecer governança e integrar unidades.

Código: R-F16
Nome do Risco: Falta de Integração Plena Entre Setores ou Sistemas
Descrição: Sistemas isolados causam retrabalho e ineficiência.
Impacto Potencial: Alto — perda de produtividade.
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Promover projetos de integração e interoperabilidade.

Código: R-F17
Nome do Risco: Excesso de Burocracia em Processos Não Digitalizados
Descrição: Processos manuais geram atrasos e erros.
Impacto Potencial: Médio — insatisfação e aumento de custos.
Probabilidade: Média
Nível de Risco: Médio
Plano de Resposta: Automatizar e revisar processos para eliminar burocracia desnecessária.

Código: R-F18
Nome do Risco: Resistência Cultural à Inovação em Setores Tradicionais
Descrição: Barreiras internas dificultam a adoção de novas tecnologias.
Impacto Potencial: Alto — atraso na digitalização.
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Implementar programas de gestão de mudança e engajamento cultural.

Código: R-F19
Nome do Risco: Baixa Maturidade Analítica em Algumas Áreas
Descrição: Uso insuficiente de dados para tomada de decisão adequada.
Impacto Potencial: Médio — decisões inadequadas.
Probabilidade: Média
Nível de Risco: Médio
Plano de Resposta: Implantar ferramentas analíticas e promover treinamento orientado a dados.

Código: R-F20
Nome do Risco: Capacidade Reativa, mas Não Preventiva em Segurança da Informação
Descrição: Resposta lenta aumenta o impacto dos incidentes de segurança.
Impacto Potencial: Alto — incidentes mais graves.
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Implantar controles preventivos e monitoramento contínuo.

Código: R-F21
Nome do Risco: Desalinhamento Estratégico em Unidades Específicas
Descrição: Falta de alinhamento prejudica o alcance dos objetivos institucionais.
Impacto Potencial: Alto — perda de sinergia.
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Formalizar alinhamento estratégico e realizar reuniões periódicas.

Código: R-F22
Nome do Risco: Dependência de Profissionais-chave ou Alta Rotatividade
Descrição: Ausência temporária pode afetar continuidade e conhecimento.
Impacto Potencial: Alto — paralisação e perda de conhecimento institucional.

Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Desenvolver plano de sucessão, capacitação cruzada e estratégias de retenção.

Código: R-F23
Nome do Risco: Falta de Métricas Claras e Padronizadas para Desempenho
Descrição: Gestão baseada em dados insuficientes ou ausentes.
Impacto Potencial: Médio — baixa eficiência.
Probabilidade: Média
Nível de Risco: Médio
Plano de Resposta: Implantar KPIs e dashboards gerenciais.

Código: R-F24
Nome do Risco: Necessidade Contínua de Manutenção e Atualização de Sistemas Legados
Descrição: Sistemas antigos apresentam falhas e incompatibilidades crescentes.
Impacto Potencial: Alto — indisponibilidade dos serviços.
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Planejar migração progressiva, atualização e suporte contínuo.

Código: R-F25
Nome do Risco: Capacidade Limitada para Escalar Soluções Digitais Rapidamente
Descrição: Lentidão na expansão de soluções digitais frente à demanda crescente.
Impacto Potencial: Médio — atrasos e insatisfação dos usuários.
Probabilidade: Média
Nível de Risco: Médio
Plano de Resposta: Adotar plataformas flexíveis (como nuvem) e investir em escalabilidade.

Código: R-F26
Nome do Risco: Baixo Engajamento da População nos Canais Digitais
Descrição: Parte do público não utiliza plataformas digitais por desconexão ou desconhecimento.
Impacto Potencial: Médio — desperdício de recursos públicos.
Probabilidade: Média
Nível de Risco: Médio
Plano de Resposta: Realizar campanhas educativas e melhorar acessibilidade e usabilidade.

Código: R-F27
Nome do Risco: Falta de Estratégia Unificada de Transformação Digital
Descrição: Projetos fragmentados sem convergência para objetivo único.
Impacto Potencial: Alto — dispersão de esforços.
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Desenvolver e implementar plano estratégico unificado.

Código: R-F28
Nome do Risco: Baixa Capacidade Interna para Aproveitar Editais e Linhas de Financiamento
Descrição: Incapacidade técnica para buscar e utilizar oportunidades de financiamento.
Impacto Potencial: Médio — restrição de recursos.
Probabilidade: Média
Nível de Risco: Médio
Plano de Resposta: Capacitar equipe para elaboração de projetos e firmar parcerias estratégicas.

Código: R-F29
Nome do Risco: Desconhecimento ou Baixa Adoção de Frameworks como ISO 27001/NIST
Descrição: Ausência de adoção de padrões reconhecidos internacionalmente em segurança.
Impacto Potencial: Alto — maior vulnerabilidade a incidentes.
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Implantar progressivamente frameworks, realizar treinamentos e certificações.

Código: R-F30
Nome do Risco: Dependência Excessiva de Parcerias Externas para Consultoria e Tecnologia
Descrição: Baixa autonomia e custos elevados devido à dependência de fornecedores.
Impacto Potencial: Médio — impactos operacionais.
Probabilidade: Média
Nível de Risco: Médio
Plano de Resposta: Desenvolver competências internas e estabelecer cláusulas contratuais rígidas.

Código: R-F31
Nome do Risco: Infraestrutura Digital Insuficiente para Suportar Automação de Processos
Descrição: Limitação tecnológica impede automação e otimização dos processos.
Impacto Potencial: Alto — manutenção de processos manuais.
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Investir em infraestrutura tecnológica moderna e escalável.

Código: R-F32
Nome do Risco: Equipe Pouco Capacitada para Tecnologias Emergentes e Análise de Dados
Descrição: Subutilização do potencial tecnológico pela baixa capacitação.
Impacto Potencial: Médio — baixa inovação.
Probabilidade: Média
Nível de Risco: Médio
Plano de Resposta: Programas contínuos de capacitação e incentivo à especialização.

Código: R-F33
Nome do Risco: Governança Fraca ou Fragmentada para Coordenação Entre Órgãos
Descrição: Falta de coordenação e estratégias unificadas entre setores.
Impacto Potencial: Alto — baixa eficiência.
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Fortalecer governança com comitês unificados e processos padronizados.

Código: R-F34
Nome do Risco: Ausência de Estratégia Clara para Monitoramento e Avaliação de Serviços Digitais
Descrição: Serviços digitais sem monitoramento contínuo de desempenho.
Impacto Potencial: Médio — problemas não detectados.
Probabilidade: Média
Nível de Risco: Médio
Plano de Resposta: Implantar KPIs, dashboards e auditorias constantes.

Código: R-F35
Nome do Risco: Cultura Institucional Pouco Voltada à Inovação ou Transformação Digital

Descrição: Falta de incentivo e cultura para inovação digital.
Impacto Potencial: Alto — estagnação organizacional.
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Programas de incentivo, comunicação interna e liderança engajada.

Código: R-F36
Nome do Risco: Comunicação Limitada Com o Cidadão Sobre Serviços Digitais
Descrição: População pouco informada reduz demanda por serviços digitais.
Impacto Potencial: Médio — baixa eficiência dos canais digitais.
Probabilidade: Média
Nível de Risco: Médio
Plano de Resposta: Estratégia multicanal de comunicação, campanhas educativas e escuta ativa.

Código: R-F37
Nome do Risco: Carência de Políticas Públicas Municipais Estruturadas Baseadas em Dados
Descrição: Falta de fundamentação em dados para gestão pública e definição de estratégias.
Impacto Potencial: Alto — desperdício de recursos públicos.
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Desenvolver governança de dados, promover uso analítico e capacitação.

Código: R-A01
Nome do Risco: Crescimento Exponencial de Ataques Cibernéticos (Ransomware e Phishing)
Descrição: Crescimento de ataques cibernéticos pode causar indisponibilidade total de sistemas críticos.
Impacto Potencial: Alto
Probabilidade: Alta
Nível de Risco: Crítico
Plano de Resposta: Implementar backups offline, manter antivírus atualizados e treinar colaboradores.

Código: R-A02
Nome do Risco: Sanções Legais e Reputacionais por Não Conformidade com LGPD e Outras Normas
Descrição: Multas e penalidades por descumprimento da LGPD e legislações correlatas.
Impacto Potencial: Alto
Probabilidade: Média
Nível de Risco: Alto
Plano de Resposta: Realizar diagnóstico de adequação e implementar controles e políticas.

Código: R-A03
Nome do Risco: Dificuldade de Retenção de Talentos em Áreas Técnicas
Descrição: Perda de continuidade e expertise causada por desmotivação ou saída de profissionais.
Impacto Potencial: Médio
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Desenvolver planos de carreira e incentivos para retenção.

Código: R-A04
Nome do Risco: Baixa Notificação de Incidentes, Gerando Riscos Jurídicos e Perda de Confiança
Descrição: Falta de reporte de incidentes cibernéticos pode comprometer confiança e gerar litígios.
Impacto Potencial: Alto
Probabilidade: Média
Nível de Risco: Alto
Plano de Resposta: Estabelecer política obrigatória de notificação e resposta a incidentes.

Código: R-A05
Nome do Risco: Pressão Regulatório Crescente Sem Estrutura Interna Adequada
Descrição: Falta de estrutura para cumprimento normativo gera riscos de penalizações.
Impacto Potencial: Alto
Probabilidade: Média
Nível de Risco: Alto
Plano de Resposta: Fortalecer áreas jurídicas e técnicas, mapear requisitos regulatórios.

Código: R-A06
Nome do Risco: Baixa Maturidade Digital Pode Gerar Multas e Sanções
Descrição: Insuficiente maturidade digital expõe a instituição a penalidades.
Impacto Potencial: Alto
Probabilidade: Média
Nível de Risco: Alto
Plano de Resposta: Planejar roadmap de transformação digital com foco em compliance.

Código: R-A07
Nome do Risco: Incidentes de Segurança ou Falhas Digitais Impactam Imagem Institucional
Descrição: Falhas digitais afetam credibilidade e confiança pública.
Impacto Potencial: Alto
Probabilidade: Alta
Nível de Risco: Crítico
Plano de Resposta: Criar plano de contingência, comunicação de crise e melhorar experiência do usuário.

Código: R-A08
Nome do Risco: Perda e/ou Vazamento de Dados Sensíveis
Descrição: Exposição de dados compromete segurança e pode gerar ações judiciais.
Impacto Potencial: Alto
Probabilidade: Alta
Nível de Risco: Crítico
Plano de Resposta: Criptografar dados, revisar permissões e monitorar acessos.

Código: R-A09
Nome do Risco: Sequestro do Site Institucional ou Sistemas Críticos
Descrição: Ataques que sequestram sites ou sistemas afetam continuidade dos serviços.
Impacto Potencial: Alto
Probabilidade: Média
Nível de Risco: Alto
Plano de Resposta: Manter cópias isoladas e plano de recuperação de desastres.

Código: R-A10
Nome do Risco: Perda de Recursos por Não Aproveitamento de Editais e Financiamentos
Descrição: Falta de preparo técnico gera perda de oportunidades de financiamento.

Impacto Potencial: Médio
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Capacitar equipe para elaboração de propostas e monitorar editais.

Código: R-A11
Nome do Risco: Atraso na Adequação à LGPD e Riscos Legais Associados
Descrição: Atrasos na adequação expõem a instituição a riscos legais.
Impacto Potencial: Alto
Probabilidade: Alta
Nível de Risco: Crítico
Plano de Resposta: Criar comitê LGPD e priorizar ações com cronogramas e metas claras.

Código: R-A12
Nome do Risco: Desigualdade Digital Ampliada
Descrição: Falta de inclusão digital marginaliza grupos vulneráveis.
Impacto Potencial: Alto
Probabilidade: Alta
Nível de Risco: Crítico
Plano de Resposta: Criar programas de inclusão e oferecer acesso gratuito à internet.

Código: R-A13
Nome do Risco: Crescimento da Desconfiança Pública na Gestão Digital
Descrição: Falta de transparência e incidentes reduzem o uso dos serviços públicos online.
Impacto Potencial: Alto
Probabilidade: Média
Nível de Risco: Alto
Plano de Resposta: Comunicar benefícios digitais e fortalecer segurança.

Código: R-A14
Nome do Risco: Concorrência Entre Órgãos por Recursos em Detrimento da Colaboração
Descrição: Disputa por recursos compromete eficiência institucional.
Impacto Potencial: Médio
Probabilidade: Média
Nível de Risco: Médio

Plano de Resposta: Criar comitê de governança interinstitucional para fortalecer a colaboração.

Código: R-A15
Nome do Risco: Obsolescência Tecnológica Acelerada
Descrição: Tecnologias antigas geram falhas, lentidão e custos elevados.
Impacto Potencial: Alto
Probabilidade: Alta
Nível de Risco: Crítico
Plano de Resposta: Mapear ativos e planejar substituições periódicas.

Código: R-A16
Nome do Risco: Risco de Vazamentos e Ciberataques por Falta de Governança
Descrição: Ausência de segurança e governança permite brechas de dados.
Impacto Potencial: Alto
Probabilidade: Alta
Nível de Risco: Crítico
Plano de Resposta: Implantar governança de dados e controles de segurança robustos.

Código: R-A17
Nome do Risco: Baixo Engajamento da População nas Soluções Digitais Criadas
Descrição: Ferramentas são subutilizadas por falta de engajamento dos cidadãos.
Impacto Potencial: Médio
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Investir em comunicação e capacitação cidadã.

Código: R-A18
Nome do Risco: Dependência Excessiva de Fornecedores de Tecnologia
Descrição: Risco de interrupção de serviços em caso de falência ou término de contrato.
Impacto Potencial: Alto
Probabilidade: Média
Nível de Risco: Alto
Plano de Resposta: Criar planos de transição e múltiplos fornecedores para continuidade.

Código: R-A19
Nome do Risco: Pressão Social e Política por Resultados Rápidos
Descrição: Implementações apressadas podem causar erros graves.
Impacto Potencial: Alto
Probabilidade: Alta
Nível de Risco: Crítico
Plano de Resposta: Estabelecer metas realistas e monitoramento rigoroso dos projetos.

Código: R-A20
Nome do Risco: Desvalorização de Profissionais Capacitados Pelo Mercado Privado
Descrição: Profissionais qualificados saem do serviço público por salários menores.
Impacto Potencial: Médio
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Criar incentivos e programas de reconhecimento a colaboradores.

Código: R-A21
Nome do Risco: Corte de Investimentos Públicos em Capacitação Contínua
Descrição: Limitação orçamentária reduz qualificação técnica da equipe.
Impacto Potencial: Alto
Probabilidade: Alta
Nível de Risco: Crítico
Plano de Resposta: Reservar verba mínima anual para capacitação contínua.

Código: R-A22
Nome do Risco: Dificuldade de Retenção de Conhecimento Institucional
Descrição: Rotatividade e falta de documentação provocam descontinuidade.
Impacto Potencial: Alto
Probabilidade: Alta
Nível de Risco: Crítico
Plano de Resposta: Implantar gestão do conhecimento com repositórios e manuais atualizados.

Código: R-A23
Nome do Risco: Falta de Regulamentações Claras ou Mudanças Abruptas nas Leis de Segurança Digital
Descrição: Atualizações constantes exigem adaptações rápidas de sistemas e equipes.

Impacto Potencial: Alto
Probabilidade: Alta
Nível de Risco: Crítico
Plano de Resposta: Manter plano de atualização tecnológica e vigilância legislativa contínua.

Código: R-A24
Nome do Risco: Instabilidade Institucional e Mudanças Frequentes em Políticas Públicas
Descrição: Leis novas ou contraditórias dificultam a operação consistente.
Impacto Potencial: Médio
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Monitorar marcos legais e envolver setor jurídico em projetos.

Código: R-A25
Nome do Risco: Resistência de Lideranças à Continuidade da Transformação Digital
Descrição: Trocas de governo prejudicam continuidade dos processos digitais.
Impacto Potencial: Alto
Probabilidade: Alta
Nível de Risco: Crítico
Plano de Resposta: Formalizar políticas de Estado e manter projetos em estruturas permanentes.

Código: R-A26
Nome do Risco: Aumento das Exigências Legais Sem Suporte Técnico ou Orçamentário
Descrição: Normas sem suporte técnico geram riscos de não conformidade.
Impacto Potencial: Alto
Probabilidade: Média
Nível de Risco: Alto
Plano de Resposta: Solicitar apoio técnico e manter capacitação constante.

Código: R-A27
Nome do Risco: Desigualdade Digital e Exclusão de Populações Vulneráveis
Descrição: Falta de acesso universal dificulta o uso de serviços públicos digitais.
Impacto Potencial: Alto
Probabilidade: Alta
Nível de Risco: Crítico
Plano de Resposta: Garantir pontos públicos de conectividade e melhorar usabilidade.

Código: R-A28
Nome do Risco: População Não Engajada
Descrição: Falta de confiança ou conhecimento inibe uso das plataformas digitais.
Impacto Potencial: Médio
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Realizar campanhas educativas e promover escuta ativa dos usuários.

Código: R-A29
Nome do Risco: Perda de Credibilidade
Descrição: Incidentes graves em serviços digitais afetam a confiança no governo.
Impacto Potencial: Alto
Probabilidade: Alta
Nível de Risco: Crítico
Plano de Resposta: Implantar padrões de qualidade e resposta rápida a falhas.

Código: R-A30
Nome do Risco: Dependência de Softwares de Terceiros
Descrição: Paralisação dos serviços por problemas com fornecedores externos.
Impacto Potencial: Alto
Probabilidade: Alta
Nível de Risco: Crítico
Plano de Resposta: Criar ambiente híbrido e exigir acesso ao código-fonte quando possível.

Código: R-A31
Nome do Risco: Novos Investimentos Não Planejados
Descrição: Mudanças tecnológicas exigem orçamento adicional urgente e imprevisto.
Impacto Potencial: Alto
Probabilidade: Alta
Nível de Risco: Crítico
Plano de Resposta: Prever fundo de inovação e orçamento flexível para adaptações rápidas.

Código: R-A32
Nome do Risco: Integração Ineficiente
Descrição: Falta de integração entre sistemas gera duplicidade e retrabalho.
Impacto Potencial: Médio

Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Mapear processos e implantar soluções de interoperabilidade.

Código: R-A33
Nome do Risco: Decisões com Dados Incompletos
Descrição: Má qualidade dos dados prejudica formulação de políticas públicas.
Impacto Potencial: Alto
Probabilidade: Alta
Nível de Risco: Crítico
Plano de Resposta: Implantar governança e assegurar qualidade dos dados.

Código: R-A34
Nome do Risco: Uso Indevido de Dados
Descrição: Riscos legais e reputacionais mesmo com boas intenções.
Impacto Potencial: Alto
Probabilidade: Média
Nível de Risco: Alto
Plano de Resposta: Criar comitê de ética em dados e revisar políticas de uso.

Código: R-A35
Nome do Risco: Falta de Regulamentação Digital
Descrição: Insegurança jurídica paralisa iniciativas e inibe inovação.
Impacto Potencial: Médio
Probabilidade: Alta
Nível de Risco: Alto
Plano de Resposta: Atuar junto ao legislativo para criação de normas claras.

Código: R-A36
Nome do Risco: Resistência Política à Transformação Digital
Descrição: Mudança de prioridades impede continuidade dos projetos digitais.
Impacto Potencial: Alto
Probabilidade: Alta
Nível de Risco: Crítico
Plano de Resposta: Formalizar políticas de Estado e envolver lideranças em capacitação.

5. ESTIMATIVA DA CAPACIDADE DE EXECUÇÃO DE TIC

ÁREA	SITUAÇÃO ATUAL	IMPACTO NA CAPACIDADE DE EXECUÇÃO
Infraestrutura de TI	Hardware e servidores obsoletos, sem garantia, sem padronização, sem licenciamento.	Reduz drasticamente a produtividade e confiabilidade. Aumenta custos e risco de falhas.
Rede e Comunicação	Equipamentos domésticos, rede sem gerenciamento, topologia instável.	Dificulta escalabilidade, segurança e disponibilidade dos serviços digitais
Segurança da Informação	Falta de política, ferramentas inadequadas, não conformidade com LGPD	Alto risco de incidentes e sanções legais, incapacidade de proteger dados e ativos
Data Center / Energia	Estrutura improvisada, sem redundância ou proteção adequada.	Elevado risco de indisponibilidade e perda de dados críticos
RH de TIC	Equipe pequena, sem capacitação contínua, alta dependência externa.	Limita a execução de projetos e sustentação dos sistemas; risco de perda de conhecimento técnico
Governança e Processos	Inexistência de políticas de backup, manutenção, controle de custos e inventário.	Aumenta ineficiência operacional e riscos organizacionais

5.1 – ANÁLISE DA CAPACIDADE ATUAL

Muito baixa – A equipe e a infraestrutura atuais são capazes de manter somente operações básicas e reativas. A execução de novos projetos estratégicos está altamente comprometida.

5.2 – GARGALOS-CHAVE IDENTIFICADOS

CATEGORIA	GARGALO
Tecnológico	Equipamentos e sistemas defasados, rede instável, ausência de redundância
Operacional	Falta de processos padronizados, gestão de ativos e indicadores
Pessoal	Número insuficiente de técnicos, sem plano de carreira ou capacitação
Jurídico/Regulatório	Riscos legais por uso de software sem licença e ausência de adequação à LGPD
Gestão de Riscos	Ausência de contingência, backups frágeis, segurança de informação falha

5.3 – CAPACIDADE INSTALADA X CAPACIDADE NECESSÁRIA

RECURSO/ CAPACIDADE	ESTIMATIVA HOJE	IDEAL PARA EXECUÇÃO PLENA
Profissionais de TIC	≅ 6 a 8 técnicos	12 a 18 (incluindo gestor, analistas, suporte, segurança)

Equipamentos compatíveis	< 30%	100% (computadores, impressoras, servidores atualizados)
Infraestrutura de rede	Obsoleta	Rede gerenciável, segmentada, segura e redundante
Segurança da informação	Inexistente	Múltiplas camadas, DPO, política formal, LGPD
Capacidade de resposta a falhas	Reativa e lenta	Preventiva, com redundância e automação

6. PLANEJANDO O LEVANTAMENTO DAS NECESSIDADES DE TIC

6.1 - CURTO PRAZO (0 A 6 MESES)

Objetivo: Estabilizar serviços essenciais, eliminar riscos críticos e criar base mínima de governança:

Infraestrutura:

- Substituição imediata de computadores mais obsoletos (prioridade: setores críticos);
- Aquisição emergencial de nobreaks para servidores e switches principais;
- Regularização de licenciamento de sistemas operacionais e antivírus;
- Início da estruturação do inventário de TI e auditoria dos ativos;

Segurança da Informação:

- Instituir Grupo Trabalho de privacidade de dados;
- Implantação de antivírus centralizado e controle de acesso básico por usuários;
- Elaboração e disseminação da primeira política de uso aceitável dos recursos de TI
-

Rede:

- Substituição de roteadores domésticos por modelos corporativos nos pontos críticos;
- Organização inicial do endereçamento IP e segmentação mínima da rede

Gestão e Processos:

- Criação de procedimentos documentados para backup, suporte e controle de equipamentos;
- Definição de prioridades de curto prazo com base em risco e impacto

6.2 – MÉDIO PRAZO (6 A 18 MESES)

Infraestrutura:

- Renovação completa do parque computacional com equipamentos padronizados por perfil;
- Implantação de impressoras corporativas gerenciadas;
- Implantação de software de inventário, gestão de ativos e helpdesk;
- Implantação de storage centralizado e servidores virtualizados com alta disponibilidade

Segurança da Informação:

- Aquisição e implantação de firewall corporativo (NGFW) com IDS/IPS;
- Implantação de sistema de backup automatizado (seguindo regra 3-2-1);
- Capacitação da equipe em LGPD e gestão de incidentes;
- Mapeamento de dados pessoais e definição de trilhas de auditoria

Rede:

- Redesenho da topologia de rede (VLANs, backbone redundante, monitoramento SNMP);
- Troca de switches Layer 1 por modelos Layer 2/3 gerenciáveis;
- Início da substituição do cabeamento estruturado por CAT 6A

Recursos Humanos:

- Contratação de equipe técnica complementar (analista de redes, segurança, suporte);
- Implementação de plano de capacitação técnica formal;
- Criação de plano de carreira e incentivos à certificação

Governança e Gestão:

- Criação de dashboard com indicadores de desempenho (KPIs);
- Implantação de processos com base em boas práticas (ITIL, COBIT);
- Criação de política de manutenção preventiva para todos os equipamentos

6.3 – LONGO PRAZO (18 A 48 MESES)

Infraestrutura:

- Construção/adaptação de Data Center conforme TIER III / NBR ISO/IEC 22237;
- Instalação de sala-cofre para dados essenciais;

- Conclusão da substituição do cabeamento estruturado e instalação de dutos e racks adequados;
- Implantação de sistema de monitoramento ambiental (temperatura, fumaça, umidade)

Segurança da Informação:
- Implantação de SIEM (monitoramento de eventos de segurança);
- Autenticação forte (MFA), criptografia de dados sensíveis, controle de acessos por perfil;
- Testes periódicos de resposta a incidentes, simulações de desastre e recuperação;
- Revisão e atualização contínua da política de segurança e privacidade

Rede:
- Contratação de links redundantes com failover automático;
- Adoção de VPN corporativa para acesso remoto seguro;
- Implementação de redes Wi-Fi segregadas por tipo de usuário

Recursos Humanos:
- Estabelecimento de uma estrutura permanente de TIC, com equipe completa;
- Implantação de programa de retenção de talentos e avaliação de desempenho técnica;
- Redução da dependência de terceiros para áreas estratégicas (virtualização, segurança)

Governança e Gestão:
- Planejamento estratégico de TIC alinhado com o plano diretor do município;
- Participação ativa da área de TIC nos projetos de todas as secretarias;
- Inclusão de indicadores de desempenho de TIC nos relatórios de gestão pública

7. IDENTIFICAR AS NECESSIDADES DE INFORMAÇÃO E COMUNICAÇÃO

O Levantamento das Necessidades de Informação e Comunicação (LNIC) deve focar em preencher as lacunas de maturidade digital, infraestrutura, normatização, serviços e capital humano, conforme o diagnóstico de "Cenário Atual".

7.1 - GOVERNANÇA E PLANEJAMENTO ESTRATÉGICO DE TIC

O foco é entender as necessidades de informação para criar e operar o modelo de governança e os documentos estratégicos ausentes **(Infraestrutura de TIC e Segurança Cibernética, Governança de Dados e Conformidade Legal, Oferta de Serviços Digitais e Capital Humano)**.

Eixo de Levantamento	O que precisa ser coletado (Informação/ Comunicação)	Objetivo Técnico
Parque de Computadores	1. **Inventário Ativo e Uso**: Quantidade exata, localização, idade, configuração (CPU, RAM, Disco) e função de cada equipamento. 2. **Especificação de Substituição**: Definição das especificações técnicas padronizadas (por perfil de usuário: administrativo, técnico, alta gestão) para a renovação. 3. **Levantamento de Licenças**: Detalhamento dos softwares essenciais e o status do licenciamento atual para a formalização da aquisição	Viabilizar a renovação completa, padronizar o hardware e software e eliminar riscos jurídicos.
Impressoras/ Periférico	1. **Mapeamento de Demanda**: Volume de impressão/cópia mensal por setor e tipo de documento (preto e branco, cor). 2. **Requisitos Funcionais**: Necessidade de multifuncionais, digitalização em rede, e recursos avançados. 3. **Especificação de Contrato**: Dados para o Termo de Referência de contratação de serviços de impressão (SLA, cotas, manutenção preventiva)	Implantação de parque corporativo, controle de custos e otimização do fluxo de trabalho.

Servidores e Virtualização	1. **Carga de Trabalho Atual**: Uso de CPU, memória e armazenamento (disco) dos servidores atuais. 2. **Requisitos de Capacidade**: Projeção de crescimento para Servidores, Storage (RAID 10/6) e infraestrutura virtual (Número de VMs e requisitos de HA). 3. **Seleção de Plataforma**: Definição da solução de virtualização a ser adotada (Hyper-V, RHV, Proxmox) para fins de licenciamento e treinamento.	Dimensionar e especificar a nova infraestrutura de servidores e storage com redundância e escalabilidade.
Proteção de Energia	1. **Mapeamento de Carga**: Levantamento da carga elétrica (kVA) real dos equipamentos críticos (servidores e switches de backbone). 2. **Requisitos de Autonomia**: Tempo mínimo de autonomia exigido para desligamento seguro em caso de falha de energia. 3. **Localização Crítica**: Identificação exata dos nodes críticos que exigem **Nobreaks Online de dupla conversão** e redundância.	Dimensionar corretamente os Nobreaks, garantindo a proteção de pelo menos 100% dos ativos críticos.
Data Center Físico	1. **Diagnóstico Estrutural Detalhado**: Pontos de não conformidade atuais em relação à NBR ISO/IEC 22237. 2. **Requisitos de Adequação**: Definição dos requisitos de climatização	Elaborar projeto de adequação física para atender a padrões de segurança e disponibilidade (TIER III).

	(**N+1**), piso elevado, sistemas de combate a incêndio (sem água) e segurança física (biometria/CFTV) para o projeto.	
Rede Lógica e Ativos	1. **Hierarquia e Segmentação**: Definição das VLANs necessárias (Administrativo, Convidados, VoIP, Servidores, CFTV). 2. **Especificação de Switches**: Quantidade e especificação técnica (Layer 2/3, Gerenciáveis, Suporte a QoS/SNMP/Port Security) para a substituição de toda a base.	Redesenhar a rede, implementando gerenciabilidade, controle e segurança granular nos acessos.
Topologia e Cabeamento	1. **Mapeamento de Conexão Crítica**: Levantamento das conexões entre secretarias que precisam de **redundância** (anéis duplos/ligações paralelas). 2. **Requisitos de Cabeamento**: Quantidade de pontos de rede e extensão total de **cabeamento Categoria 6A** necessário. 3. **Requisitos de Conectividade Externa**: Velocidade e quantidade de **links de internet de backup** para o failover automático.	Eliminar falhas recorrentes, garantir alta disponibilidade de rede e suportar a largura de banda.

Segurança e Conformidade (LGPD)	1. **Mapeamento de Dados Pessoais**: Inventário detalhado dos dados pessoais, localização, finalidade do tratamento e fluxo (para atendimento à LGPD). 2. **Requisitos de Proteção Ativa**: Especificação técnica e localização dos **Firewalls NGFW e IDS/IPS**. 3. **Requisitos de SIEM**: Volume de eventos (logs) gerados pela rede e sistemas para dimensionar a solução de monitoramento.	Atingir a conformidade com a LGPD e implementar uma defesa em múltiplas camadas (segurança ativa e passiva).
Recursos Humanos de TI	1. **Dimensionamento do Quadro**: Definição do número ideal de profissionais por perfil (**Analistas de Redes/SI, Administradores, Técnicos de Suporte**) e a distribuição de responsabilidades. 2. **Requisitos de Capacitação**: Levantamento dos treinamentos e certificações prioritárias (LGPD, ITIL, Cisco, Microsoft) para o plano de capacitação anual.	Estruturar um quadro de TI adequado, reduzindo a dependência de terceiros e retendo o conhecimento institucional.

8. IDENTIFICAR AS NECESSIDADES DE SERVIÇOS DE TIC

Com base em todo o histórico apresentado, incluindo o diagnóstico técnico, cenário ideal, análise de capacidade e planejamento por fases, podemos agora identificar de forma objetiva as necessidades de serviços de TIC. Aqui, "serviços de TIC se referem às necessidades de Infraestrutura, Contratações e Pessoal de forma a garantir que as entregas, operações ou funções tecnológicas sejammantidas ou implementadas garantindo o funcionamento pleno da área de tecnologia da Prefeitura Municipal de Arraial do Cabo.

8.1 – NECESSIDADES DE INFRAESTRUTURA DE TIC

8.1.1 - Necessidades Críticas de Infraestrutura de TIC

ÁREA	NECESSIDADE DE INFRAESTRUTURA	JUSTIFICATIVA
Servidores e Data Center	**Renovação de Servidores Modernos** (em rack com fontes redundantes). **Solução de Storage Escalável** (Ex: RAID 6/10). **Solução de Virtualização Licenciada.**	Eliminar o risco de falha de hardware obsoleto, permitir expansão planejada e garantir alta disponibilidade (HA) de sistemas.
Proteção de Energia	**Nobreaks Online de Dupla Conversão** para ativos críticos. **Plano de Manutenção Preventiva** (principalmente baterias)	Garantir desligamento seguro e proteger equipamentos/dados contra instabilidade elétrica.
Data Center Físico	**Projeto de Adequação Estrutural** (NBR ISO/IEC 22237). **Climatização Redundante** (N+1). **Sistema de Detecção e Combate a Incêndios** (sem água).	Oferecer um ambiente seguro e controlado, essencial para a longevidade e funcionamento dos novos servidores e storage.

Backup	**Rotinas Rigorosas e Automatizadas de Backup (3-2-1). Mídia de Backup Dedicada e Off-site.**	Eliminar o risco de perda definitiva de dados, garantindo a **recuperação de desastres (DR).**

8.1.2 – Necessidades de Contratação de Rede e Conectividade

ÁREA	NECESSIDADE DE INFRAESTRUTURA	JUSTIFICATIVA
Switches e Roteadores	Switches Gerenciáveis (Layer 2/3). Roteadores Corporativos/Firewall (NGFW).	Possibilitar a segmentação lógica da rede (**VLANs**), implementar controle de acesso (QoS, Port Security) e integrar funções avançadas de segurança na borda.
Topologia de Rede	**Redesenho da Topologia** com redundância (anéis duplos/ligações paralelas). **Cabeamento Estruturado (Cat. 6A),** organizado e certificado.	Eliminar falhas recorrentes e instabilidade. Melhorar a largura de banda e facilitar a manutenção, separando dados da rede elétrica.
Conectividade Externa	**Links de Internet de Backup Dedicados com Failover Automático.**	Garantir a disponibilidade e continuidade dos serviços digitais municipais mesmo em caso de falha de um link principal.

Proteção Ativa	**Firewalls NGFW (Next-Generation Firewall). Sistemas IDS/IPS. Solução Anti-malware Centralizada (Endpoint Protection)**.Implementar defesa em múltiplas camadas, monitorar tráfego malicioso e gerenciar a segurança em todo o parque.	Implementar defesa em múltiplas camadas, monitorar tráfego malicioso e gerenciar a segurança em todo o parque.
Monitoramento	**SIEM (Security Information and Event Management)** e/ou **Sistema de Monitoramento Centralizado.**	Coletar, analisar logs e alertar sobre vulnerabilidades e incidentes em tempo real, essenciais para a **resposta a incidentes.**
Controle de Acesso	**Infraestrutura para Autenticação Forte (MFA)** e **Controle de Acesso por Perfil/Criticidade.**	Cumprir requisitos de segurança e LGPD, garantindo que apenas usuários autorizados tenham acesso aos recursos, conforme a necessidade

8.1.3 – Necessidades de Infraestrutura de Pessoal de TIC

ÁREA	JUSTIFICATIVA
Gestor/ Coordenador de Projetos de TIC	Essencial para planejar e supervisionar a transição do cenário atual para o ideal, gerenciar os múltiplos projetos (Data Center, Rede, Servidores) e garantir o alinhamento com a estratégia.

Administrador de Servidores e Virtualização	Profissional especializado para gerenciar o novo ambiente virtualizado (Hyper-V, RHV, Proxmox), configurar a alta disponibilidade (HA) e administrar as rotinas rigorosas de backup e recuperação de desastres (DR).
Analista de Redes e Segurança	Profissional focado em configurar e manter os novos switches gerenciáveis (VLANs, QoS, etc.), os firewalls NGFW, IDS/IPS, e gerenciar a topologia de rede estável.
Analista de Segurança da Informação	Profissional para atuar na criação das políticas de segurança documentadas e resposta a incidentes, auxiliando o DPO
Técnicos de Suporte	Aumento do quadro de técnicos para atender às demandas rotineiras, liberando os especialistas para projetos estratégicos.

9. CONSOLIDAR O INVENTÁRIO DE NECESSIDADES

Anexo 1 – Inventário das Necessidades Consolidadas

10. ALINHAR AS NECESSIDADES DE TIC ÀS ESTRATÉGIAS DA ORGANIZAÇÃO

O presente relatório abaixo alinha a Estratégia de Governo Digital (EGD) da Prefeitura Municipal de Arraial do Cabo (Versão 1.0, 2025-2035) com as necessidades críticas de infraestrutura de Tecnologia da Informação e Comunicação (TIC) identificadas no plano de ação. A EGD diagnostica um "Parque Tecnológico ultrapassado e defasado" e uma "Baixíssima maturidade digital institucional", o que justifica plenamente o detalhamento das necessidades de infraestrutura de base, rede, segurança e pessoal técnico para o sucesso da transformação digital.

10.1 - ALINHAMENTO COM NECESSIDADES CRÍTICAS DE INFRAESTRUTURA DE BASE (SERVIDORES, DATA CENTER E BACKUP)

A necessidade de modernização da infraestrutura de base é um fator implícito e essencial para suportar o Cenário Almejado da EGD em todas as dimensões, principalmente a de Segurança Cibernética e Governança de Dados.

Dimensão da EGD	Necessidade Crítica de Infraestrutura de Base	Alinhamento da EGD (Cenário, Objetivo ou Fator Chave)
SEGURANÇA CIBERNÉTICA	Servidores e Data Center (Renovação, Storage, Virtualização)	**Cenário Atual:** "Parque Tecnológico ultrapassado e defasado." **Cenário Almejado**: "Upgrade no Parque Tecnológico." **Objetivo**: "Garantir a segurança e eficiência do parque tecnológico."
	Proteção de Energia (Nobreaks Online)	**Cenário Almejado**: "Monitoramento REAL TIME da infraestrutura e soluções tecnológicas." (Equipamentos de energia estáveis são a base do monitoramento).
	Data Center Físico (Adequação, Climatização, Incêndios)	**Fator Chave**: "Renovação e Modernização Contínua dos Ativos de TI." (A modernização exige um ambiente físico adequado para garantir a longevidade e segurança dos equipamentos.)

	Backup (Rotinas Automatizadas, Mídia Off-site)	**Cenário Atual**: Ausência de PSI e Plano de Contingência. **Objetivo**: "Elaborar um Plano Municipal de Contingência Cibernética." (Backup é o pilar da recuperação de desastres.)
GOVERNANÇA DE DADOS	Servidores e Data Center (HA, Storage Escalável)	**Objetivo**: "Garantir a conformidade com a LGPD." (A LGPD exige disponibilidade e integridade dos dados, que dependem diretamente de servidores, storage e virtualização licenciada e redundante.)

10.2 - ALINHAMENTO COM NECESSIDADES DE CONTRATAÇÃO DE REDE E CONECTIVIDADE

As dimensões **"INFRAESTRUTURA DE SOLUÇÕES DIGITAIS"** e **"SEGURANÇA CIBERNÉTICA"** abordam diretamente a conectividade e a rede, tornando as necessidades de **Switches, Topologia e Conectividade Externa** ações prioritárias para a EGD.

Dimensão da EGD	Necessidade Crítica de Infraestrutura de Base	Alinhamento da EGD (Cenário, Objetivo ou Fator Chave)
INFRAESTRUTURA DE SOLUÇÕES DIGITAIS	Switches e Roteadores (Gerenciáveis, NGFW)	**Cenário Almejado**: "Fornecimento de conexão gratuita sem fio nos espaços públicos." **Fator Chave**: "Garantir o fornecimento de conexão gratuita sem fio (Wi-Fi) em espaços públicos." (Requer switches e roteadores modernos e gerenciáveis para segmentação e QoS.)
	Topologia de Rede (Redesenho, Redundância, Cabeamento)	**Objetivo:** "Aumentar a eficiência e a agilidade dos serviços públicos através de soluções digitais." (Serviços digitais eficientes dependem de uma rede estável e de alta velocidade.)
	Conectividade Externa (Links Dedicados com Failover)	**Cenário Atual:** "Conectividade (conexão de internet) não satisfatória." **Objetivo**: "Melhorar a conectividade e infraestrutura tecnológica." (O failover é essencial para garantir a continuidade dos serviços digitais.)

SEGURANÇA CIBERNÉTICA	Switches e Roteadores (NGFW, Segmentação)	**Fator Chave:** "Desenvolvimento e Implementação de Políticas de Segurança da Informação." (A segmentação de rede via switches e o NGFW são pilares de uma PSI moderna.)

10.3 - ALINHAMENTO COM NECESSIDADES DE INFRAESTRUTURA DE SEGURANÇA E CONFORMIDADE

A conformidade com a legislação federal (LGPD, Lei do Governo Digital) e a necessidade de proteger os dados municipais são objetivos centrais da EGD, sendo as necessidades de segurança e monitoramento as ferramentas para atingi-los.

Dimensão da EGD	Necessidade Crítica de Infraestrutura de Base	Alinhamento da EGD (Cenário, Objetivo ou Fator Chave)
SEGURANÇA CIBERNÉTICA	Proteção Ativa (Firewalls NGFW, IDS/IPS, Anti-malware)	**Cenário Atual:** Ausência de PSI e Tratamento de Incidentes. **Objetivo**: "Elaborar e implementar uma Política de Segurança da Informação (PSI)." (Estes ativos são a execução prática da PSI e dos Planos de Contingência.)

	Monitoramento (SIEM/Sistema Centralizado)	**Cenário Almejado**: "Monitoramento REAL TIME da infraestrutura e soluções tecnológicas." **Objetivo**: "Implementar sistemas de monitoramento em tempo real da infraestrutura de TI."
	Controle de Acesso (MFA, Controle por Perfil)	**Fator Chave:** "Gestão de Riscos e Conformidade Legal."

10.4 - ALINHAMENTO COM NECESSIDADES DE INFRAESTRUTURA DE PESSOAL DE TIC

A "**DIMENSÃO: CAPITAL HUMANO**" é diretamente atendida pela contratação de pessoal especializado. A baixa maturidade digital e a ausência de especialistas são pontos críticos que a EGD e a contratação de pessoal técnico visam resolver.

Dimensão da EGD	Necessidade Crítica de Infraestrutura de Base	Alinhamento da EGD (Cenário, Objetivo ou Fator Chave)
CAPITAL HUMANO	Gestor/Coordenador de Projetos de TIC	**Cenário Atual**: "Baixo incentivo a facilitadores digitais." **Objetivo**: "Estabelecer planejamento estratégico claro para a transformação digital." (O Gestor é essencial para o planejamento e a implementação da EGD e do PDTIC.)

	Administrador de Servidores e Virtualização	**Ponto de Atenção:** "Carência de Especialistas em Tecnologia." **Objetivo:** "Aumentar a capacitação contínua dos servidores públicos." (A contratação supre a carência imediata e serve como base para a transferência de conhecimento.)
GOVERNANÇA DIGITAL	Gestor/Coordenador de Projetos de TIC	**Objetivos**: "Elaborar o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC)" e "Elaborar o Plano de Contratação Anual de TI (PCA de TI)." (A coordenação técnica é necessária para a elaboração desses planos estratégicos.)
SEGURANÇA CIBERNÉTICA	Profissionalização da rede (VLANs, QoS) e implementação técnica da segurança na borda (Firewalls NGFW, IDS/IPS), essenciais para o "Upgrade nas estruturas municipais de conectividade". Perfil necessário: Analista de Redes e Segurança.	**Objetivo:** "Implementar sistemas de monitoramento em tempo real da infraestrutura de TI." Fator Chave: "Integração de Conectividade e Infraestrutura Tecnológica."

	Criação das "políticas de segurança documentadas" e implementação da "capacidade de resposta rápida e eficiente a incidentes de segurança." Perfil necessário: Analista de Segurança da Informação.	**Objetivos:** "Elaborar e implementar uma Política de Segurança da Informação (PSI)." "Elaborar uma Política de Tratamento de Incidentes de Segurança da Informação."
GOVERNANÇA DE DADOS	Apoio ao Encarregado de Dados (DPO) na garantia da segurança dos dados pessoais e na gestão da conformidade.	**Objetivo:** "Garantir a conformidade com a LGPD."
CAPITAL HUMANO	Liberar os especialistas (Analistas) para projetos de transformação, garantindo que as demandas rotineiras não atrasem o avanço da EGD.	**Ponto de Atenção:** "Desmotivação e Baixo Engajamento dos Servidores." (Suporte adequado melhora o ambiente de trabalho). **Objetivo:** "Melhorar a qualidade no atendimento ao cidadão." (Suporte interno eficiente reflete no serviço externo).

10.5. PLANO DE AÇÃO – NECESSIDADES TIC

Eixo de Atuação	Ação Estratégica	Descrição Detalhada	Responsável / Unidade	Prazo Estimado	Recursos Necessários
Infraestrutura de Base	Renovação de Servidores e Storage	Aquisição e instalação de servidores em rack com fontes redundantes e storage escalável (RAID 6/10) com virtualização licenciada (Hyper-V/VMware/Proxmox).	Ciência e Tecnologia	12 meses	
Infraestrutura de Base	Implantação de Nobreaks Online e Plano de Manutenção	Instalação de nobreaks de dupla conversão em todos os racks críticos e criação de rotina de manutenção preventiva de baterias	Ciência e Tecnologia	12 meses	
Infraestrutura Física	Aquisição do Data Center Municipal	Aquisição física conforme NBR ISO/IEC 22237, instalação de climatização redundante (N+1) e sistema de combate a incêndio sem água.	Ciência e Tecnologia	12 meses	
Backup e Continuidade	Elaboração de uma Política de Backup	Elaborar Política de Backup estabelecendo procedimentos para criação, armazenamento e verificação de cópias de segurança, assegurando a integridade e recuperação dos dados em caso de falhas ou incidentes.	Ciência e Tecnologia	3 meses	
Backup e Continuidade	Implantação de Rotinas de Backup 3-2-1 e Mídia Off-site	Implantar software automatizado de backup com replicação externa e testes periódicos de restauração.	Ciência e Tecnologia	12 meses	
Rede e Conectividade	Aquisição de Switches Gerenciáveis e Roteadores Corporativos (NGFW)	Substituir equipamentos legados por switches L2/L3 e roteadores corporativos com firewall integrado e QoS.	Ciência e Tecnologia	12 meses	
Rede e Conectividade	Redesenho da Topologia de Rede	Implementar topologia redundante (anéis duplos) e cabeamento estruturado Cat 6A certificado.	Ciência e Tecnologia	12 meses	
Rede e Conectividade	Links de Internet de backup	Ofertar conexões alternativas que entram em operação automaticamente quando o link principal falha, garantindo a continuidade das atividades corporativas sem interrupções perceptíveis.	Ciência e Tecnologia	12 meses	
Rede e Conectividade	Poluição visual, risco de acidentes e dificuldade de manutenção	Eliminar os riscos de acidentes, facilitando as ações de manutenção	Ciência e Tecnologia	12 meses	
Conectividade Externa	Links Dedicados e Failover Automático	Contratar links de internet redundantes com balanceamento e failover automático.	Ciência e Tecnologia	18 meses	
Segurança e Conformidade	Elaboração de uma Política de Segurança da Informação	Definir diretrizes para proteger dados, sistemas e recursos tecnológicos, garantindo confidencialidade, integridade, disponibilidade e conformidade com normas e legislações vigentes.	Ciência e Tecnologia	3 meses	
Segurança e Conformidade	Ausência de avaliação de desempenho e análise crítica sobre a segurança da informação	Garantir a eficácia dos controles, identificar vulnerabilidades e promover melhorias contínuas	Ciência e Tecnologia	12 meses	
Segurança e Conformidade	Implantar Firewall NGFW, IDS/IPS e Anti-malware Centralizado	Implantar proteção multicamadas e monitoramento em tempo real.	Ciência e Tecnologia	12 meses	

Segurança e Conformidade	Implantar Sistema SIEM para Monitoramento Centralizado	Coleta e análise automatizada de logs e eventos de segurança	Ciência e Tecnologia	12 meses	
Segurança e Conformidade	Implantar Autenticação Forte (MFA) e Controle de Acesso	Definir políticas de acesso por criticidade e implementar autenticação multifator.	Ciência e Tecnologia / DPO (Data Protection Officer)	12 meses	
Segurança e Conformidade	Planos de contingência e Recuperação de Desastres	Desenvolver e testar regularmente planos de contingência e recuperação em caso de desastres	Ciência e Tecnologia	12 meses	
Segurança e Conformidade	Papéis, Responsabilidades e autoridades em	Estabelecer papéis, responsabilidades e	Ciência e Tecnologia	12 meses	
	Segurança da Informação	Autoridades em Segurança da Informação			
Segurança e Conformidade	Tratar a ausência de gerência sobre os riscos de segurança da informação	Promover a identificação, avaliação, mitigação e monitoramento adequados das ameaças que podem comprometer a confidencialidade, integridade e disponibilidade dos dados.	Ciência e Tecnologia	18 meses	
Segurança e Conformidade	Tratar Ausência de governança sobre a segurança da informação	Ofertar um conjunto de processos, políticas, diretrizes e estruturas responsáveis por assegurar que a segurança da informação esteja alinhada à estratégia do negócio e que os riscos sejam gerenciados adequadamente	Ciência e Tecnologia	18 meses	
Segurança e Conformidade	Tratar Ausência de tratamento dos ativos não autorizados encontrados na infraestrutura institucional	Reduzir as vulnerabilidades, acessos indevidos, falhas operacionais e comprometimento da integridade, confidencialidade e disponibilidade dos dados.	Ciência e Tecnologia	18 meses	
Segurança e Conformidade	Tratar a Ausência de seguridade para que todo software autorizado seja	Buscar a estabilidade, segurança e continuidade operacional da organização. O suporte oficial do	Ciência e Tecnologia	18 meses	
	suportado pelo fabricante	fabricante é fundamental para garantir que o software funcione corretamente, receba atualizações de segurança e tenha resolução técnica adequada em caso de problemas			
Segurança e Conformidade	Tratar a ausência de processos voltados a gestão de dados	Promover o controle, proteção e aproveitamento eficaz das informações, eliminando as perdas, acessos indevidos e não conformidade legal.	Ciência e Tecnologia	18 meses	
Segurança e Conformidade	Tratar a ausência de lista de controle de acesso e dados institucional	Criar a lista de controle, garantindo uma ferramenta essencial para definir e gerenciar quem pode acessar, modificar ou compartilhar os dados e recursos institucionais.	Ciência e Tecnologia	18 meses	
Segurança e Conformidade	Tratar a ausência de política institucional referente a descarte de dados com segurança	Elaborar uma política institucional referente ao descarte seguro de dados, eliminando significativamente riscos como vazamento de informações sensíveis, não conformidade legal, perda de confiança e impactos financeiros.	Ciência e Tecnologia	12 meses	

Segurança e Conformidade	Tratar a ausência de procedimento de hardening expondo fragilidades no processo de configuração segura	Reduzir/Eliminar fragilidades significativas no processo de configuração segura, reduzindo o a superfície de ataque e a vulnerabilidade a ameaças cibernéticas.	Ciência e Tecnologia	12 meses	
Segurança e Conformidade	Tratar a ausência de implementação e gerencia de firewalls nos servidores e dispositivos de usuários finais	Reduzir/Eliminar fragilidade crítica na segurança da infraestrutura institucional, que expõem a ede a ameaças, acessos não autorizados e ataques cibernéticos.	Ciência e Tecnologia	12 meses	
Segurança e Conformidade	Tratar a ausência de tratamento das contas padrão dos ativos e softwares	Reduzir/Eliminar riscos significativos para a segurança da informação, pois as contas padrão geralmente vêm com configurações e privilégios altos que, se não modificados, podem ser explorados por atacantes para obter acesso não autorizado ao sistema.	Ciência e Tecnologia	12 meses	
Segurança e Conformidade	Tratar a não utilização de senhas exclusivas	Reduzir/Eliminar riscos elevados para a segurança da informação, pois aumenta a probabilidade de acessos não autorizados e comprometimento de	Ciência e Tecnologia	12 meses	
		múltiplas contas em caso de vazamento.			
Segurança e Conformidade	Número insuficiente de profissionais especializados para atendimento de demandadas rotineiras e de projetos estruturantes	Investir em capacitação contínua e programas de formação especializados. Criar políticas de retenção e valorização dos profissionais; Uso de tecnologias de automação e Inteligência Artificial para completar a equipe humana.	Ciência e Tecnologia	3 meses	
Segurança e Conformidade	Tratar a ausência de política institucional voltada a desabilitação de contas inativas após um tempo pré-definido	Elaborar Política eficaz definindo prazo máximo para a inatividade, levando à desabilitação automática. Implementar auditorias periódicas para identificar contas inativas, etc...	Ciência e Tecnologia	12 meses	
Segurança e Conformidade	Tratar a ausência de processo institucional para a concessão de acesso	Reduzir/Eliminar fragilidades críticas na segurança da informação, implementando um processo institucional claro de concessão de acesso	Ciência e Tecnologia	12 meses	
Segurança e Conformidade	Tratar a ausência de autenticação multifator para autorização dos usuários a seus ativos	Fortalecer a segurança da autorização de usuários em seus ativos, protegendo a organização contra uma ampla gama de ameaças	Ciência e Tecnologia	12 meses	
		cibernéticas e melhorando sua postura de segurança.			
Segurança e Conformidade	Tratar a ausência de política institucional voltada a restringir os privilégios de administrador às contas dedicadas para o perfil de administrador	Proteger a organização de riscos internos e externos, assegurar conformidade e manter a integridade dos sistemas.	Ciência e Tecnologia	12 meses	
Segurança e Conformidade	Tratar a ausência de processo institucional para revogação de acesso	Mitigar riscos de segurança, assegurar conformidade e proteger os ativos da organização contra acessos indevidos.	Ciência e Tecnologia	12 meses	

Segurança e Conformidade	Regularização e Gestão de Licenciamento de Softwares	Mapear e adquirir licenças legais de sistemas operacionais, pacotes Office e demais softwares essenciais. Implantar ferramenta de inventário e controle de licenciamento (Software Asset Management – SAM).	Ciência e Tecnologia	12 meses	
Pessoal de TIC	Contratação de Administrador de Servidores e Virtualização	Profissional especializado para manter o ambiente virtualizado e políticas de backup/DR.	Ciência e Tecnologia / Administração	12 meses	
Pessoal de TIC	Contratação de Analista de Redes e Segurança		Ciência e Tecnologia / Administração	12 meses	
Pessoal de TIC	Contratação de Analista de Segurança da Informação/Cibernética		Ciência e Tecnologia / Administração	12 meses	
Pessoal de TIC	Ampliação do Quadro de Técnicos de Suporte	Reforçar o suporte operacional para liberar especialistas para projetos estratégicos.	Ciência e Tecnologia / Administração	12 meses	
Pessoal de TIC	Capacitação	Ofertar cursos de capacitação	Ciência e Tecnologia	12 meses	
Pessoal de TIC	Ausência de plano de carreira, incentivos à certificação e política de treinamento continuado.	Oferecer aos colaboradores uma visão clara de crescimento profissional, definindo etapas, competências requeridas e oportunidades dentro da área de segurança da informação. Possibilitará reter talentos, aumentar a satisfação e criar uma equipe qualificada e engajada ao longo do tempo	Ciência e Tecnologia	18 meses	
Continuidade de Negócios	Elaboração e Implantação do Plano de Recuperação de Desastres (PRD).	Definir procedimentos e infraestrutura para recuperação de sistemas críticos, com testes anuais de restauração e plano de contingência	Ciência e Tecnologia	18 meses	
Sistemas e Serviços Digitais	Inventário e catálogo oficial dos sistemas utilizados	Elaborar inventário e catálogo oficial dos sistemas utilizados	Ciência e Tecnologia	12 meses	
Sistemas e Serviços Digitais	Oferta de serviços digitais	Oferecer serviços digitais acessíveis, inclusivos e centrados no cidadão, com canais de comunicação eficientes e eficazes.	Ciência e Tecnologia	06 meses	
Sistemas e Serviços Digitais	Interoperabilidade	Priorizar a integração dos sistemas para eliminar redundâncias e promover interoperabilidade	Ciência e Tecnologia	36 meses	
Governança e Gestão de TIC	Indicadores de desempenho	Definir indicadores de desempenho (KPIs) para monitoramento do progresso do PDTIC	Ciência e Tecnologia	12 meses	
Governança e Gestão de TIC	Inventário detalhado de ativos corporativos	Criar o Inventário Detalhado de Ativos Corporativos	Ciência e Tecnologia	12 meses	
Governança e Gestão de TIC	Inventário detalhado de softwares	Criar o Inventário Detalhado de Softwares	Ciência e Tecnologia	12 meses	
Governança e Gestão de TIC	Tratamento de softwares não autorizados	Identificar, bloquear e remover esses programas dos sistemas de uma organização para garantir segurança e conformidade	Ciência e Tecnologia	12 meses	
Governança e Gestão de TIC	Inventário de Dados	Criar o Inventário de Dados	Ciência e Tecnologia	12 meses	

Governança e Gestão de TIC	Retenção de Dados	Reter dados seguindo princípios de proteção, privacidade e conformidade regulatória	Ciência e Tecnologia	12 meses	
Governança e Gestão de TIC	Criptografia dos dados nos dispositivos dos usuários	Garantir a proteção das informações pessoais e sensíveis contra acessos não autorizados, vazamentos e ataques cibernéticos	Ciência e Tecnologia	12 meses	
Governança e Gestão de TIC	Bloqueio automático de sessão nos ativos corporativos	Bloquear o acesso aos dispositivos após um período de inatividade, protegendo dados e sistemas contra acessos não autorizados	Ciência e Tecnologia	12 meses	
Governança e Gestão de TIC	Gerência de ativos de softwares de maneira segura	Assegurar o controle, utilização adequada e proteção dos softwares dentro do ambiente corporativo	Ciência e Tecnologia	12 meses	
Governança e Gestão de TIC	Inventário detalhado de contas	Promover o registro sistemático e minucioso de todas as contas usadas pela empresa, como contas de usuário, contas financeiras, e contas de sistemas, visando controle, segurança e conformidade	Ciência e Tecnologia	12 meses	
Governança e Gestão de TIC	Controles de acesso por criticidade, mecanismos de resposta e mitigação a incidentes	Proteger os ativos de uma organização, priorizando recursos e respostas conforme a importância e o risco associado.	Ciência e Tecnologia	12 meses	
Governança e Gestão de TIC	Implantação de Sistema de Impressão Corporativa	Substituir impressoras residenciais por multifuncionais corporativas com cotas e controle de custos, via contrato de outsourcing com manutenção preventiva.	Ciência e Tecnologia	12 meses	

ANEXO II - PLANO DE CONTRATAÇÃO ANUAL TI – 2026 – ESTIMATIVA GLOBAL

ITEM	SETOR	VALOR ESTIMADO
1	SECRETARIA DE ADMINISTRAÇÃO TRIBUTÁRIA	1.024.000,00
2	SECRETARIA DE ASSISTÊNCIA SOCIAL	750.000,00
3	SECRETARIA DE CULTURA	200.000,00
4	SECRETARIA DE FINANÇAS E ORÇAMENTO	3.612,50
5	FIPAC	257.000,00
6	FUNDAÇÃO DO MEIO-AMBIENTE – FUNTEC	221.839,31
7	SECRETARIA DE MEIO-AMBIENTE E SANEAMENTO	265.400,00
8	SECRETARIA DE SEGURANÇA PÚBLICA	135.600,00
9	SECRETARIA DE HABITAÇÃO E REGULARIZAÇÃO FUNDIÁRIA	255.000,00
10	INSTITUTO DE DESENVOLVIMENTO DE ARRAIAL DO CABO – IDAC	219.500,00
11	INSTITUTO DE PREVIDÊNCIA CABISTA – IPC	111.000,00
12	SECRETARIA DE MOBILIDADE URBANA	7.000.000,00
13	SECRETARIA DE OBRAS	285.000,00
14	SECRETARIA DE POSTURA	187.000,00
15	PROCON	0,00
16	PROCURADORIA GERAL DO MUNICÍPIO	19.200,00
17	SECRETARIA DE SAÚDE	2.400.000,00
18	SECRETARIA DE COMPRAS E LICITAÇÃO	49.200,00
19	SECRETARIA DE SERVIÇOS PÚBLICOS	198.000,00
20	SECRETARIA MUNICIPAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA E ESPORTE E LAZER	60.445.000,00
TOTAL GLOBAL		**74.026.351,81**

SÍNTESE E CONCLUSÃO FINAL

A Estratégia de Governo Digital (EGD) de Arraial do Cabo, alinhada a este Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) elaborado para a Prefeitura Municipal, apresentam um diagnóstico preciso do cenário de "Baixíssima maturidade digital institucional" e de um "Parque Tecnológico ultrapassado" e em grande parte obsoleto". O plano de ação e as necessidades críticas detalhadas configuram uma abordagem coesa para a transformação digital no decênio 2025-2035, destacando os recursos humanos e tecnológicos como elementos interdependentes essenciais para o sucesso dessa trajetória.

Este PDTIC deverá ser revisto periodicamente de modo a mantermos o plano sempre alinhado com as mudanças tecnológicas, demandas institucionais e riscos emergentes, garantindo assim a efetividade e a segurança dos serviços de TIC. A revisão anual permite atualizar necessidades, incorporar novas prioridades, adaptar-se a alterações regulatórias, como a LGPD, e corrigir eventuais falhas identificadas.

Pontos de Atenção:

- Contratos com empresas terceirizadas que prestam serviços de TI;
- Infraestrutura elétrica;
- Equipe de Desenvolvimento item 8.1.3