PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO E TELECOM DE TIJUCAS DO SUL

ANO 2023-2027

TIJUCAS DO SUL
JANEIRO - 2023

SUMÁRIO

ÍNDICE DE TABELAS

ÍNDICE DE FIGURAS

INTRODUÇÃO

Atualmente vivemos em um mundo altamente globalizado, caracterizado por constantes transformações, e inundado regularmente por novos produtos, serviços e descobertas. Isso tem feito com que as organizações também da gestão pública se preocupem cada vez mais em identificar a melhor forma de empregar seus recursos, buscando a melhoria na qualidade dos serviços prestados ao cidadão. Isso significa melhorias no ambiente da gestão pública pelo aumento da eficácia organizacional: a agilidade nos processos, na estrutura, na comunicação e na eliminação da burocracia.

Na atual “Era da Informação”, o uso estratégico da tecnologia da informação e a administração dos recursos de informática podem e devem melhorar o atendimento da população e no desenvolvimento sustentável do município.

Nesse contexto, a Tecnologia da Informação (TI), que durante muito tempo foi considerada apenas um item de suporte aos processos internos, uma fonte de despesas, sem influência direta nos objetivos e metas da gestão pública, deve ser repensada como um fator crítico para a prestação de serviços públicos, resultando no crescimento da atuação do poder público, exercendo assim, um forte domínio sobre os interesses da população.

A Prefeitura Municipal de Tijucas do Sul (PMTS), denominada entidade de direito pública do Poder Executivo, não distante do cenário revolucionário da “Era da Informação”, vive a necessidade de transformação de seu cenário tecnológico, precisamente no que diz respeito à informação, para alcançar a maturidade através de uma readequação de sua estrutura de tecnologia da informação ao novo cenário de desenvolvimento municipal.

CAPÍTULO I – PLANEJAMENTO ESTRATÉGICO

1. REFERENCIAIS ESTRATÉGICOS DA UNIDADE DE INFORMÁTICA

1.1. Missão

"Prover sistematicamente a aplicação de conhecimentos em tecnologia da informação por meio de soluções e serviços, integrado às estratégias da Prefeitura Municipal de Tijucas do Sul, contribuindo para a melhoria na prestação de serviços ao cidadão e ao desenvolvimento municipal."

1.2. Visão

"Integrar os serviços e as tendências de tecnologia da informação cada dia mais na gestão municipal de Tijucas do Sul."

1.3. Negócio

"Apoio tecnológico aos projetos municipais, prestação de serviço de suporte técnico, manutenção reativa e proativa, integração e administração de sistemas de gestão e infraestrutura de tecnologia da informação nas unidades da gestão municipal de Tijucas do Sul".

Com vista aos objetivos estratégicos do município, este Plano Diretor de Tecnologia da Informação e Telecom pretende estabelecer linhas coerentes e concisas capazes de nortear a Unidade de Tecnologia da Informação para com seus investimentos em infraestrutura, sistemas corporativos e de apoio ao cidadão.

1.4. Forças e Fraquezas

Tabela 1 - Forças e Fraquezas

Foco	Forças	Fraquezas
Pessoas, Processos e Organização.	• Profissionais resilientes e motivados para o desempenho de suas atividades; • Sinergia e integração entre os profissionais da equipe; • Consciência da necessidade de readequação da estrutura; • Compreensão da tecnologia como investimento; • Satisfação dos usuários com relação aos profissionais de atendimento; • Boa integração entre o departamento e a demais áreas da gestão municipal.	• Superalocação de atividades para funcionários do departamento; • Equipe com conhecimentos técnicos limitados; • Atividades de caráter confidencial e críticas nas mãos de terceiros; • Ausência de planos de treinamento para aperfeiçoamento e evolução da equipe; • Ausência de políticas para conscientização da segurança da informação; • Região carente de fornecimento de mão-de-obra qualificada; • Baixo vínculo prático do Plano Diretor Municipal com os investimentos em TI; • Carência de analistas de negócios para promover a interface entre tecnologia e a gestão pública; • Inexistência de processos e fluxos de trabalho formais; • Gestão descentralizada da estrutura de tecnologia da informação de toda a Prefeitura.
Sistemas e Bancos de Dados	• Visão voltada para a melhoria no provimento de serviços corporativos; • Sistema de Gestão Municipal relativamente aderente às necessidades dos usuários.	• Ausência de sistemas com recursos de tolerância a falhas; • Módulo do sistema localizado e administrado externamente; • Inexistência de meios de proteção/auditoria; • Mão-de-obra carente de conhecimentos específicos em bancos de dados.

Foco	Forças	Fraquezas
Infraestrutura de Tecnologia da Informação	• Foco atual voltado na reestruturação e modernização da infraestrutura; • Novos investimentos na eminência de serem realizados na reestruturação física e lógica da rede.	• Infraestrutura obsoleta e carente de investimentos; • Região carente de fornecimento de equipamentos e serviços; • Recursos tecnológicos limitados para o provimento de novas rotinas e controles; • Tráfego limitado ou inexistente entre unidades remotas/secretarias; • Conectividade Internet com redundância manual.
Segurança da Informação	• Consciência da necessidade de readequação da estrutura de segurança; • Existência de cópias de segurança em diversos locais.	• Ausência de solução automatizada para cópias de segurança (backups); • Baixa conscientização dos usuários quanto ao valor da informação; • Necessidade de aprimoramento e adequações aos sistemas de segurança lógicos existentes; • Ausência de planos e procedimentos de continuidade do negócio; • Perímetro Internet com proteção insuficiente.

1.5. Objetivos

Os objetivos estratégicos da Unidade de Tecnologia da Informação, devidamente alinhados aos objetivos estratégicos da gestão municipal, apresentam-se como tangíveis dentro de um prazo de 03 (três) anos, a contar a partir de janeiro de 2018. Porém, a volatilidade do segmento de tecnologia da informação exige manutenção constante do plano, haja vista a possibilidade de mudanças de tendências.

Tabela 2 - Objetivos Estratégicos

Item	Objetivo
01	Melhorar as condições de trabalho da equipe de tecnologia da informação com os novos equipamentos.
02	Assegurar ganho de desempenho na conectividade entre unidades remotas/secretarias e internamente na rede local.
03	Reformulação do Data Center, com reestruturação física da sala e modernização de equipamentos de tecnologia da informação.
04	Consolidar a infraestrutura de servidores com novas aquisições, readequações e upgrades estruturais.
05	Promover a segurança lógica da rede através de segmentações físicas, lógicas, controle de acesso à rede lógica e soluções de armazenamento seguro.
06	Promover segurança por meio de políticas, planos, documentações e reorganização formal das rotinas de trabalho da unidade de tecnologia da informação.
07	Aprimorar processos e sistemas de atendimento a usuários de tecnologia da informação por meio de sistemas de Service Desk e acesso físico.
08	Implantar novos sistemas corporativos para automatizar rotinas de trabalho e reduzir custos operacionais.
09	Flexibilizar o acesso à rede local de forma segura e com mobilidade através de Implantação de pontos de acesso via rádio frequência.
10	Promover a inclusão digital e social por meio de programas municipais de implantação de tele centros e “Internet para Todos”.

CAPÍTULO II – DIAGNÓSTICO DE TECNOLOGIA DA INFORMAÇÃO

1. INTRODUÇÃO

Identificar os principais pontos fracos de uma organização é uma tarefa essencial para a melhoria contínua dos ganhos de produtividade e, na maioria dos casos, até mesmo na sobrevivência de empresas.

O Diagnóstico de Tecnologia da Informação endereça esta demanda de autoconhecimento, provendo meios para a tomada futura de decisões que mitiguem os riscos e reduzam os custos relacionados aos eventuais incidentes de Tecnologia da Informação (TI).

Outros importantes fatores motivadores para esta análise são as diversas modificações, expansões e atualizações sofridas nos últimos anos pelo ambiente de tecnologia da informação, que acabaram por inserir novas e sérias questões relacionadas ao crescimento.

Este projeto permitiu uma avaliação do quesito tecnologia da informação para um conjunto pré-definido de ativos de tecnologia da informação da Prefeitura, observando a aderência destes quanto às melhores práticas de mercado e de fabricantes, além das normas de tecnologia da informação.

As informações que alimentam este diagnóstico foram obtidas por meio de entrevistas com agentes públicos da Prefeitura e por inspeções físicas onde se fazia necessário e possível. Porém, devido à falha no controle do inventário dos recursos de tecnologia da informação, os dados apresentados a partir desse momento podem apresentar pequenas variações para mais ou para menos.

2. VISÃO GERAL

O ambiente de tecnologia da informação da gestão municipal da Prefeitura do município de Tijucas do Sul, no Estado do Paraná, é composto dos seguintes ativos:

Tabela 3 - Descrição de Ativos

Ativos	Quantidade
Servidores Físicos	**02**
Servidores Virtuais	**08**
Switches (não gerenciados)	**66**
Wireless Access Points	**100**
Roteadores	**60**
Estações de Trabalho	**550**
Impressoras e Print Servers	**100**
Nobreaks	**78**
Circuitos de Comunicação Dedicados	**01**
Circuitos de Comunicação Internet	**01**
Geradores Elétricos	**02**
Usuários	**600**

As próximas seções deste documento apresentam as disposições físicas e lógicas do ambiente de tecnologia da informação da Prefeitura de Tijucas do Sul, assim como a identificação de deficiências, necessidades de adaptações e reformulações consideradas de grau médio e alto para um ambiente tão dependente de tecnologia da informação.

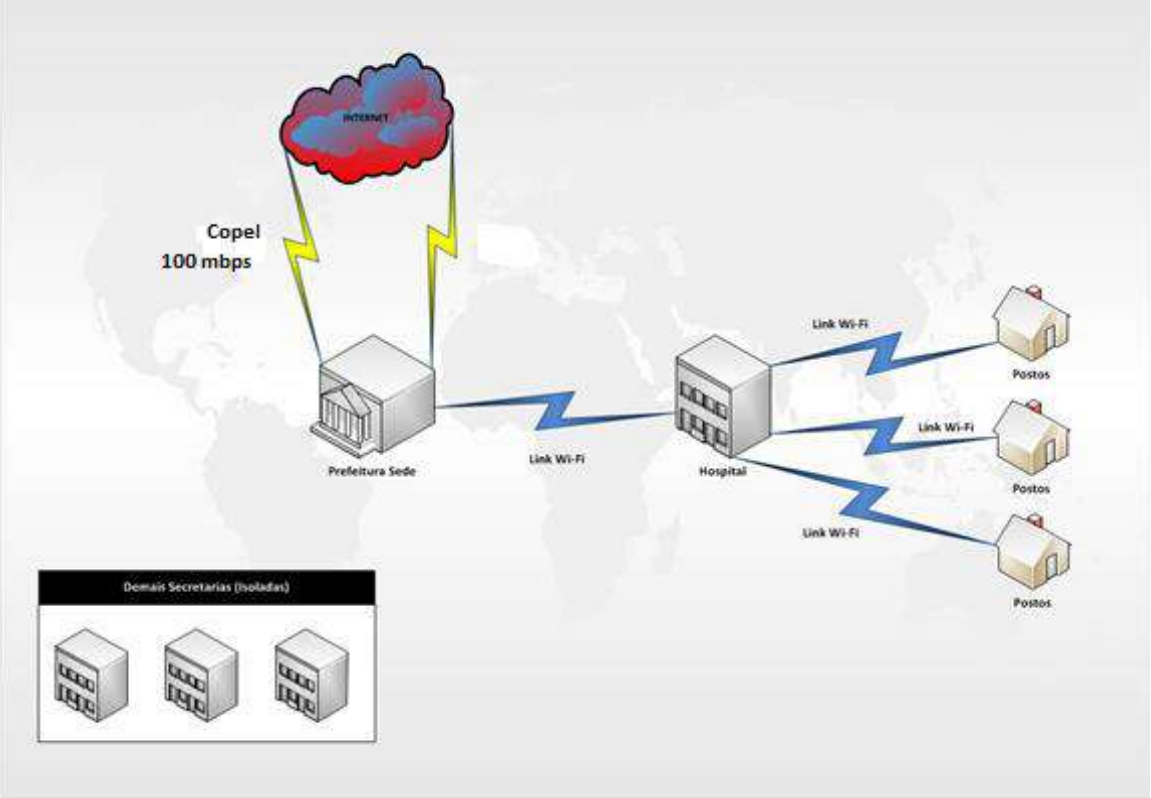


Figura 1 - Topologia WAN

3. INFRAESTRUTURA

3.1. Infraestrutura Física

A Gestão Pública Municipal de Tijucas do Sul, no Estado do Paraná, possui uma estrutura predial conectada por cabos UTP categoria 5 e 5e. Tal estrutura de cabeamento encontra-se exposta em alguns locais, ficando sujeita às condições extremas de temperatura, umidade, roedores, pássaros, chuvas e outras variáveis capazes de degradar ou até mesmo interromper a continuidade da comunicação de forma intencional ou acidental. Todo esse cabeamento converge para o CPD, atual local de trabalho da equipe de tecnologia da informação.

O cabeamento nas dependências da prefeitura encontra-se disposto em canaletas ou exposto ao acesso físico irrestrito. A atual condição permite com que ocorra eventuais sabotagens da comunicação, como por exemplo, por meio do rompimentos dos cabos.

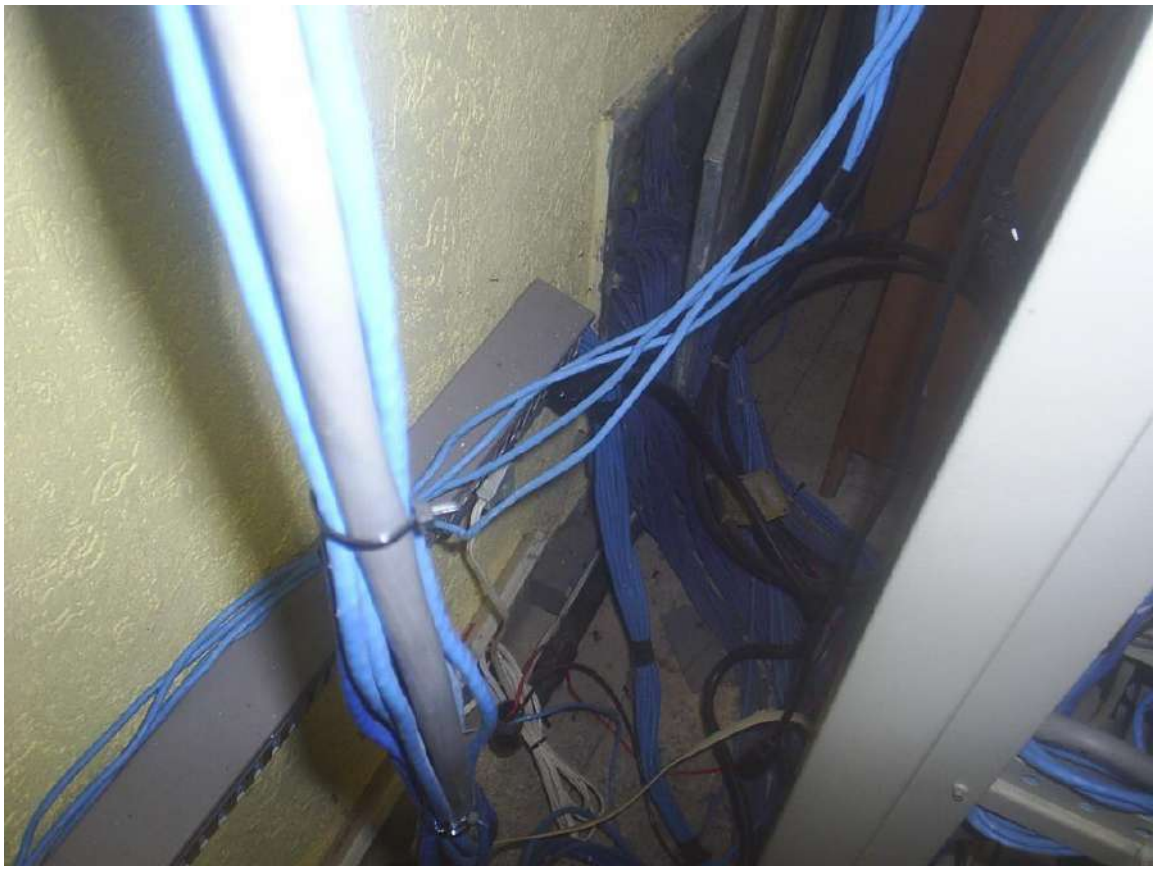


Figura 2 - Cabeamento Interno

Algumas edificações, tais como secretarias, não estão integradas à rede da Prefeitura, portanto a administração do ambiente de tecnologia da informação encontra-se descentralizada, o que dificulta bastante a administração dos ativos existentes nestes locais. No entanto, o hospital é interligado via link de rádio frequência não proprietária, assim como os postos e unidades de saúde.

Não há uma estrutura mínima adequada para acomodação de equipamentos tais como roteadores, switches e servidores. O local onde os ativos de tecnologia da informação estão dispostos carece de armários (racks) adequados, mostrados nas figuras de 3 a 11 e servidores com arquitetura adequada e controle de intempéries – temperatura, umidade e fogo.

Figura 3 - Acomodação de Servidores

Figura 4 - Acomodação de Servidores

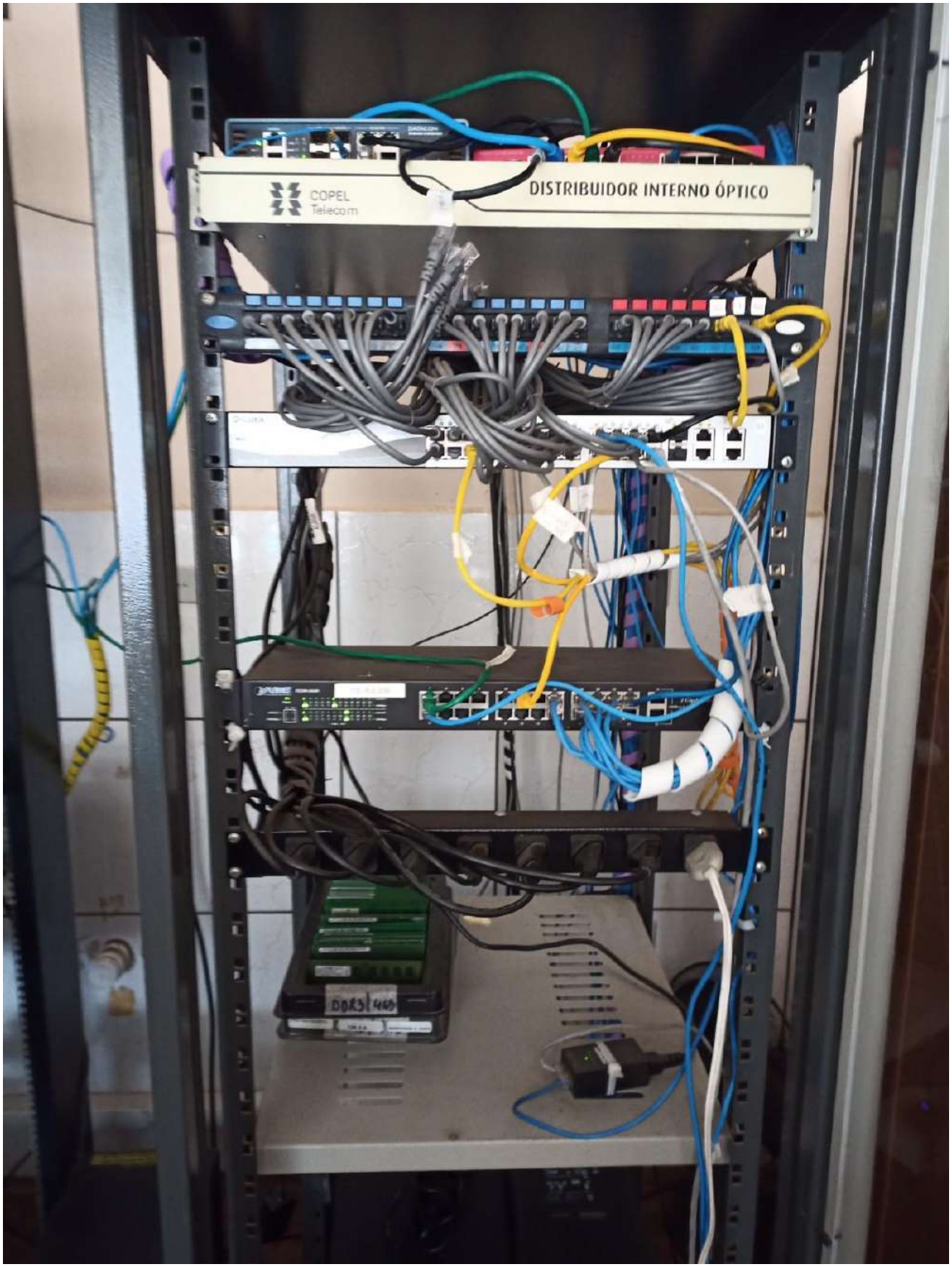


Figura 5 - Switches, Roteadores e Firewall

Figura 6 - Switches, Roteadores e Firewall

Figura 7 - Nobreak

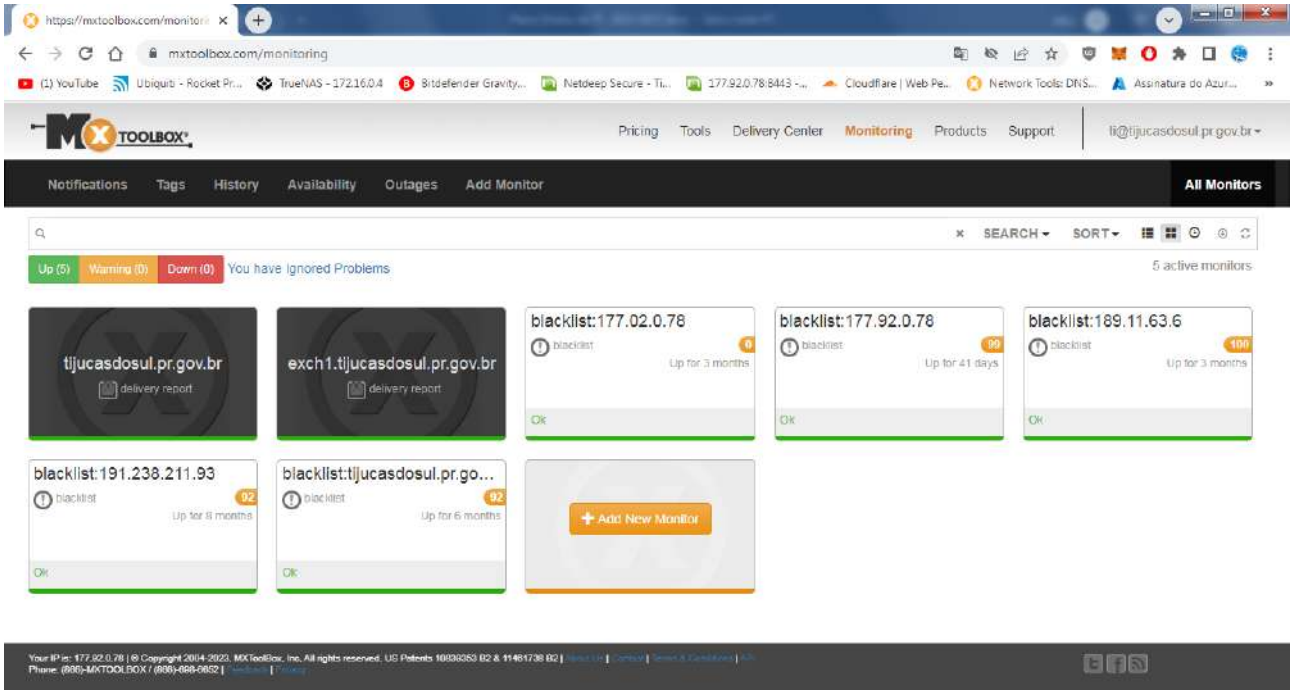


Figura 8 – Sistema de Monitoramento Blaklist

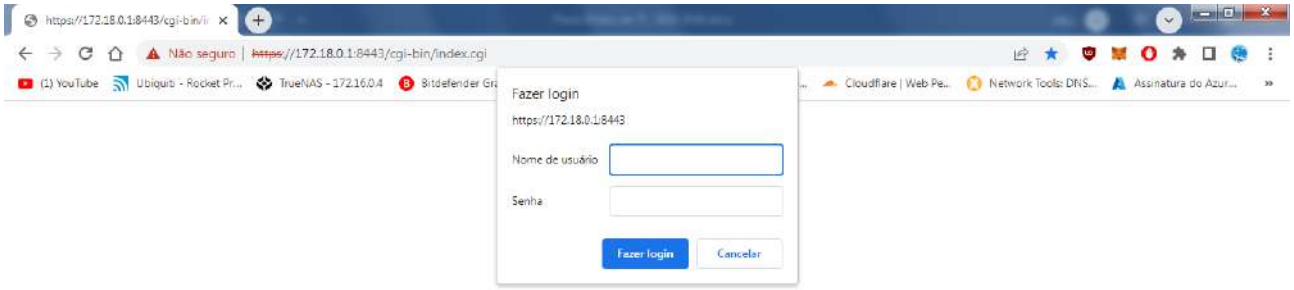


Figura 9 – Firewall (Software)

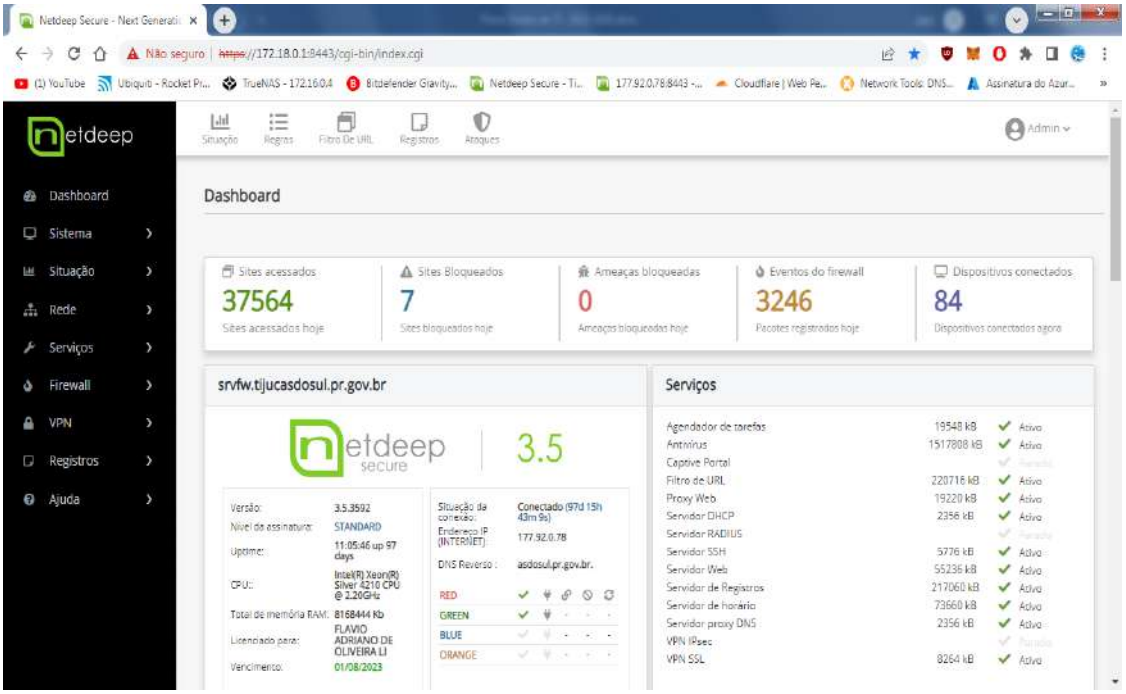


Figura 10 – Firewall (Software)

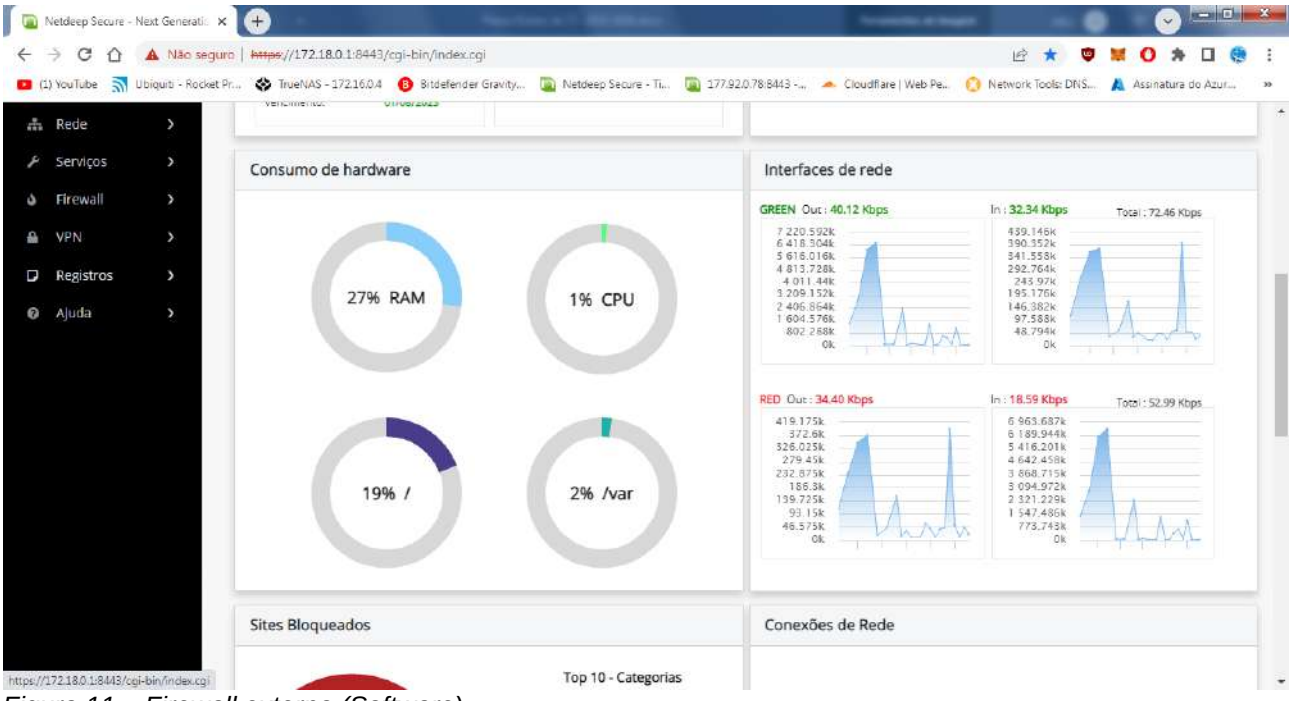


Figura 11 – Firewall externo (Software)

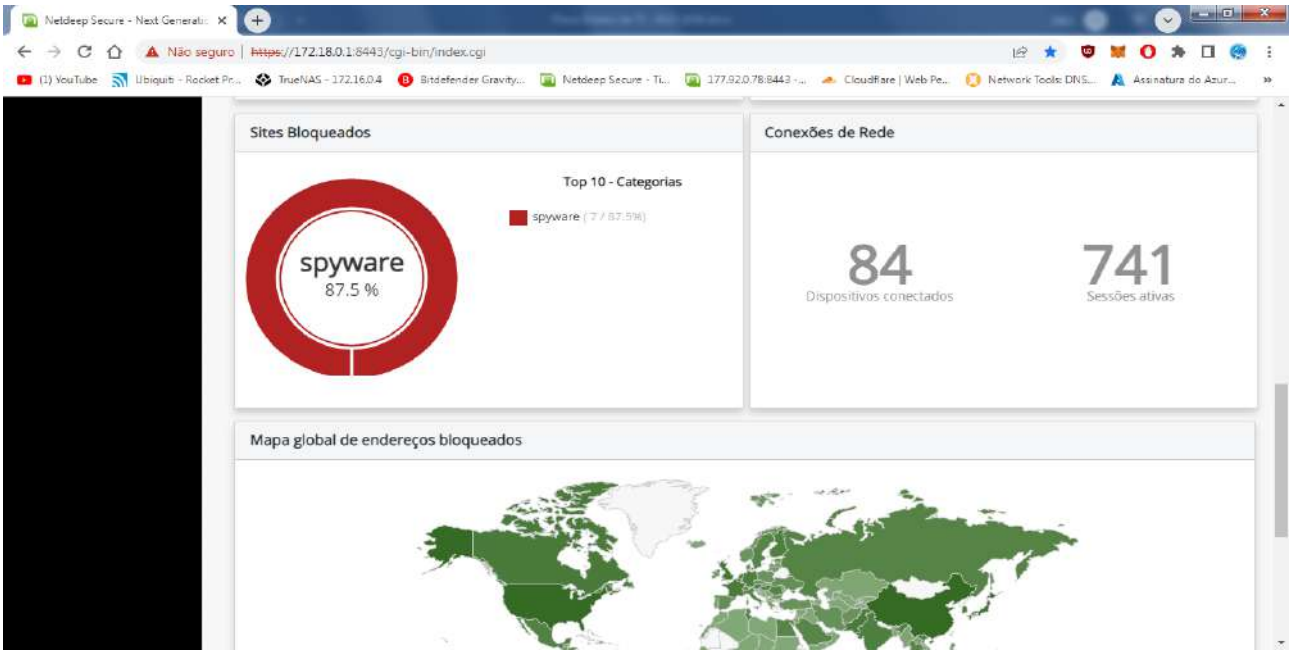


Figura 12 – Firewall externo (Software)

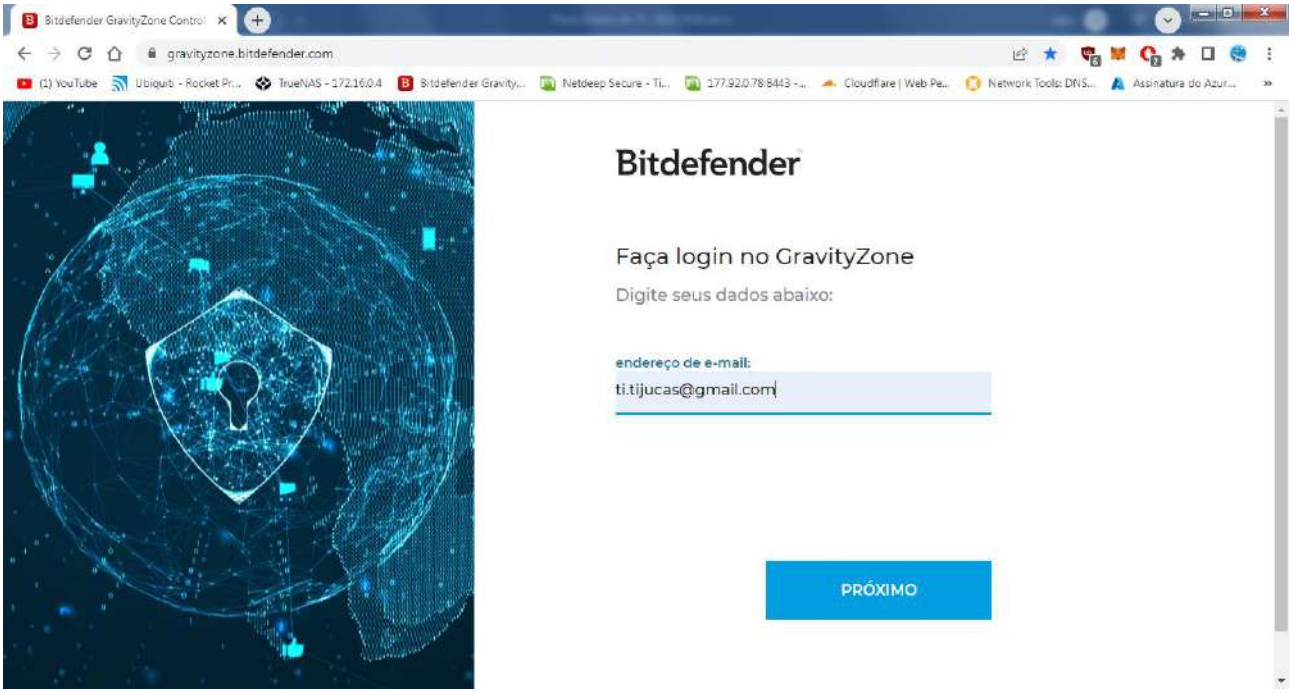


Figura 13 – Antivírus (Software)

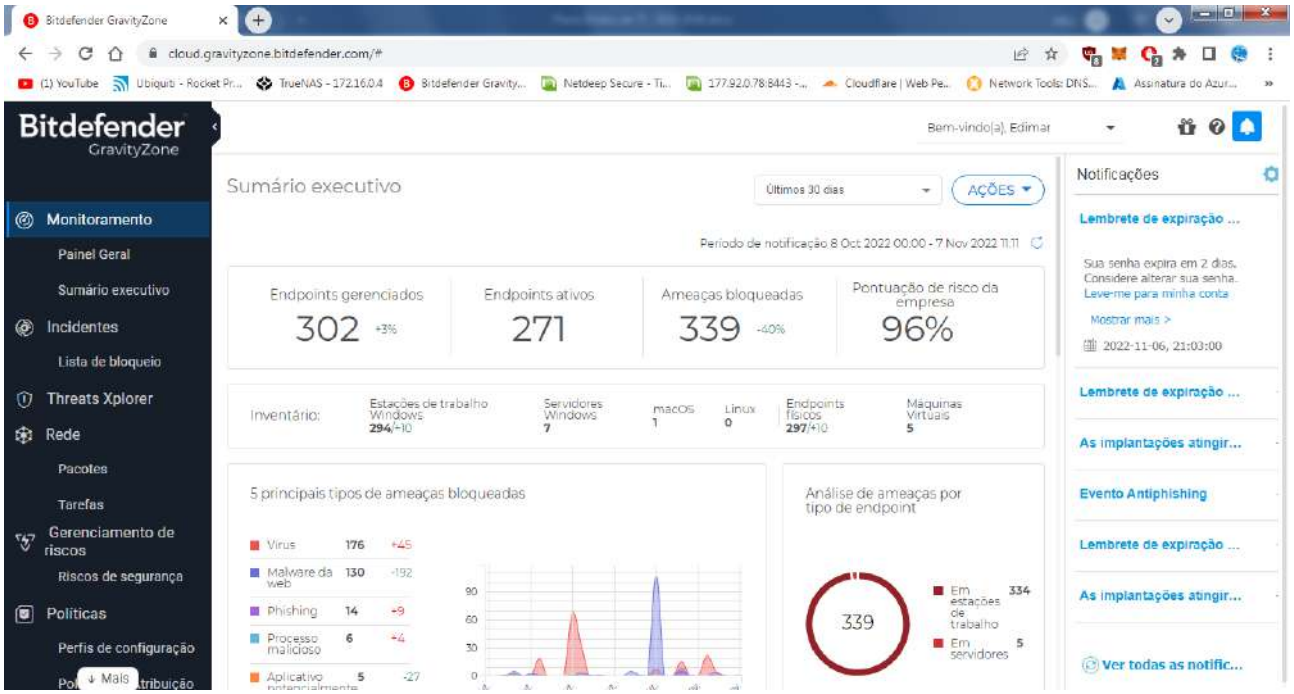


Figura 14 Antivírus (Software)

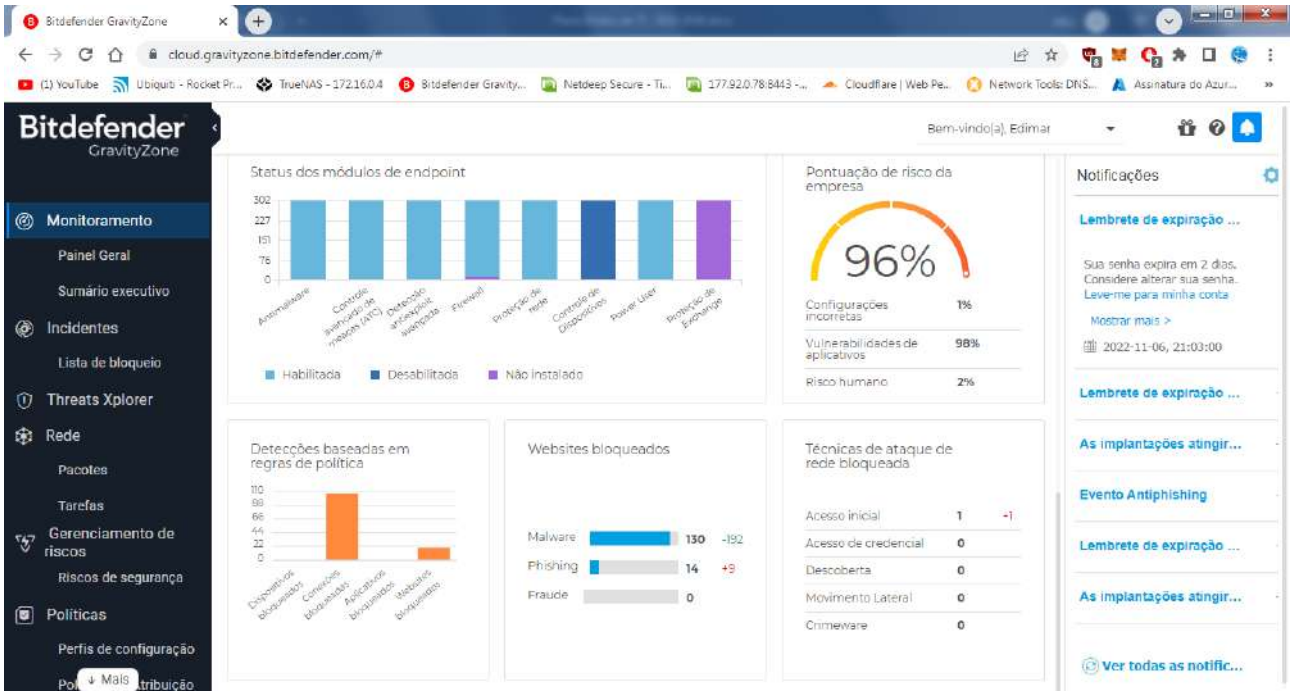


Figura 15 Antivírus (Software)

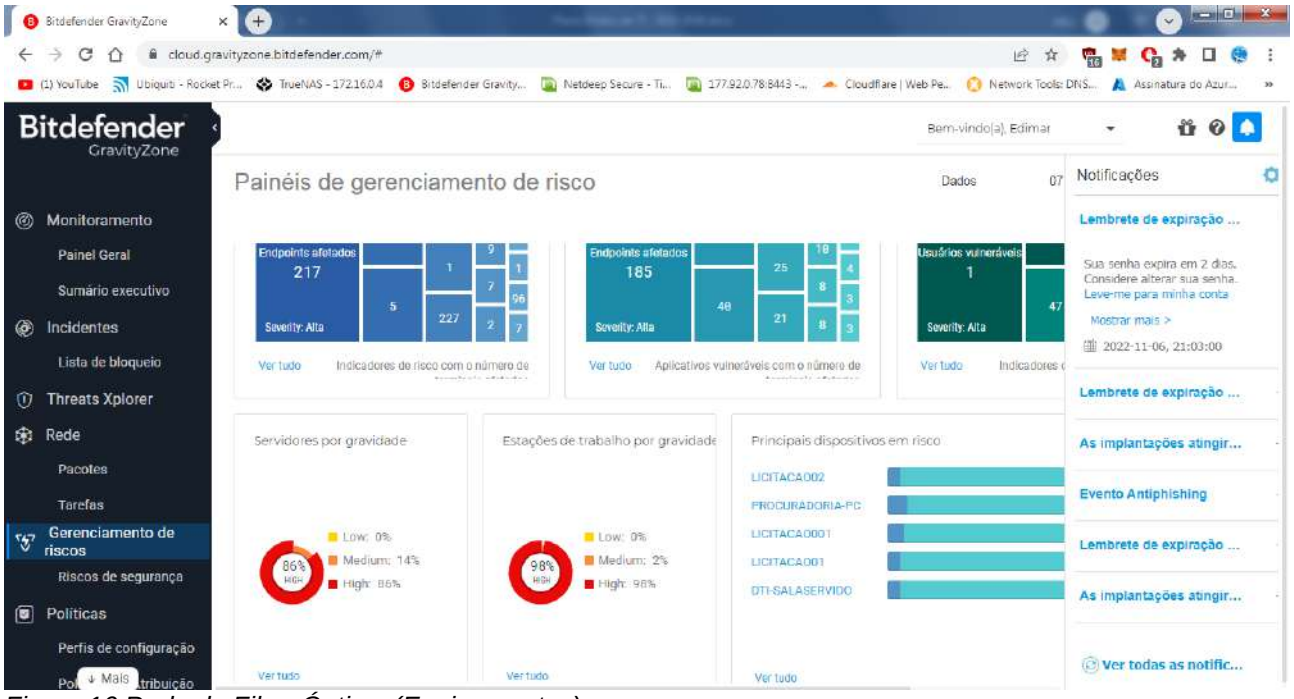


Figura 16 Rede de Fibra Óptica (Equipamentos)

Figura 17 Rede de Fibra Óptica (Rede)

Figura 18 Fibra Óptica (Projeto)

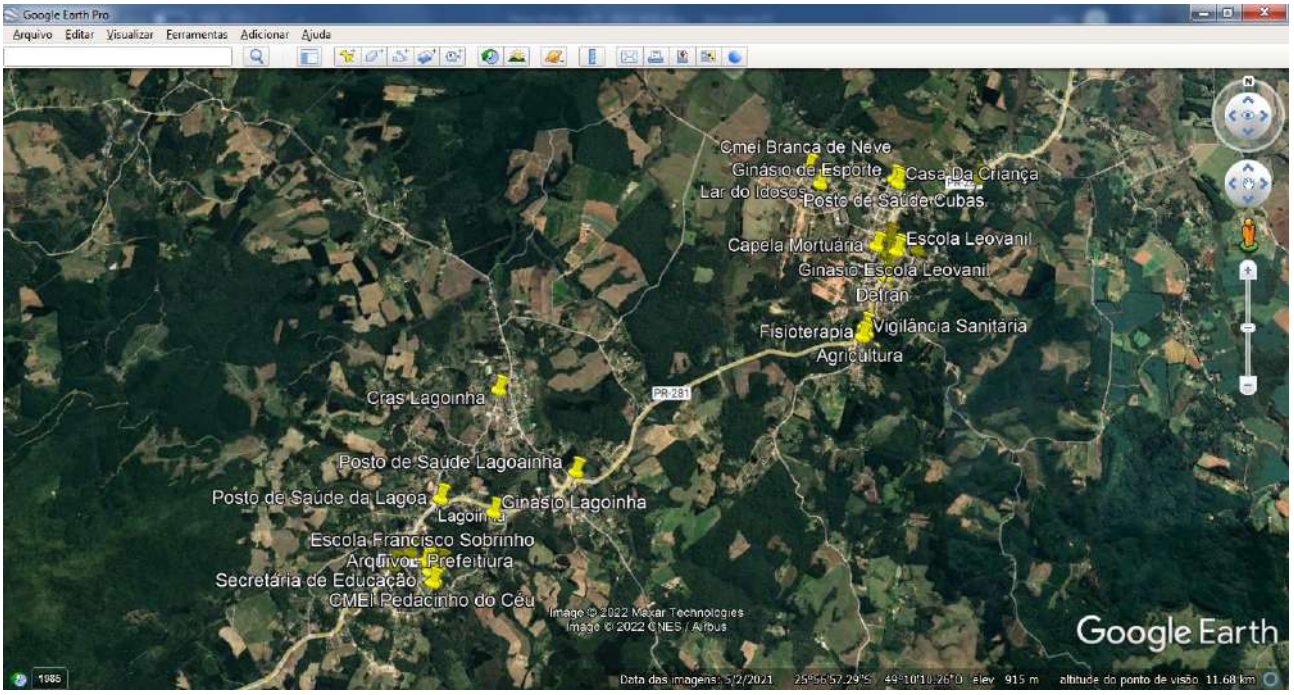


Figura 19 Rede de Fibra Óptica (Projeto)

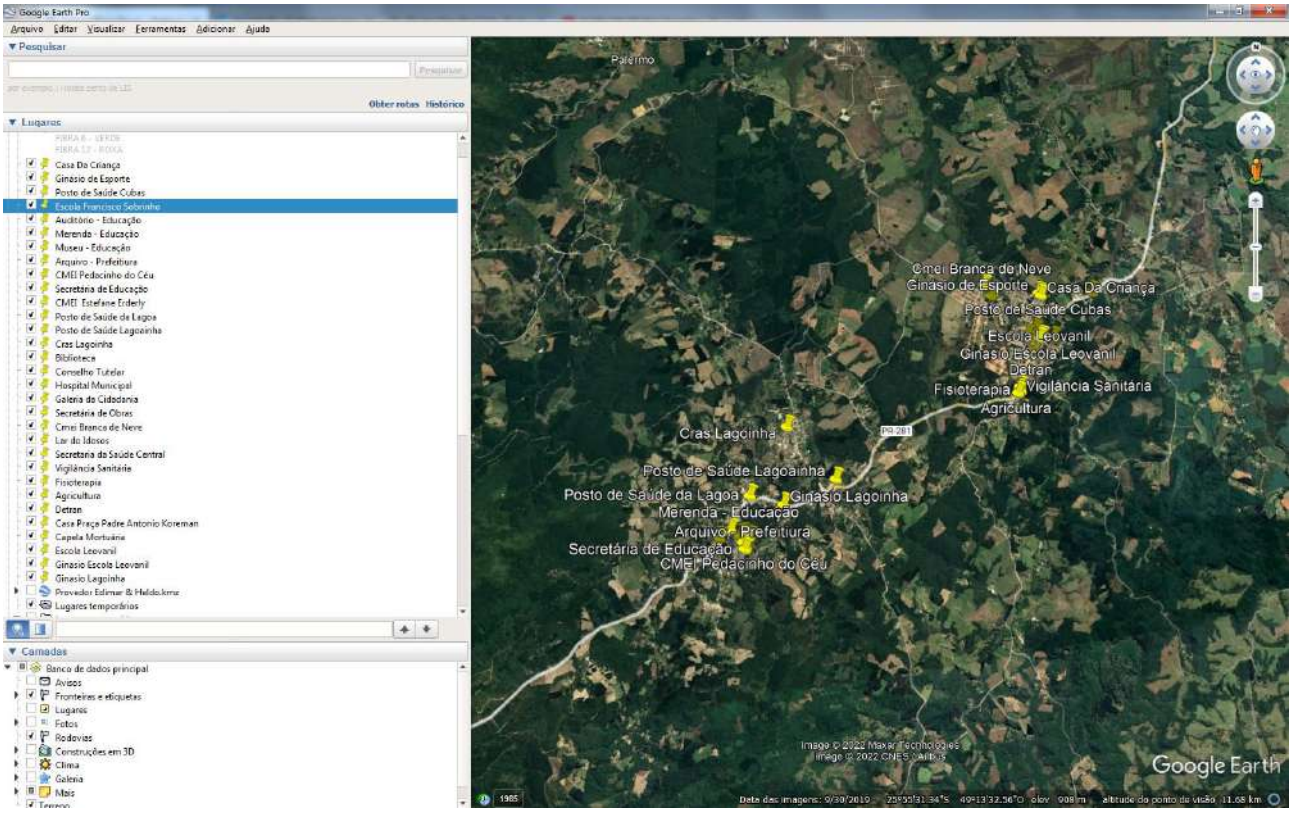


Figura 20 Rede de Fibra Óptica (Projeto)

Apesar de o ambiente computacional dos servidores possuir um sistema de estabilidade/alimentação elétrica (nobreak), refrigeração e proteção contra incêndios, não se encontra em conformidade com as melhores práticas de acomodação, conforme exibido nas imagens a seguir:

Figura 21 - Proteção Contra Incêndio

Figura 22 - Proteção Elétrica (Nobreaks)

Logo abaixo, são apresentadas as imagens da Sala de Tecnologia da Informação da Prefeitura de Tijucas do Sul:

Figura 23– Acomodações Internas

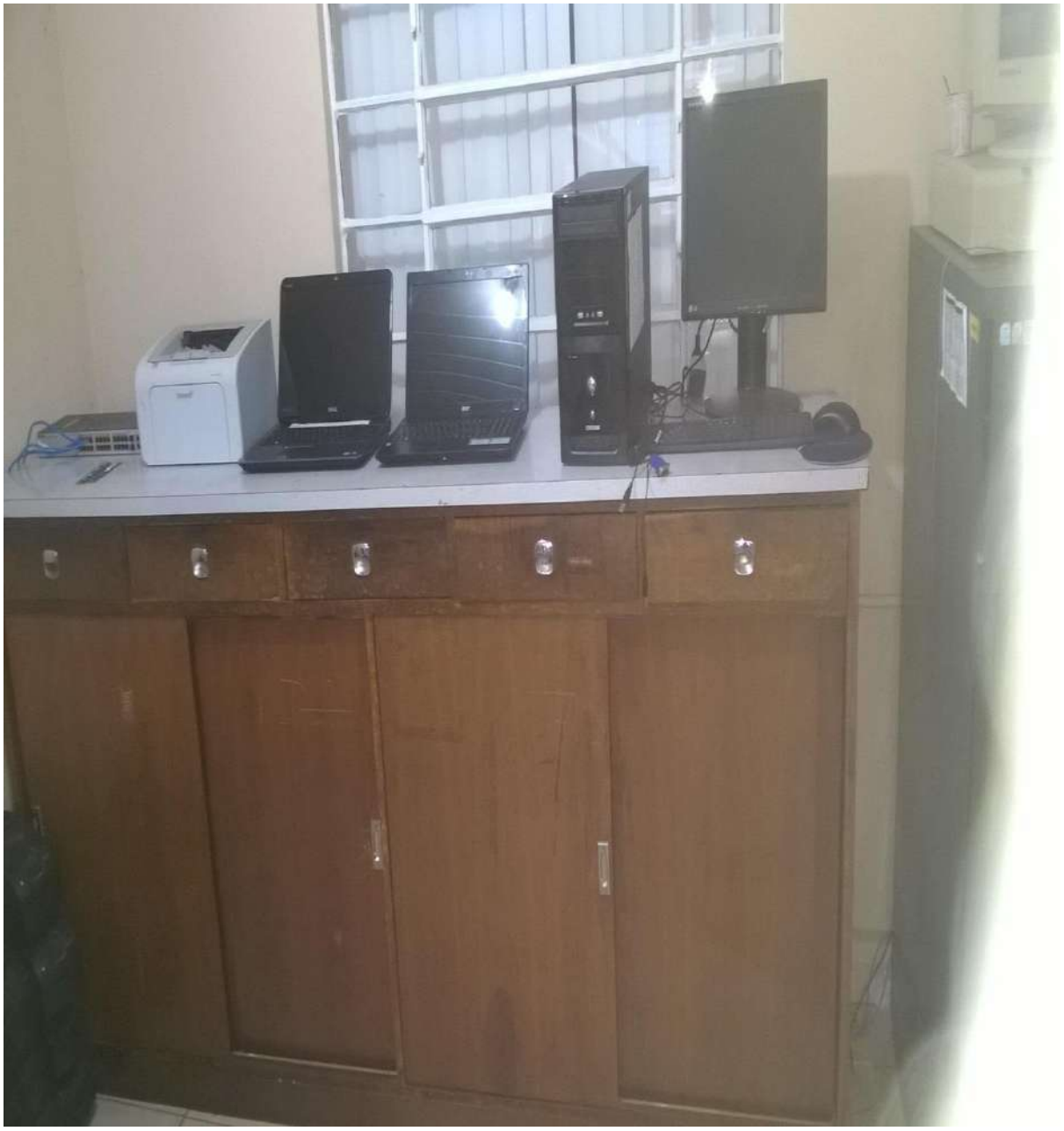


Figura 24 – Acomodações Internas

Figura 25 – Acomodações Internas

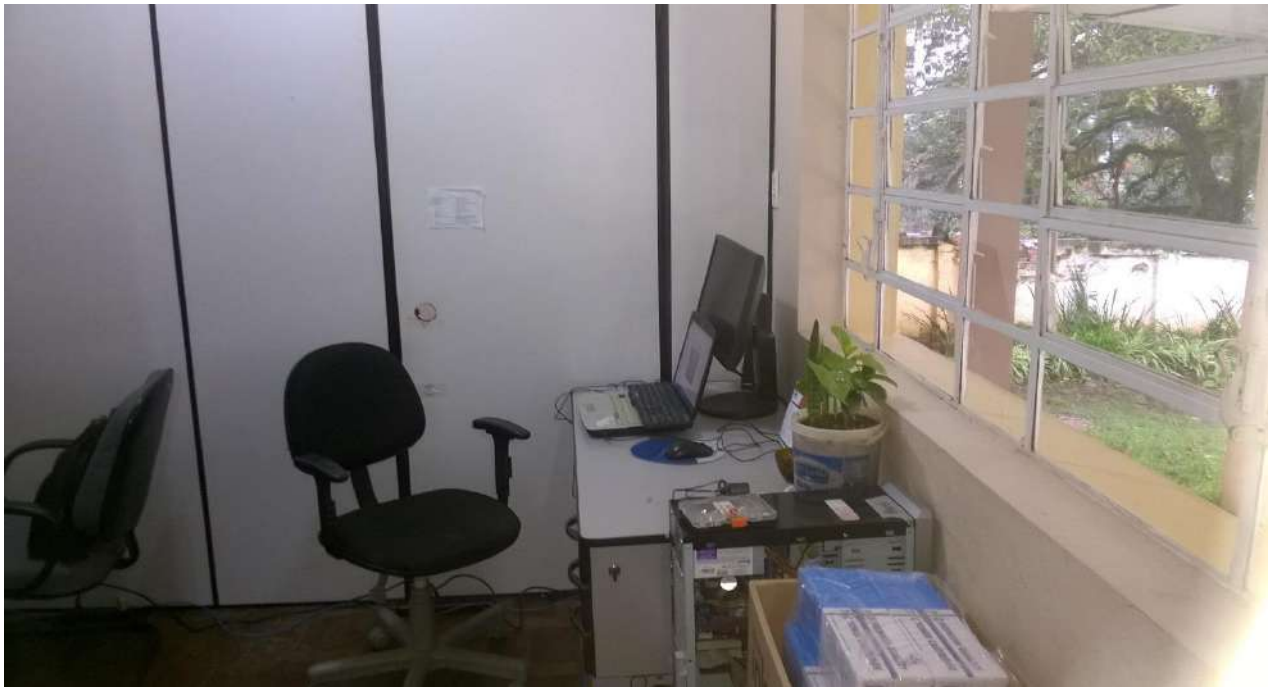


Figura 26 – Acomodações Internas

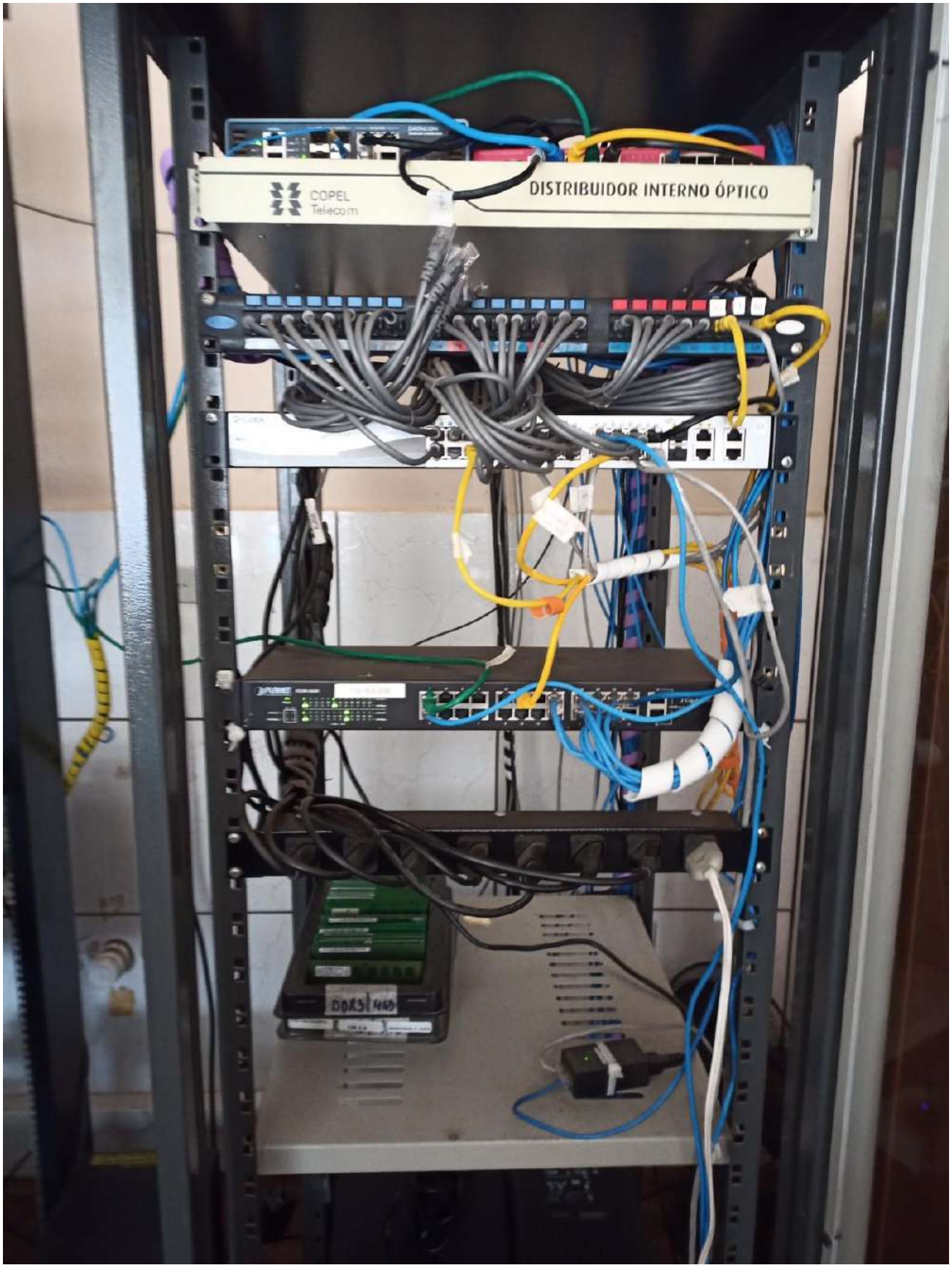


Figura 27 – Acomodações Internas

Figura 28 – Acomodações Internas

Figura 29 – Acomodações Internas

Figura 30 – Acomodações Internas

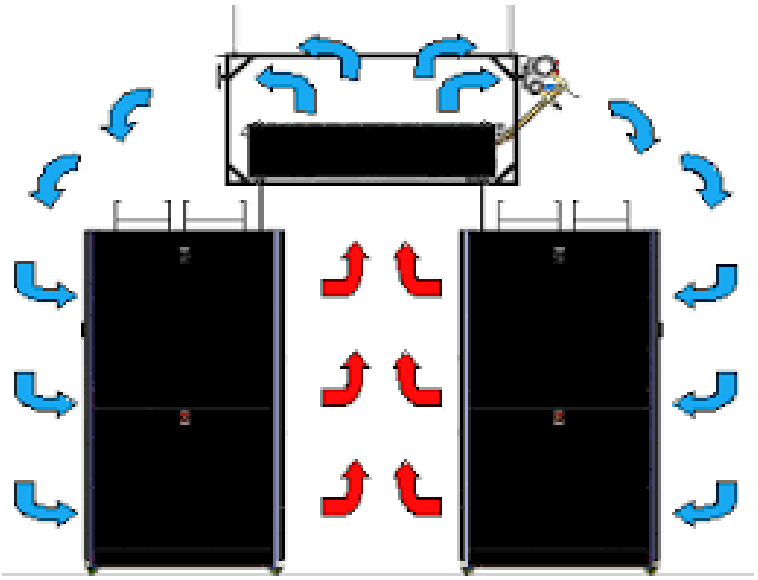


Figura 31 - Refrigeração DataCenter

3.2. Infraestrutura Telecom

Dentro do cenário encontrado na infraestrutura lógica da rede da Prefeitura de Tijucas do Sul, alguns itens precisam ser evidenciados, pois se caracterizam como falhas ou oportunidades de melhoria para a estrutura de tecnologia da informação.

As edificações da gestão municipal interconectadas utilizam-se do mesmo segmento de rede camada 2, ou seja, não existe uma segmentação do tráfego, o que ocasiona um único domínio de broadcast. Sendo que o provimento da Internet na sede é realizado através de um link WAN fornecido por:

- Ligga l Telecom - 200 (Duzentos) Mbps;

Figura 32 – Torre São Paulo 5

Estas figuras foram utilizadas para afirmar a contratação do aluguel das torres perante a São Paulo 5. As figuras 21 e 22 foram utilizadas para acertar o contrato de locação

para a utilização da mesma. Nesta mesma torre, está fixado um equipamento (central) ROCKET (GEN2 figura 23). Já a figura 24, serve para ilustrar o modo como essa central é acessada e configurada por usuário administrator restrito, se utilizando de um login com nome e senha. A figura 25 representa a antena existente em cada setor, como por exemplo: no Detran, no Hospital e no Posto de Saúde Central, havendo uma antena própria em cada uma dessas unidades para recebimento do sinal diretamente da Torre São Paulo 5. Por sua vez, as figuras 26, 27 e 28 são referentes às conexões existentes com cada um dos setores. Por fim, a figura 29 serve para ilustrar o medidor de velocidade, sendo que atualmente, o plano da Copel é de 100MB.

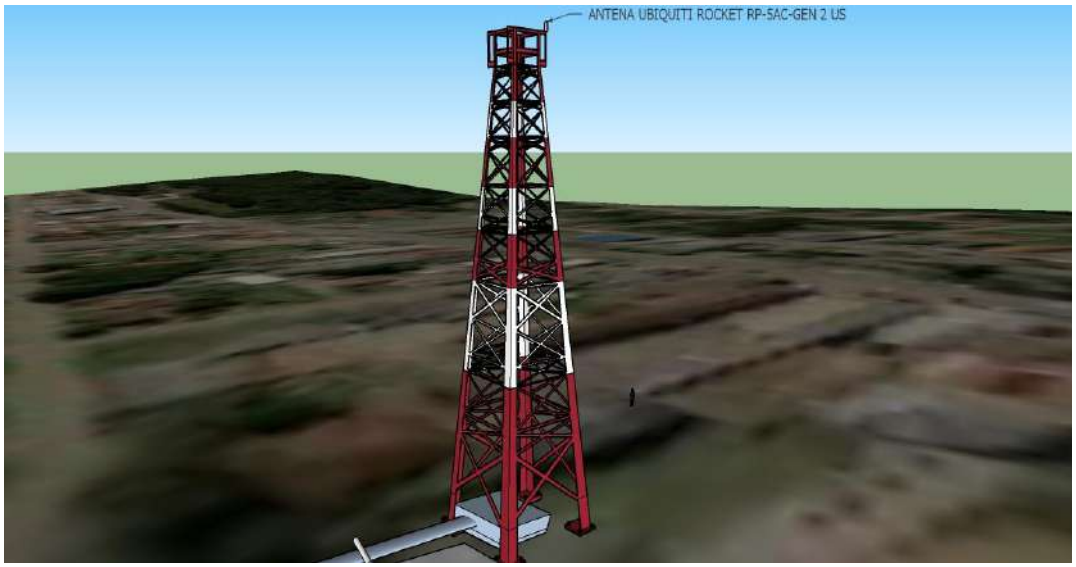


Figura 33 - Aluguel da torre

Figura 34 -Aluguel da torre

Figura 35 – Central da internet para a distribuição

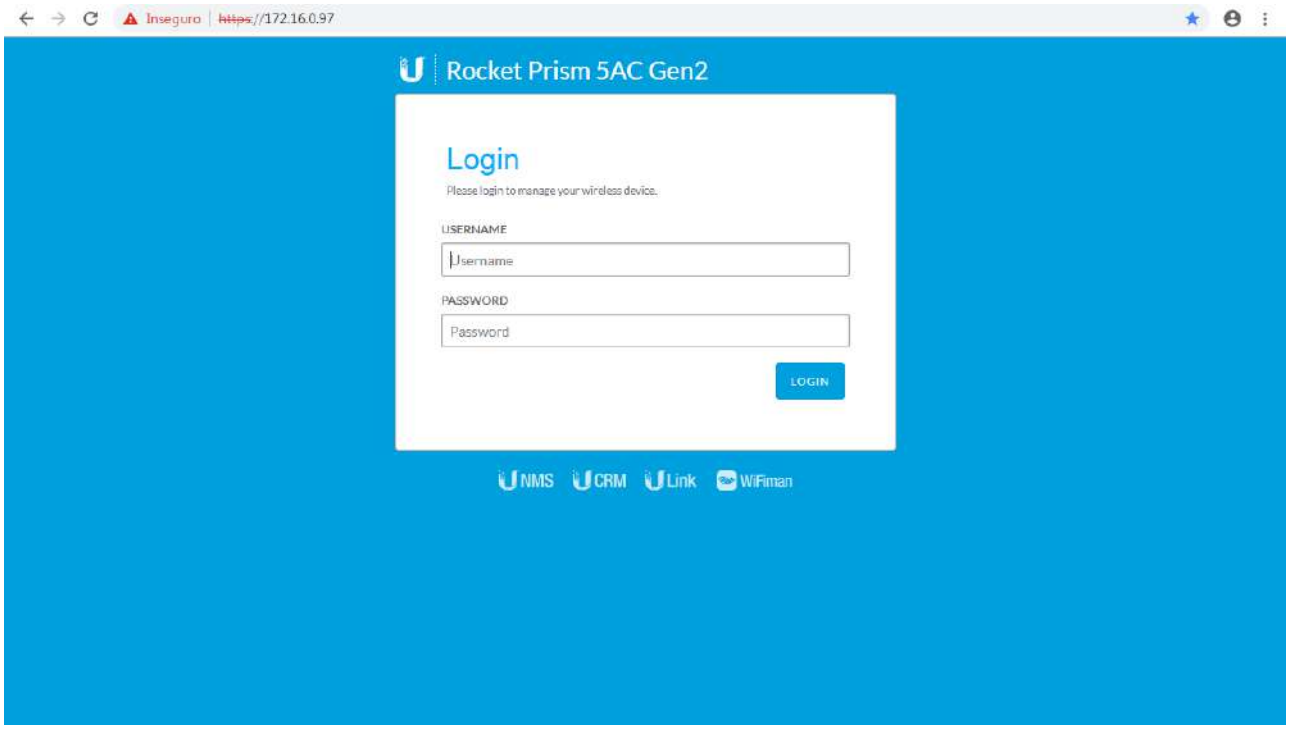


Figura 36 - Tela login

Figura 37- Antena G2

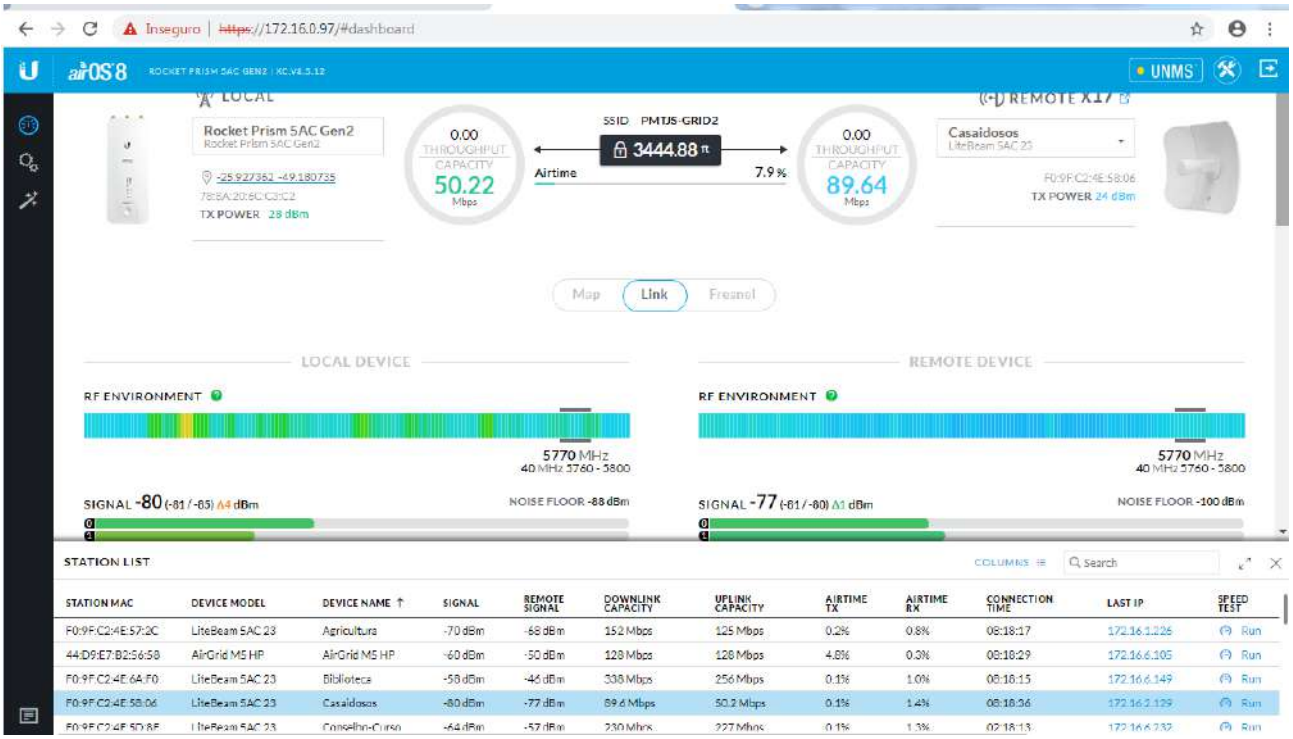


Figura 38 – Conexão com os órgãos públicos

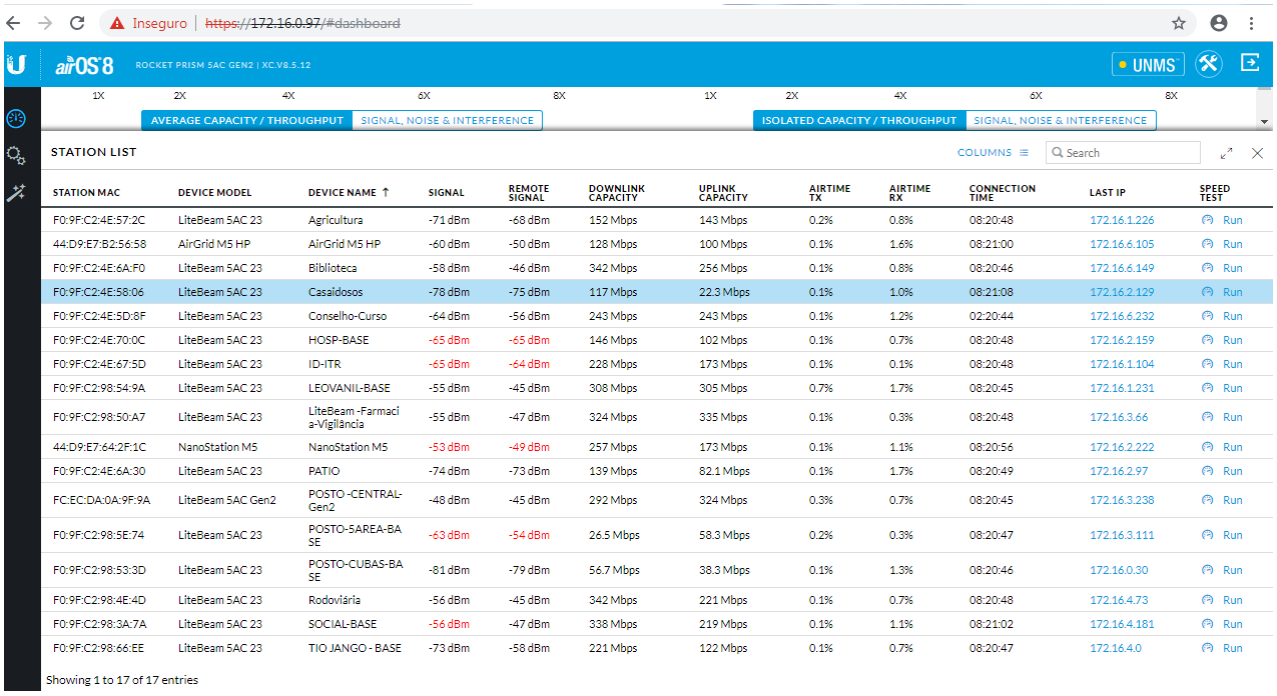


Figura 39-– Tela de todas as conexões G2 do município

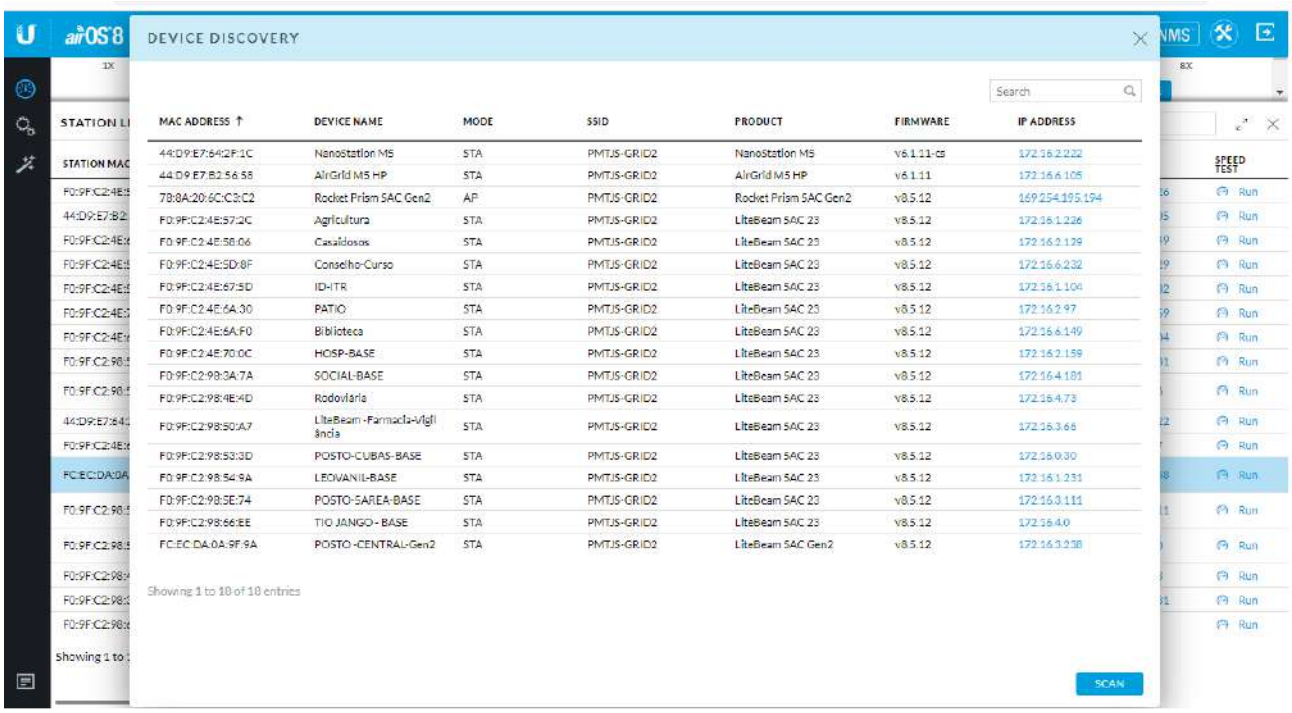


Figura 40 - Tela de todas as conexões G2 do município

Figura 41 – Teste de velocidade

Todas as unidades centrais Administração/Secretarias (Industria e Comércio, Saúde, Agricultura, Obras e Rodoferroviária) e mais o Hospital Municipal, Detran, Biblioteca e Escolas são interligadas à rede própria. Nas localidades interiores é necessário que os serviços sejam realizados por terceiros, quando necessário, possuindo a conectividade de

internet e utilizando plataforma ubiquiti.

A segunda fase do projeto Telecom, com a aquisição de recursos necessários, será interligar todas as unidades da Prefeitura em uma mesma rede. Por fim, observa-se na Prefeitura Municipal a ausência de elementos e soluções consideradas pré-requisitos para uma estrutura de tecnologia da informação, sendo elas:

- Sistema de Inventário e Distribuição de Aplicações; Pendente;
- Solução de Segurança de Perímetro Internet (UTM Firewall) - Ativo;
- Solução de Virtualização de Servidores, Estações e Aplicações - Ativo;
- Estrutura de Arquivos Distribuídos - Ativo;
- Estrutura de Arquivos Distribuídos - Ativo;
- Sistema de Correio Eletrônico Corporativo - Ativo;
- Solução de Cópias de Segurança (*Backup*) Corporativo - Ativo;
- Soluções de Proteção de Endpoint Corporativo - Ativo;
- Solução de Armazenamento de Dados (Storage) - Ativo;
- Sistema de Controle de Impressão - Pendente;
- Sistema de Geração Própria de Energia Elétrica Sustentável - Pendente;
- Sistema de Gerenciamneto de Nobreak Energia Elétrica – Ativo;
- Sistemas de Missão Crítica com Redundância/Contingência - Pendente;
- Sistema de ERP Proprietário – Pendente;
- Sistema de Workflow Proprietário – Pendente;
- Outros.
- Banco de Dados e BI, próprio – Pendente;

Figura 42 – Banco de dados

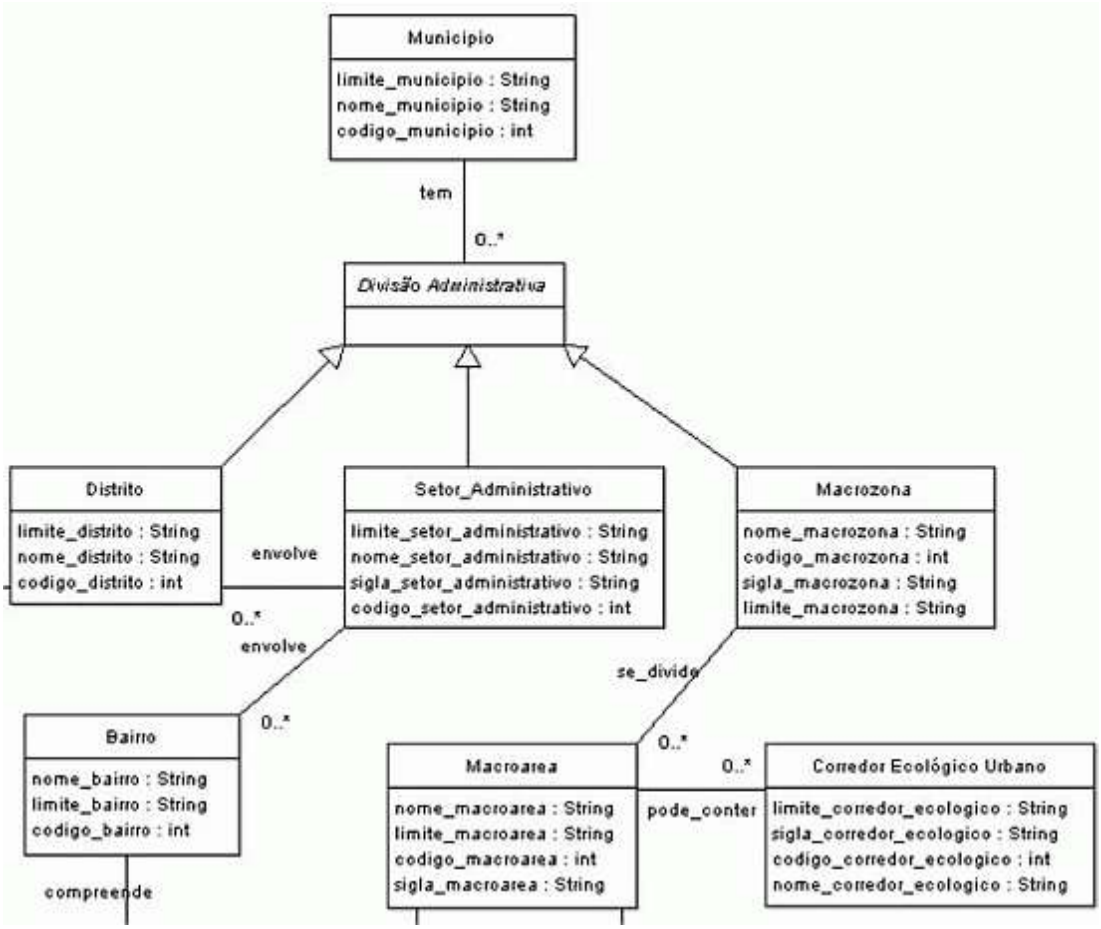


Figura 43 – Diagrama ER possível software residente da prefeitura

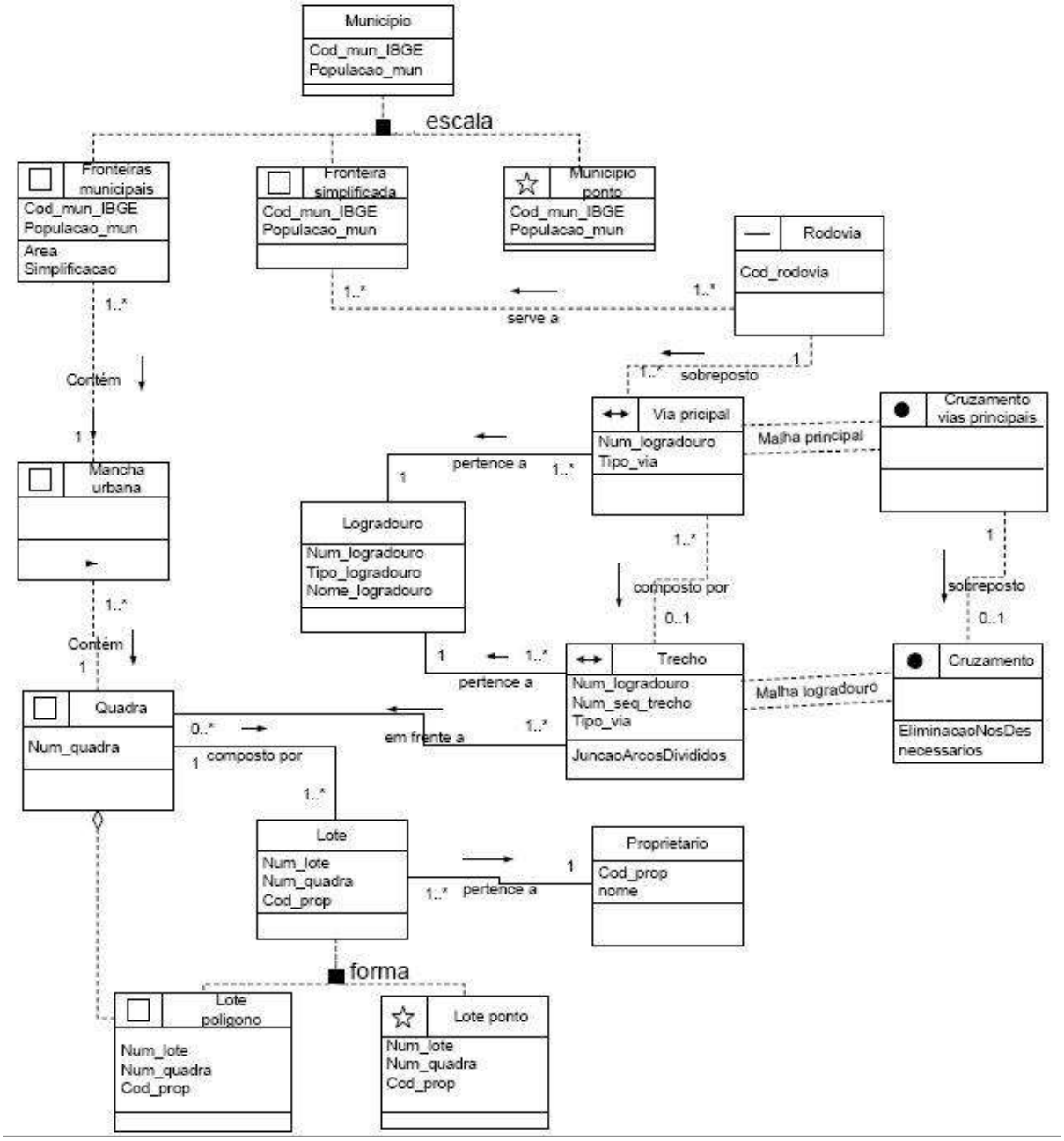


Figura 44 - Diagrama ER possível software residente da prefeitura

Existe uma necessidade urgente de integrar os Banco de Dados da Prefeitura Municipal, bem como da Câmara de Vereadores e do Instituto de Previdência de Tijucas do Sul; sendo que com essa unificação, a agilidade e economia para o município seriam enormes. Também com isso, haveria o desenvolvimento de um sistema próprio e unificado, dessa forma, obtendo uma redução de custo. Sendo que o ponto principal consiste, que com isso, com a adoção de tais medidas, o próprio Município seria proprietário de seu

software, deixando de ser refém de empresas terceirizadas, agregando com isso, mais agilidade e autonomia nas decisões tomadas por seus próprios gestores.

4. SISTEMAS

O sistema de gestão municipal utilizado pela Prefeitura Municipal de Tijucas do Sul é contratado da empresa terceirizada Equiplano, cuja plataforma é WEB e possui os seguintes módulos implantados em servidores sem nenhuma redundância e proteção contra desastres, mostrado na figura abaixo:

Figura 45 – Sistema Equiplano

- Acompanhamento Jurídico;
- Almoxarifado;
- Arrecadação Municipal;
- Contabilidade Pública;
- Folha de Pagamento e Recursos Humanos;
- Licitações e Contratos;
- Protocolo;
- Frotas.

Figura 46 – Relógio ponto biométrico

Aqui encontra-se o modelo referente ao Sistema de Ponto Biométrico integrado ao Sistema Equiplano.

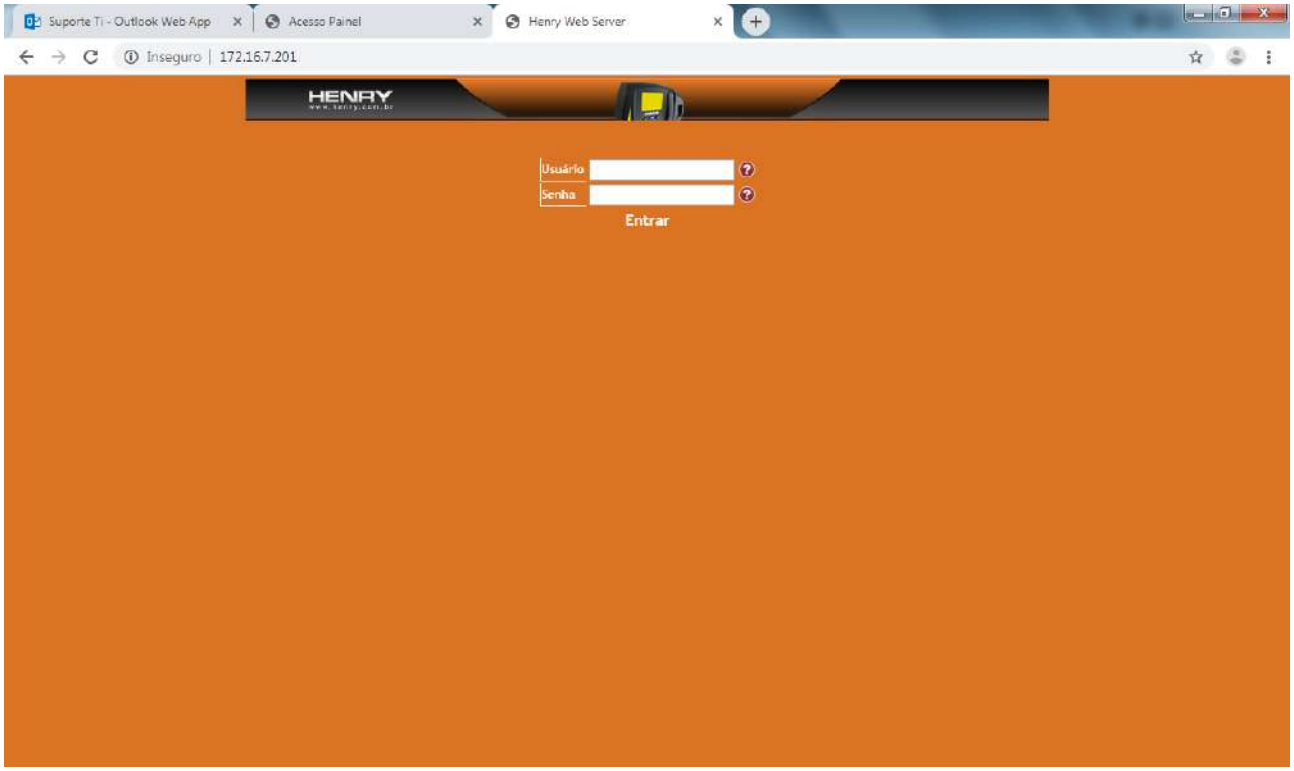


Figura 47 - Configurações do relógio ponto

Figura 48 - Configurações do relógio ponto

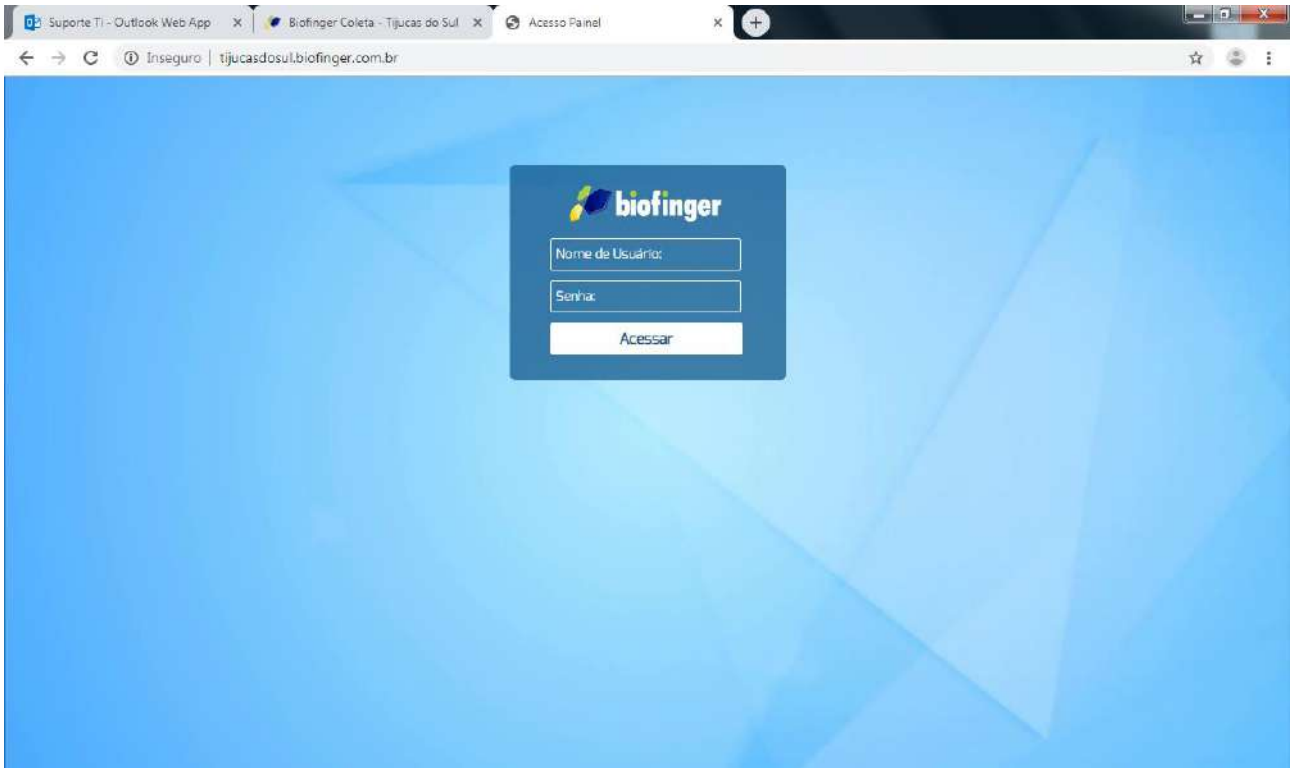


Figura 49 - Configurações do relógio ponto

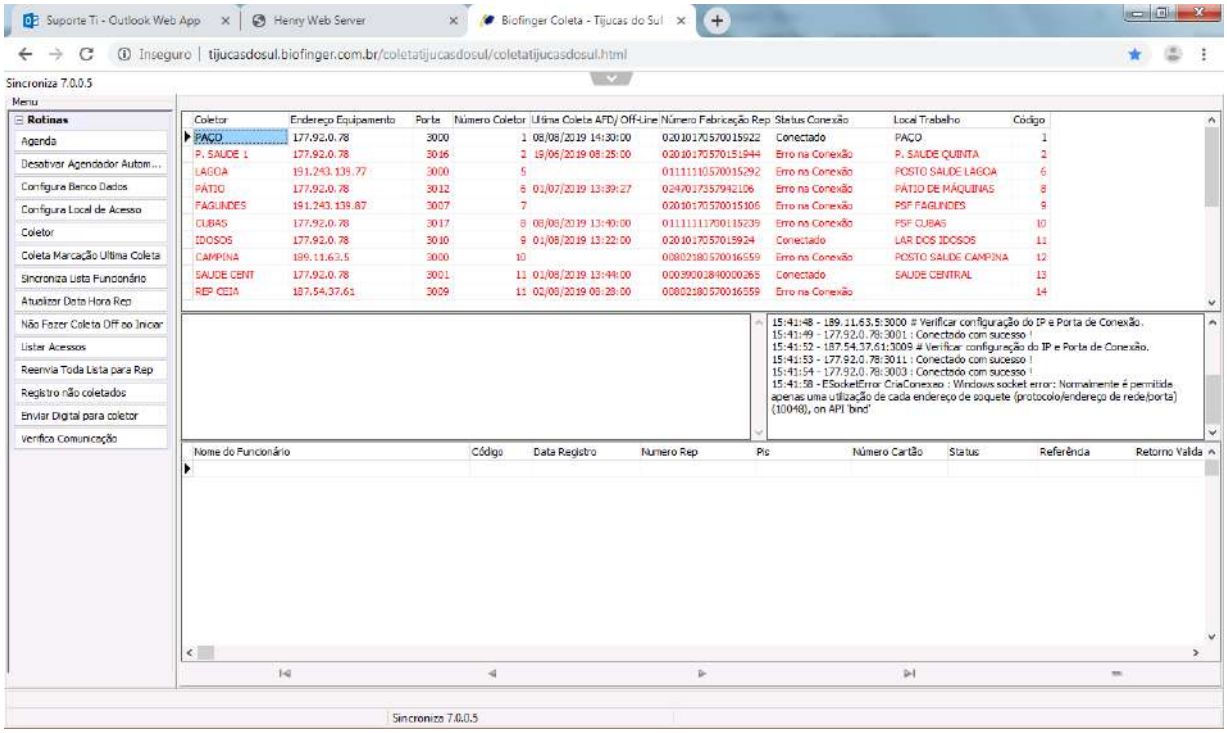


Figura 50 – Tela de Captura das biometrias

O sistema de gestão na área de obras é o SiobraWeb, sendo utilizado pelo setor de Engenharia:

Sempre que clicar em Página Inicial o SisobraPref volta para tela inicial contém todos os menus necessários para utilização do sistema.

Figura 51 - Tela inicial do Sistema SisobraWeb

https://www.gov.br/receitafederal/pt-br/assuntos/orientacao-tributaria/declaracoes-e-demonstrativos/sisobrapref-sistema-de-cadastro-de-obra-modulo-prefeitura-novo/arquivos-1/manual-sisobrapref-web-v-1-4-contribuinte-prefeitura-102020-atual.pdf

O sistema de gestão na área da saúde é o IDS:

http://tijucasdosul.ids.inf.br:8085/tijucasdosul/IDSSaude/idssaude.dl

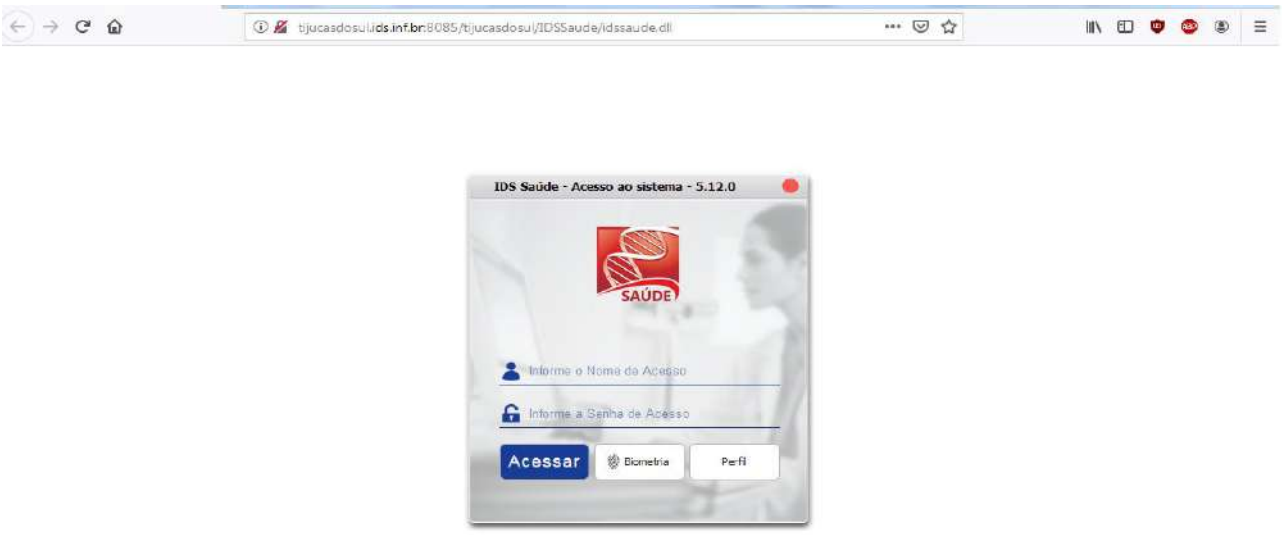


Figura 52 - Tela inicial do Sistema IDS

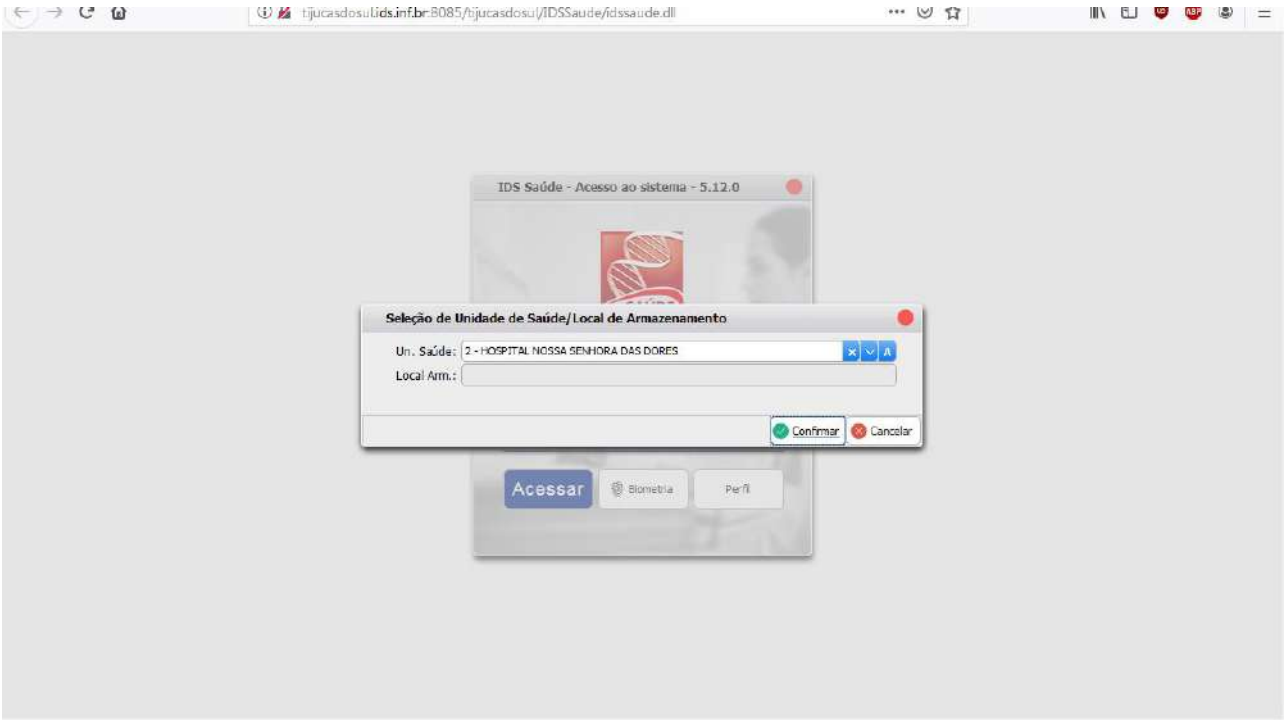


Figura 53 - Tela de login do Sistema IDS.

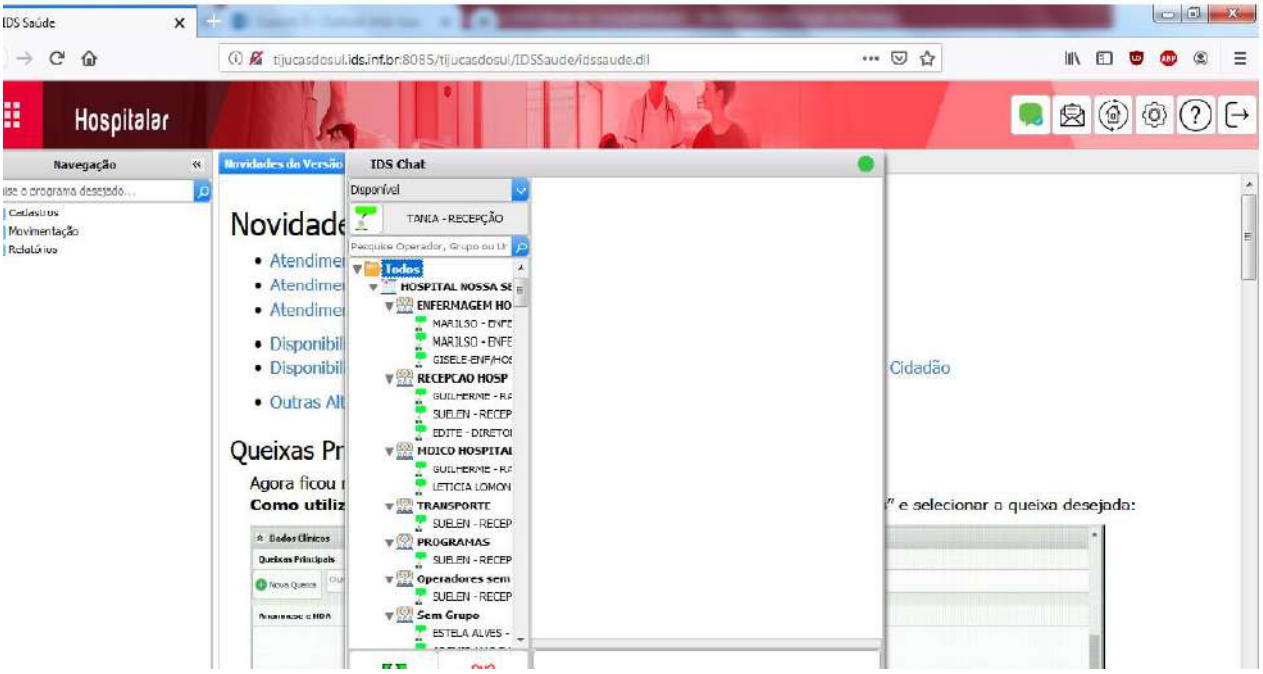


Figura 54 – Tela de recursos do software

Outro ponto relacionado aos sistemas é o fato de a Prefeitura não possuir uma estrutura de correio eletrônico que lhe permita conceder caixas-postais para seus agentes

públicos, o que evidencia ainda mais a fragilidade da segurança envolvida na troca de correios eletrônicos. Atualmente, cada funcionário da Prefeitura utiliza-se de correio eletrônico pessoal para enviar e receber e-mails corporativos.

5. SEGURANÇA E CERTIFICADOS

Atualmente, a Prefeitura possui sistemas adequados para a proteção de seus dados e de informações críticas. Os dois sistemas em vigência dizem respeito ao controle de tráfego no perímetro da Internet (Netdeep Firewall), se mostrando como oponentes e dificultando possíveis invasões ao próprio sistema.

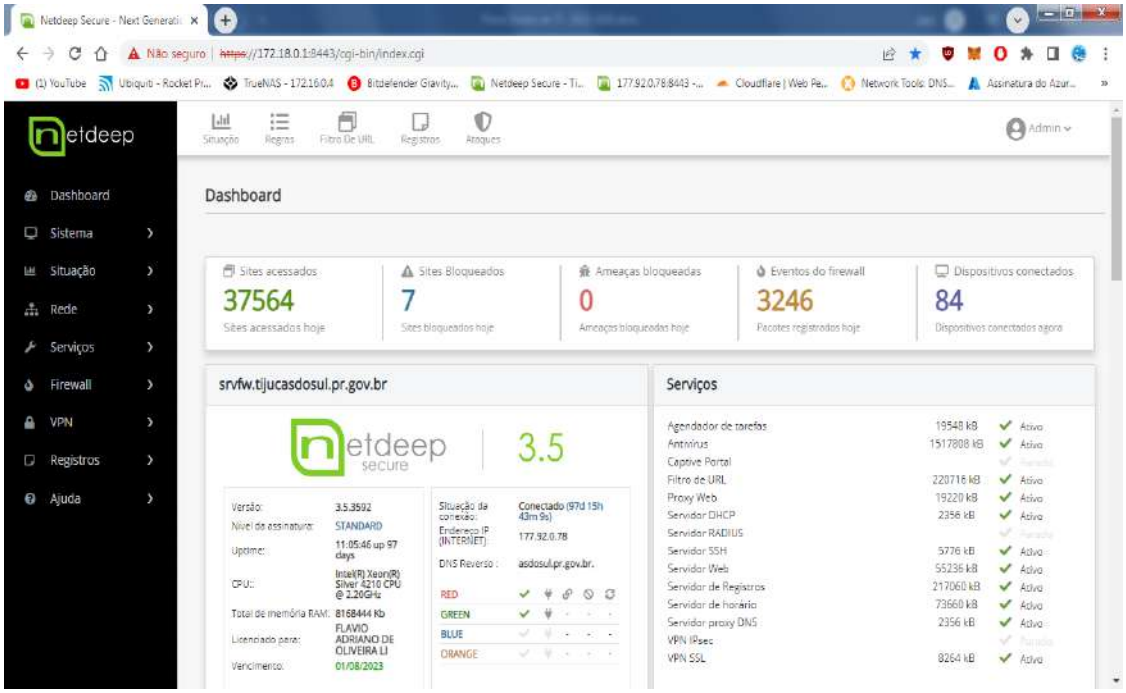
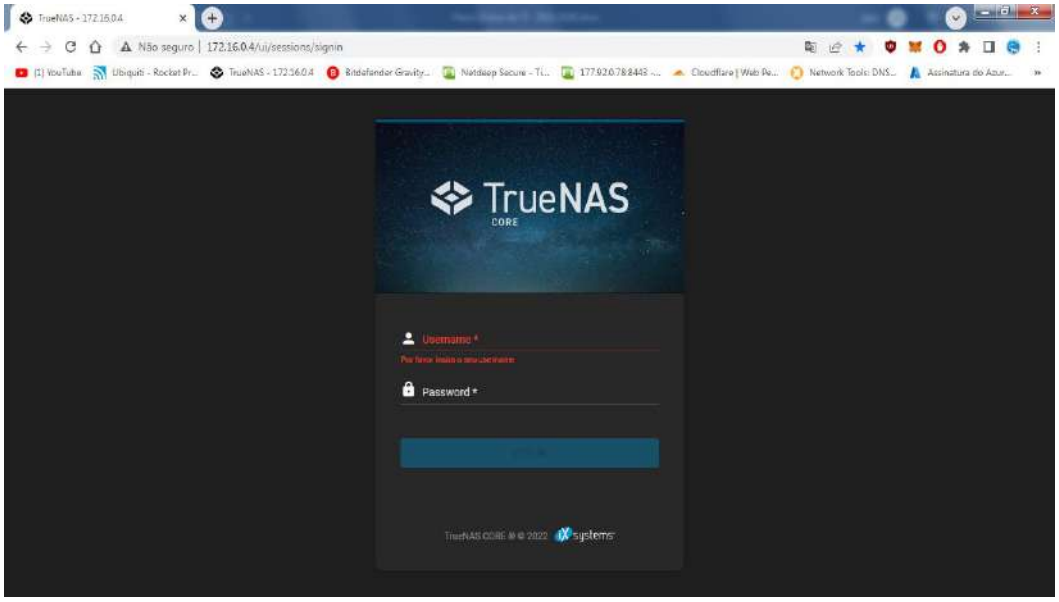


Figura 55 – Tela de recursos do firewall

Com este sistema de controle, torna-se possível a troca de dados entre a rede interna da Prefeitura com a Internet, fazendo com que ocorra de modo livre e sem restrições. Também existe uma solução de segurança de EndPoint corporativa (Sister Center e TrueNAS), o que não coloca em risco todo o parque computacional quanto às ameaças viróticas existes.



http://172.16.0.4/ui/sessions/signin

Figura 56 – Tela de recursos do TrueNAS

O processo de cópia de segurança (backup) dos servidores atualmente é feito em três camadas (Servidores, Backup Cofre e Backup Nuvem). Há solução corporativa para automatizar as rotinas de cópias de segurança, armazená-las em mídias confiáveis e gerar notificações e relatórios de administração. Atualmente, a rotina de cópia de segurança é realizada automaticamente pelo Veeam Backup & Replication 11

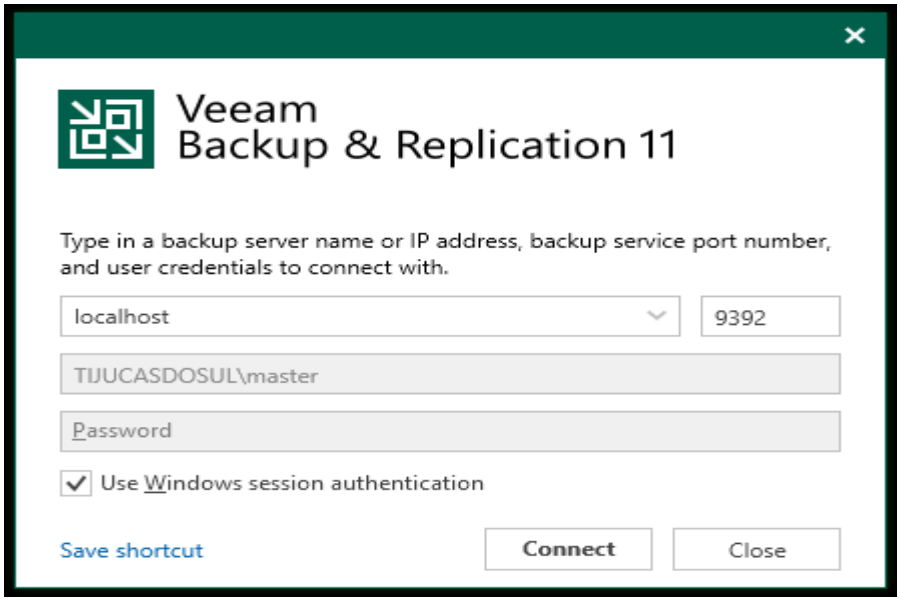


Figura 57 – Tela de recursos do Veeam Backup & Replication

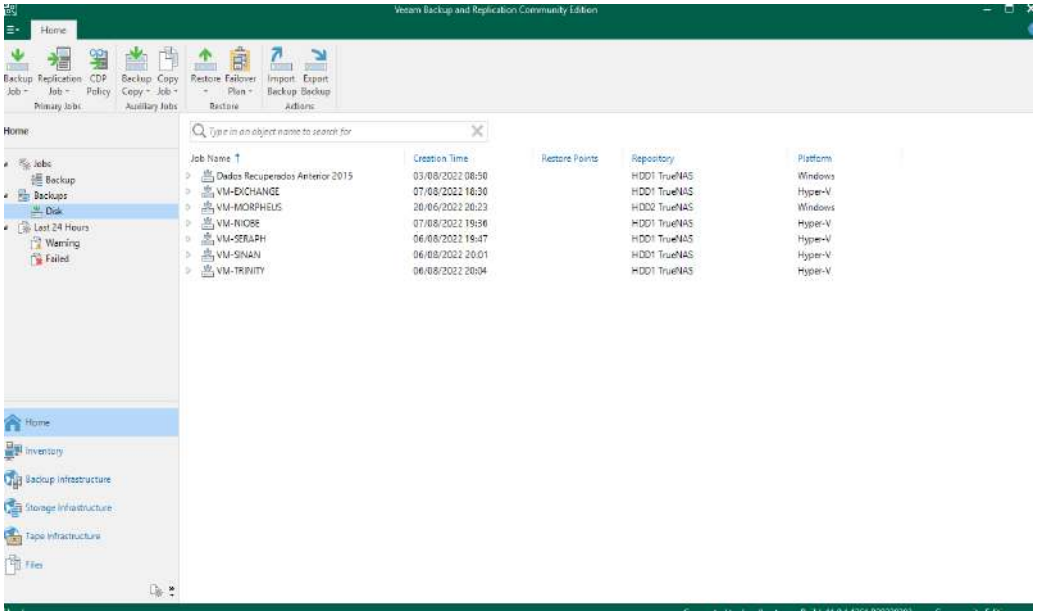


Figura 58– Tela de recursos do Veeam Backup & Replication Administração

A solução de Proxy Web atua como Web Cache transparente e controla o acesso apenas baseado nas URLs. O controle web analisa o conteúdo do site acessado e também exige autenticação baseada no usuário. Monitora lista negra (blacklist) de e-mails não autorizados .

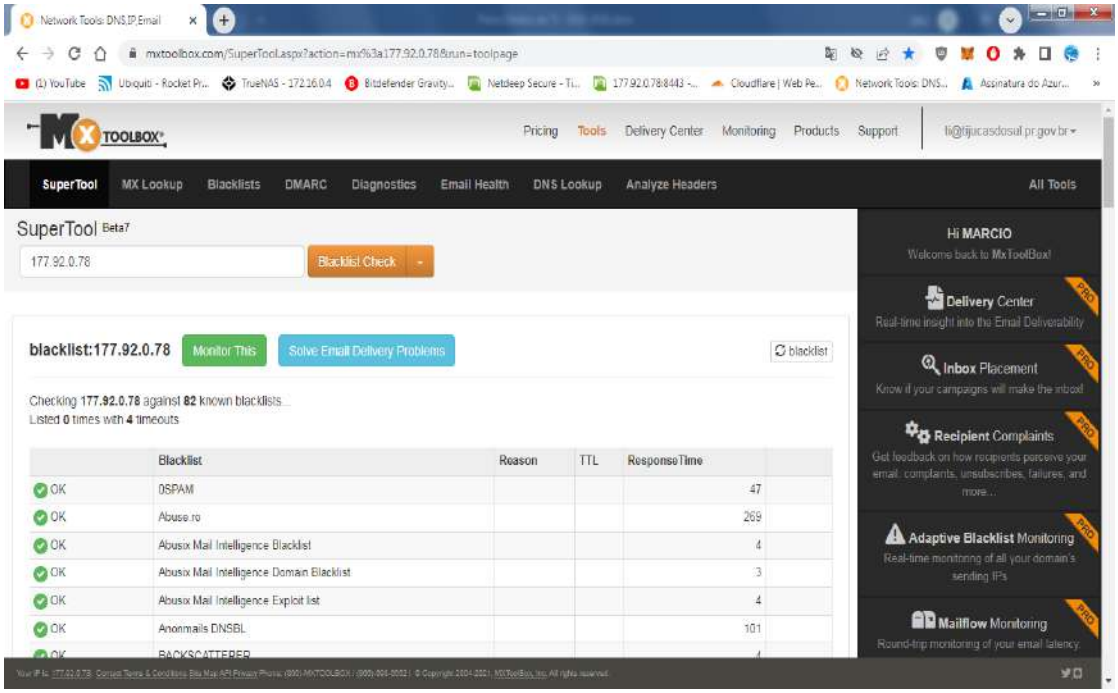


Figura 59 – Tela de recursos do MxToolbox

Observa-se na Prefeitura Municipal a ausência de soluções de segurança consideradas importantes para uma estrutura de tecnologia da informação que manipula dados confidenciais, que são as seguintes:

- Solução de criptografia de discos para dispositivos móveis; - Pendente;
- Solução de controle de conteúdo web com autenticação; - Ativa;
- Solução de controle de segurança para correio eletrônico; - Ativa;
- Solução de vídeo monitoramento para a sala de servidores; - Pendente;
- Solução de distribuição de correções e atualizações de estações; - ATIVA;
- Solução de rede para controle de acesso lógico a rede de dados; - ATIVA;
- Solução de segurança de perímetro Internet; - Ativa;
- Solução de backup corporativo para servidores e dados críticos; ATIVA;
- Atestado de Capacidade Técnica e Certificados – Ativa.
- Eficiência Energética – Pendente
- Rede de Fibra Óptica - Pendente

Eficiência energética

O foco da gestão **energética municipal** é a redução do consumo, logo, se baseia em ações de **eficiência energética** que, ao reduzirem a demanda de **energia** do sistema interligado, minimizam também o uso de termoeletricidade, caso esta seja a fonte de **energia** elétrica.

As ações de eficiência energética:

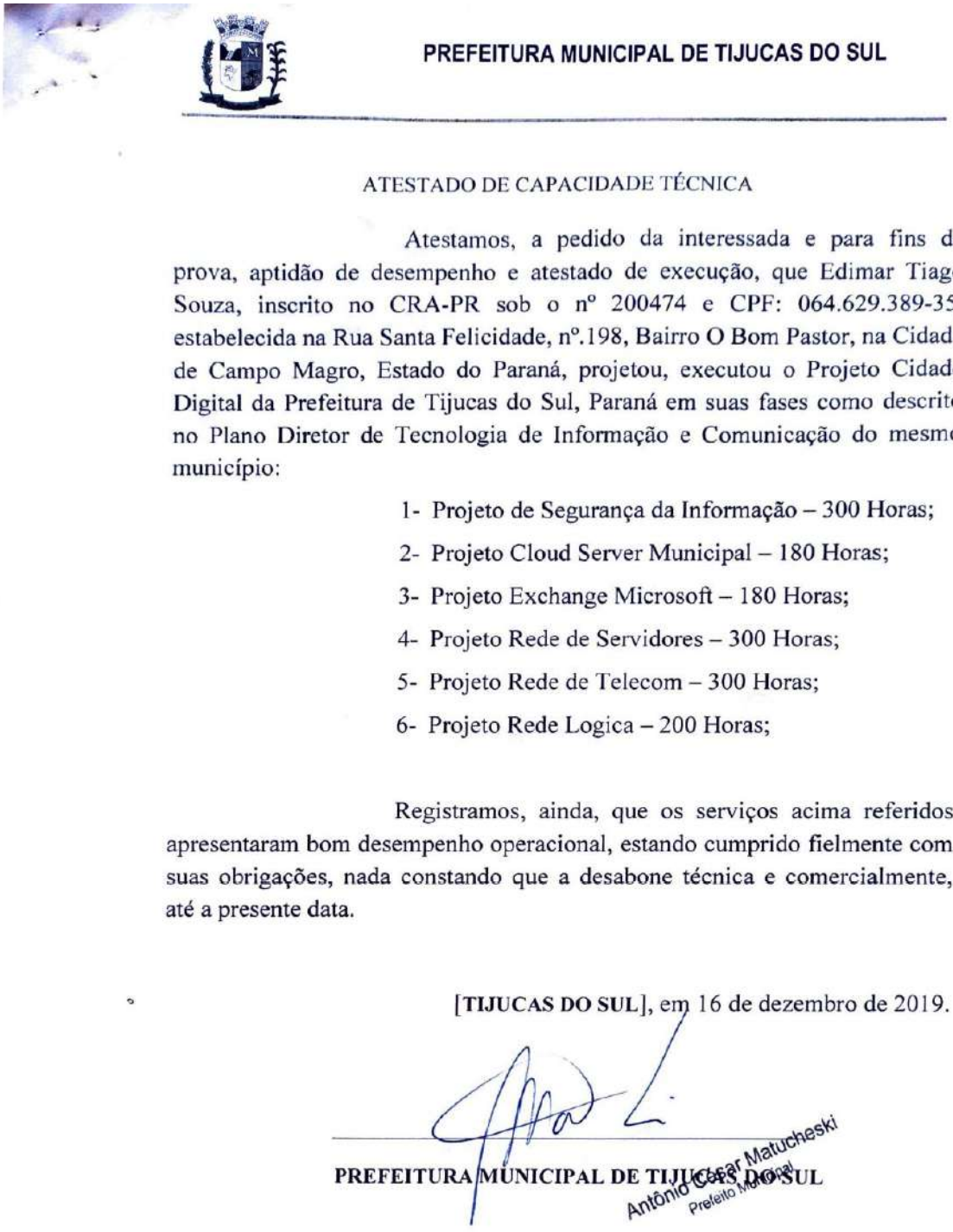
- Modernização de equipamentos;
- Reduzir excedente de **energia** reativa;
- Conquistar certificação de **eficiência energética**;
- Realizar medições setoriais;
- Adotar sistema de gerenciamento de **energia**;

Figura 60 – Ginásio de Esporte com Eficiência Energética

Figura 61 – Hospital com Eficiência Energética

Figura 62 – Rodoviária com Eficiência Energética

Figura 63 – Iluminação Pública com Eficiência Energética



PREFEITURA MUNICIPAL DE TIJUCAS DO SUL

ATESTADO DE CAPACIDADE TÉCNICA

Atestamos, a pedido da interessada e para fins de prova, aptidão de desempenho e atestado de execução, que Edimar Tiago Souza, inscrito no CRA-PR sob o nº 200474 e CPF: 064.629.389-35, estabelecida na Rua Santa Felicidade, nº.198, Bairro O Bom Pastor, na Cidade de Campo Magro, Estado do Paraná, projetou, executou o Projeto Cidade Digital da Prefeitura de Tijucas do Sul, Paraná em suas fases como descrito no Plano Diretor de Tecnologia de Informação e Comunicação do mesmo município:

1- Projeto de Segurança da Informação – 300 Horas;
2- Projeto Cloud Server Municipal – 180 Horas;
3- Projeto Exchange Microsoft – 180 Horas;
4- Projeto Rede de Servidores – 300 Horas;
5- Projeto Rede de Telecom – 300 Horas;
6- Projeto Rede Logica – 200 Horas;

Registramos, ainda, que os serviços acima referidos apresentaram bom desempenho operacional, estando cumprido fielmente com suas obrigações, nada constando que a desabone técnica e comercialmente, até a presente data.

[TIJUCAS DO SUL], em 16 de dezembro de 2019.

PREFEITURA MUNICIPAL DE TIJUCAS DO SUL
Antônio Cesar Matucheski
Prefeito Municipal

Rua XV de Novembro, 1458, Centro, Tijucas do Sul - Pr.
CEP 83.190-000, Caixa Postal nº 31, Fone/Fax (41) 3629-1186.

Figura 64 – Atestado de capacidade técnica

PREFEITURA MUNICIPAL DE TIJUCAS DO SUL

CERTIFICADO

Certificamos que **MAYCON DE OLIVEIRA,** CPF 049.092.219-80, Concluiu com sucesso o **Projeto de Rede de Servidores**, na Prefeitura Municipal de Tijucas do Sul, com carga horária de **300 horas** técnicas para a cidade digital do município com excelência e presteza.

Prefeitura Municipal de Tijucas do Sul

Maycon de Oliveira

Tijucas do Sul, 15 de Março de 2019.

PREFEITURA MUNICIPAL DE TIJUCAS DO SUL

CERTIFICADO

Certificamos que **MAYCON DE OLIVEIRA,** CPF 049.092.219-80, Concluiu com sucesso o **Projeto de Rede Lógica Estruturada**, na Prefeitura Municipal de Tijucas do Sul, com carga horária de **200 horas** técnicas para a cidade digital do município com excelência e presteza.

Prefeitura Municipal de Tijucas do Sul

Maycon de Oliveira

Tijucas do Sul, 10 de Abril de 2018.

Figura 65 - Certificados

PREFEITURA MUNICIPAL DE TIJUCAS DO SUL

CERTIFICADO

Certificamos que **MAYCON DE OLIVEIRA,** CPF 049.092.219-80, Concluiu com sucesso o **Projeto Exchange Microsoft,** na Prefeitura Municipal de Tijucas do Sul, com carga horária de **180 horas** técnicas para a cidade digital do município com excelência e presteza.

Prefeitura Municipal de Tijucas do Sul

Maycon de Oliveira

Tijucas do Sul, 25 de Agosto de 2018.

Expedição de acordo com o Decreto Municipal n° 1104 de 24/11/2010.

PREFEITURA MUNICIPAL DE TIJUCAS DO SUL

CERTIFICADO

Certificamos que **MAYCON DE OLIVEIRA,** CPF 049.092.219-80, Concluiu com sucesso o **Projeto de Rede de Telecom,** na Prefeitura Municipal de Tijucas do Sul, com carga horária de **300 horas** técnicas para a cidade digital do município com excelência e presteza.

Prefeitura Municipal de Tijucas do Sul

Maycon de Oliveira

Tijucas do Sul, 15 de Março de 2019.

Expedição de acordo com o Decreto Municipal n° 1104 de 24/11/2010.

Figura 66 - Certificados

PREFEITURA MUNICIPAL DE TIJUCAS DO SUL
Secretaria Municipal de Administração e Planejamento

Memorando n°07/2020 – ADM — Tijucas do Sul, 09 de janeiro de 2020

Departamento de T.I.
Prefeitura Municipal de Tijucas do Sul

Em atenção ao memorando 52/2019, o qual solicita validação do atestado de capacidade técnica, dos serviços executados pelo servidor Edimar Tiago Souza, encaminho documento devidamente assinado.

Atenciosamente

Kelli do Rocio Rozario.
Kelli do Rocio Rozário
Secretária de Administração e Planejamento

Rua XV de Novembro, 1458, Centro, Tijucas do Sul - PR
CEP 83.190-000, Caixa Postal: nº 31, Fone: (41) 3629-1210 Ramal (5)

Figura 67 - Memorando

6. SERVIDORES E ESTAÇÕES

O conjunto de estações de trabalho da Prefeitura se resume aos sistemas operacionais Microsoft Windows 7 e 10. As estações de trabalho são próprias e possuem o software de escritório Microsoft Office instalado, (imagens a seguir). Também existe a suíte do Open-Office distribuída em alguns ambientes. Por fim, as máquinas da engenharia fazem uso de softwares para manipulação de desenhos, plantas etc., mais conhecidos como CAD.

Figura 68 - Microsoft Windows 7

Figura 69- Microsoft Windows 10

Figura 70 - Microsoft Windows 11

Figura 71 - LibreOffice

Figura 72 - Microsoft Office 2013

Figura 73 - Microsoft Office 365

O parque de servidores é composto de 8 unidades, sendo 07 (sete) Microsoft Windows 2008 Server e 01 (um) Linux, como mostram as figuras a seguir. Todos os sistemas dos servidores não possuem garantia de suporte externo.

Figura 74 – Sistema operacionais dos Servidores

Não há licenças para utilização de todos os sistemas operacionais Microsoft Windows e também do software AutoCAD utilizado na engenharia, o que caracteriza violação de direitos com a prática de pirataria.

A utilização de impressoras não é controlada. Há apenas uma recomendação verbal para que não se utilize determinadas impressoras em processo de desenvolvimento servidor de gerenciamento de impressão.

Apesar de pequena, somente a equipe de informática possui permissão para realizar atividades administrativas nas estações de trabalho. A instalação de softwares é sempre realizada com anuência da equipe técnica local.

7. PESSOAS E PROCESSOS

Os atuais prestadores de serviço da Prefeitura Municipal, no segmento de tecnologia da informação, são:

Tabela 4 - Fornecedores

Empresa	Objeto
Equiplano	Empresa responsável pelo sistema de gestão municipal.
Ligga Telecom	Empresa responsável pelo provimento de um dos enlaces de Internet.
Lima Informática	Empresa responsável pelo provimento equipamentos de

	informática e infraestrutura de telefonia, cabeamento logico.
Lima Informática	Empresa de suporte técnico ao website da prefeitura municipal.
Gama Segurança	Monitoramento eletrônico e Câmeras de Segurança.

Em relação ao atendimento de suporte reativo, se o problema for lógico em nível de software, é realizado o acesso remoto para sua resolução. Caso o problema seja no sistema Equiplano, o usuário é orientado a abrir um chamado diretamente com a empresa fornecedora com cópia ao suporte técnico Municipal de Tijucas do Sul.

Em relação ao atendimento de suporte preventivo, há uma política definida para atualização dos softwares e sistemas operacionais das estações de trabalho e servidores. Quanto ao sistema Equiplano, o próprio fornecedor fica responsável pela manutenção e atualização dos módulos incluindo o banco de dados.

8. PRESTAÇÃO DE SERVIÇOS

O diagnóstico de tecnologia da informação, por fim, evidenciou a necessidade de implementação de novos sistemas para assegurar facilidade à vida dos munícipes, como por exemplo: o Programa Internet para Todos (Internet Livre), que se encontra em fase de implantação.

9. GAP ANÁLISE

A GAP Análise é o processo pelo qual a entidade mede o nível de aderência de seu Sistema de Gestão de Segurança da Informação em relação aos controles objetivos de acordo com o código de práticas para a gestão da segurança da informação NBR ISO/IEC 17799:2006.

Esse processo é muito importante, do ponto de vista sistemático, pois habilita um levantamento dos controles usados, apontando os controles implementados parcialmente, os não implementados e os que não se aplicam ao sistema e ao negócio da entidade.

Ao fim da GAP análise, será possível obter uma visão geral do sistema. Esse processo também serve como complemento e base para validação para o plano de ação a ser proposto a fim de se alcançar aderência e futura certificação da NBR ISO/IEC

27001:2006.

9.1. Metodologia

A metodologia usada para elaboração do GAP análise contemplou levantamento de informações por entrevistas, análise dos padrões e procedimentos existentes da entidade, análise do ambiente e/ou resultados de avaliações prévias do projeto de desenvolvimento de política de segurança.

Os resultados da GAP análise são baseados na pesquisa de ambiente da Prefeitura Municipal de Tijucas do Sul, comparado aos controles definidos do apêndice A da NBR ISO/IEC 27001. O percentual do nível de aderência conferido a cada controle é baseado na existência ou não dos controles e na quantidade de esforço necessário para a implementação dos mesmos, caso seja necessário.

Essa metodologia é uma inferência, baseado nos benchmarks de mercado bem como, na familiarização com os passos para desenvolvimento e implementação de um Sistema de Gerenciamento da Segurança da Informação - SGSI.

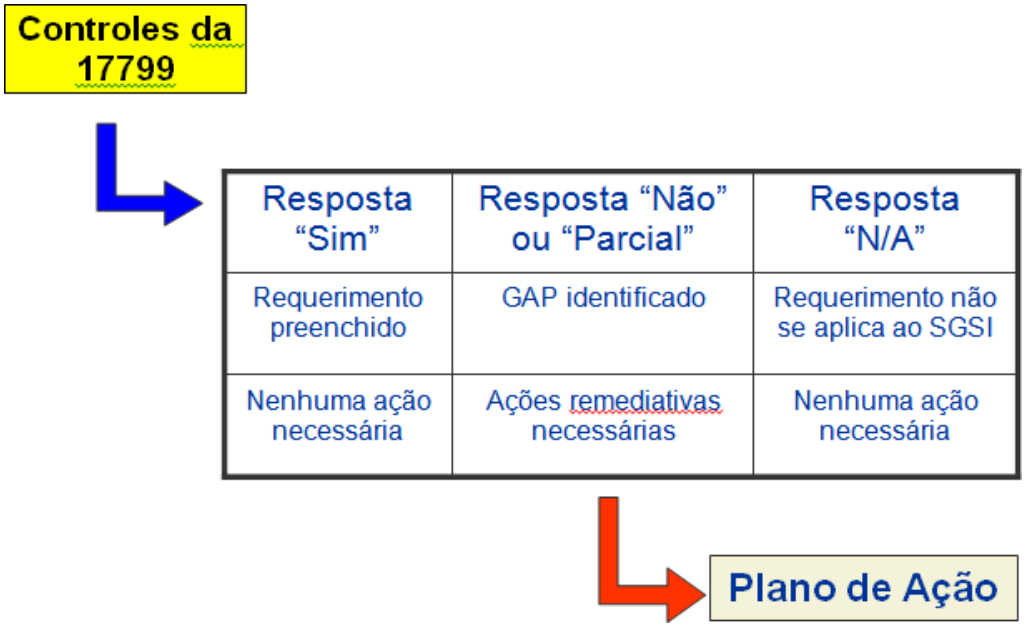


Figura 75 - Fluxo da GAP Análise

9.2. Divisão dos Controles

Os controles especificados no Sistema de Gerenciamento da Segurança da Informação são divididos nas seguintes áreas:

1. Política de segurança;
2. Organizando a segurança da informação;
3. Gestão de Ativos;
4. Segurança em recursos humanos;
5. Segurança física e do ambiente;
6. Gerenciamento das operações e comunicações;
7. Controle de acessos;
8. Aquisição, desenvolvimento e manutenção de sistemas de informação;
9. Gestão de incidentes de segurança da informação;
10. Gestão de continuidade do negócio;
11. Conformidade.

9.3. Resumo dos Controles

Visa descrever os resultados obtidos através das entrevistas:

Tabela 5 - Política de Segurança

A.5 Política de segurança			
A.5.1 Política de segurança da informação Objetivo: Prover uma orientação de apoio à direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.			
	Controle	**GAP**	**Justificativa**
A.5.1.1	Documento da política de segurança da informação	NÃO	Não existe referência das melhores práticas de segurança, conforme padrões da norma ISO 27001.
A.5.1.2	Análise crítica da política de segurança da informação	NÃO	Análises críticas devem ser realizadas ao menos uma vez a cada seis meses.

Tabela 6 - Organizando a segurança da informação

A.6 Organizando a segurança da informação			
A.6.1 Infra-estrutura da segurança da informação *Objetivo:* Gerenciar a segurança da informação dentro da organização.			
	Controle	**GAP**	**Justificativa**
A.6.1.1	Comprometimento da direção com a segurança da informação	PARCIAL	Apesar da existência de conscientização, existe a necessidade de documentação através de uma Política de Segurança.
A.6.1.2	Coordenação da segurança da informação	NÃO	Necessidade de um Comitê de Segurança da Informação.
A.6.1.3	Atribuição de responsabilidade para a segurança da informação	NÃO	As pessoas envolvidas possuem consciência de suas responsabilidades, mas é necessário documentar as responsabilidades na política de Segurança.
A.6.1.4	Processo de autorização para os recursos de processamento da informação	NÃO	Processo documentado inexistente.

A.6.1.5	Acordo de confidencialidade	NÃO	Garantir a responsabilidade e confidencialidade das informações.
A.6.1.6	Contato com autoridades	SIM	
A.6.1.7	Contato com grupos especiais	NÃO	Consultoria especializada em segurança da informação.
A.6.1.8	Análise crítica independente de segurança da informação	NÃO	A PMTS deverá determinara periodicidade e responsabilidade das análises críticas do SGSI.
A.6.2 Partes externas			
	Controle	**GAP**	**Justificativa**
A.6.2.1	Identificação dos riscos relacionados com partes externas	NÃO	A avaliação de riscos não é realizada ou documentada nestes documentos.
A.6.2.2	Identificando a segurança da informação quando tratando com os clientes	PARCIAL	Procedimentos precisam ser documentados.
A.6.2.3	Identificando a segurança da informação nos acordos com os terceiros	PARCIAL	Procedimentos precisam ser documentados.

Tabela 7 - Gestão de ativos

A.7 Gestão de ativos			
A.7.1 Responsabilidade pelos ativos *Objetivo:* Alcançar e manter a proteção adequada dos ativos da organização.			
	Controle	**GAP**	**Justificativa**
A.7.1.1	Inventário dos ativos	PARCIAL	Inventário não está completo e/ou atualizado.
A.7.1.2	Proprietário dos ativos	NÃO	Proprietários não estão documentados e o processo de classificação precisa ser desenvolvido.
A.7.1.3	Uso aceitável dos ativos	NÃO	Não existe uma política documentada que descreva as regras de utilização dos recursos.

A.7.2 Classificação da informação			
	Controle	**GAP**	**Justificativa**
A.7.2.1	Recomendações para a classificação	NÃO	Processo de classificação da Informação deve ser desenvolvido.
A.7.2.2	Rótulos e tratamento da informação	NÃO	Processo de classificação da informação deve ser desenvolvido.

Tabela 8 - Segurança em recursos humanos

A.8 Segurança em recursos humanos			
A.8.1 Antes da contratação			
Objetivo: Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades, e estejam de acordo com os seus papéis, e reduzir o risco de roubo, fraude ou mau uso de recursos.			
	Controle	**GAP**	**Justificativa**
A.8.1.1	Papéis e responsabilidades	PARCIAL	Processo não está documentado de forma formal através de Termos de Responsabilidades.
A.8.1.2	Seleção	PARCIAL	Existe um processo, mas o procedimento precisa ser documentado.
A.8.1.3	Termos e condições de contratação	PARCIAL	Termos e condições precisam ser documentados. Uma sugestão seria a publicação de um Código de Conduta.
A.8.2 Durante a contratação			
Objetivo: Assegurar que os funcionários, fornecedores e terceiros estão conscientes das ameaças e preocupações relativas à segurança da informação, suas responsabilidades e obrigações, e estão preparados para apoiar a política de segurança da informação da organização durante os seus trabalhos normais e para reduzir o risco de erro humano.			
	Controle	**GAP**	**Justificativa**
A.8.2.1	Responsabilidades da direção	PARCIAL	Inexistência de processo e conscientização.

A.8.2.2	Conscientização, educação e treinamento em segurança da informação	PARCIAL	Inexistência de programas de treinamentos e ciclos de palestras do assunto.
A.8.2.3	Processo disciplinar	PARCIAL	Não existe um processo disciplinar documentado.
A.8.3 Encerramento ou mudança da contratação *Objetivo:* Assegurar que funcionários, fornecedores e terceiros deixem a organização ou mudem de trabalho de forma ordenada.			
	Controle	**GAP**	**Justificativa**
A.8.3.1	Encerramento de atividades	PARCIAL	Existe um processo, mas o procedimento precisa ser documentado.
A.8.3.2	Devolução de ativos	NÃO	Não existe o processo documentado.
A.8.3.3	Retirada de direitos de acesso	NÃO	Não existe o processo documentação.

Tabela 9 - Segurança física e do ambiente

A.9 Segurança física e do ambiente			
A.9.1 Áreas seguras *Objetivo:* Prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização.			
	Controle	**GAP**	**Justificativa**
A.9.1.1	Perímetro de segurança física	SIM	Sistema de controle de acesso físico está presente, mas deve ser melhorado.
A.9.1.2	Controles de entrada física	SIM	Sistema de controle de acesso físico está presente, mas deve ser melhorado.
A.9.1.3	Segurança em escritórios salas e instalações	SIM	Sistema de controle de acesso físico está presente, mas deve ser melhorado.
A.9.1.4	Proteção contra ameaças externas e do meio ambiente	SIM	Pode ser melhorado.
A.9.1.5	Trabalhando em áreas seguras	PARCIAL	Pode ser melhorado.
A.9.1.6	Acesso do público, áreas de entrega e de carregamento	N/A	

A.9.2 Segurança de equipamentos *Objetivo:* Impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização.			
	Controle	**GAP**	**Justificativa**
A.9.2.1	Instalação e proteção do equipamento	NÃO	As medidas de segurança para os equipamentos dentro do CPD não são eficazes.
A.9.2.2	Utilidades	PARCIAL	Equipamentos estão protegidos por nobreaks que estabilizam a corrente elétrica e fornecem energia em caso de falhas no fornecimento primário, mas o sistema precisa ser melhorado.
A.9.2.3	Segurança do cabeamento	NÃO	Cabeamento não está de acordo com os padrões de segurança e não são certificados.
A.9.2.4	Manutenção dos equipamentos	PARCIAL	A devidas manutenções são realizadas, mas é preciso documentar o processo de manutenção preventiva dos equipamentos para evitar paradas aleatórias e não agendadas.
A.9.2.5	Segurança de equipamentos fora das dependências da organização	NÃO	Necessário definir recomendações para os usuários. Equipamentos podem transportar dados confidenciais sem proteção adequada (criptografia)
A.9.2.6	Reutilização e alienação segura de equipamentos	NÃO	Procedimentopara descartede equipamentos/mídias inexistente.
A.9.2.7	Remoção de propriedades	PARCIAL	Precisa formalizar procedimento.

Tabela 10 - Gerenciamento das operações e comunicações

A.10 Gerenciamento das operações e comunicações			
A.10.1 Procedimentos e responsabilidades operacionais *Objetivos:* Garantir a operação segura e correta dos recursos de processamento da informação			
	Controle	**GAP**	**Justificativa**
A.10.1.1	Documentação dos procedimentos de operação	NÃO	Precisa formalizar procedimento.

A.10.1.2	Gestão de mudanças	NÃO	Não existe procedimento formalizado para efetuar alterações no ambiente.
A.10.1.3	Segregações de funções	PARCIAL	Necessária a formalização.
A.10.1.4	Separação dos recursos de desenvolvimento, teste e de produção.	NÃO	Atualmente não existem ambientes de testes e homologação.

A.10.2 Gerenciamento de serviços terceirizados

Objetivo: Implementar e manter o nível apropriado de segurança da informação e de entrega de serviços em consonância com acordos de entrega de serviços terceirizados.

	Controle	GAP	Justificativa
A.10.2.1	Entrega de serviços	SIM	Cada área é responsável por gerir a entrega dos serviços prestados pelos terceiros.
A.10.2.2	Monitoramento e análise crítica de serviços terceirizados	NÃO	Procedimento inexistente.
A.10.2.3	Gerenciamento de mudanças para serviços terceirizados	NÃO	Procedimento inexistente.

A.10.3 Planejamento e aceitação dos sistemas

Objetivo: Minimizar o risco de falhas nos sistemas.

	Controle	GAP	Justificativa
A.10.3.1	Gestão de capacidade	NÃO	Os ativos não são monitorados quanto à capacidade e detecção de falhas.
A.10.3.2	Aceitação de sistemas	SIM	Os sistemas adquiridos foram homologados para execução de suas tarefas. Importante definir processo de Certificação e Acreditação.

A.10.4 Proteção contra códigos maliciosos e códigos móveis

Objetivo: Proteger a integridade do software e da informação

	Controle	GAP	Justificativa
A.10.4.1	Controle contra códigos maliciosos	SIM	Organização possui software antivírus atualizado e instalado em todas as estações. Além disso, existe um firewall protegendo a rede interna de Infecções via Internet.

A.10.4.2	Controles contra códigos móveis	SIM	Organização possui software antivírus atualizado e instalado em todas as estações. Além disso, existe um firewall protegendo a rede interna de Infecções via Internet.
A.10.5 Cópias de segurança *Objetivo:* Manter a integridade e disponibilidade da informação e dos recursos de processamento de informação.			
	Controle	**GAP**	**Justificativa**
A.10.5.1	Cópias de segurança das informações	PARCIAL	A organização não possui software de backup em uso, pois este é feito de maneira manual. No entanto: 1) Documentação dos Jobs de backup precisa ser aprimorada; 2) Testes de restore precisam ser realizados e documentados; 3) Política de Retenção e Utilização de nuvem precisa ser definida.
A.10.6 Gerenciamento da segurança em redes *Objetivo:* Garantir a proteção das informações em redes e a proteção da infraestrutura de suporte.			
	Controle	**GAP**	**Justificativa**
A.10.6.1	Controles de redes	NÃO	Inexistência de solução Network Admission Control – NAC.
A.10.6.2	Segurança dos serviços de rede	PARCIAL	Existe a utilização de Firewalls, mas possuem IPS integrado.
A.10.7 Manuseio de mídias *Objetivo:* Prevenir contra divulgação não autorizada, modificação, remoção ou destruição aos ativos e interrupções das atividades do negócio.			
	Controle	**GAP**	**Justificativa**
A.10.7.1	Gerenciamento de mídias removíveis	NÃO	Ausência de procedimentos para gerenciar mídias removíveis.
A.10.7.2	Descarte de mídias	NÃO	Ausência de procedimentos para descarte de mídias removíveis.

A.10.7.3	Procedimento para tratamento de informações	PARCIAL	Restrições de acesso encontram-se operantes, no entanto, os níveis de classificação ainda não foram definidos.
A.10.7.4	Segurança da documentação dos sistemas	SIM	Documentação se encontra armazenada na rede com controles de acesso.

A.10.8 Troca de informações

Objetivo: Manter a segurança na troca de informações e softwares internamente à organização e com quaisquer entidades externas.

	Controle	GAP	Justificativa
A.10.8.1	Políticas e procedimentos para troca de informações	NÃO	O uso aceitável de ativos não se encontra documentado, conforme requisitos da norma.
A.10.8.2	Acordo para a troca de informações	NÃO	Não existe documentação, conforme requisitos da norma.
A.10.8.3	Mídias em trânsito	N/A	No caso de contratação de empresa para armazenamento de mídias de backup, este item deverá ser revisado.
A.10.8.4	Mensagens eletrônicas	NÃO	Mensagens eletrônicas com conteúdo confidencial deveriam ser codificadas através de cifragem.
A.10.8.5	Sistemas de informações do negócio	NÃO	Atualmente não existe solução de correio eletrônico corporativo.

A.10.9 Serviços de comércio eletrônico

Objetivo: Garanti a segurança de serviços de comércio eletrônico e sua utilização segura.

	Controle	GAP	Justificativa
A.10.9.1	Comércio eletrônico	N/A	
A.10.9.2	Transações on-line	N/A	
A.10.9.3	Informações publicamente disponíveis	N/A	

A.10.10 Monitoramento

Objetivo: Detectar atividades não autorizadas de processamento de informações.

	Controle	GAP	Justificativa
A.10.10.1	Registros de auditoria	NÃO	Inexistência de Auditoria dos servidores.
A.10.10.2	Monitoramento do uso do sistema	NÃO	Inexistência de monitoramento de aplicativos, banco de dados, servidores, etc.
A.10.10.3	Proteção das informações dos registros (logs)	SIM	Informações dos registros são protegidas através de controles de acesso.
A.10.10.4	Registros de (log) de administrador e operador	PARCIAL	Registros são mantidos, no entanto, a análise crítica destes ainda não é realizada.
A.10.10.5	Registros (logs) de falhas	PARCIAL	Registros de falhas são salvos, mas não existe um processo de análise sobre os registros de falha. Processo precisa ser melhorado.
A.10.10.6	Sincronização dos relógios	NÃO	Permite o rastreamento uniforme das de auditorias etc.

Tabela 11 - Controle de acessos

A.11 Controle de acessos			
A.11.1 Requisitos de negócio para controle de acesso *Objetivo:* Controlar o acesso à informação.			
	Controle	**GAP**	**Justificativa**
A.11.1.1	Política de controle de acesso	NÃO	Política de Controle de Acesso não está documentada.
A.11.2 Gerenciamento de acesso do usuário *Objetivo:* Assegurar acesso de usuários autorizados e prevenir o acesso não autorizado ao sistema de informação.			
	Controle	**GAP**	**Justificativa**
A.11.2.1	Registro de usuários	PARCIAL	A retirada de acessos é efetuada, no entanto, é preciso documentar o processo de desligamento.

A.11.2.2	Gerenciamento de privilégios	PARCIAL	Gerenciamento de privilégios é realizado sem procedimento documentado.
A.11.2.3	Gerenciamento de senha do usuário	PARCIAL	Realizado através das aplicações disponíveis, no entanto é preciso documentar.
A.11.2.4	Análise crítica dos direitos de acesso de usuário	NÃO	A revisão dos acessos não é realizada em intervalos regulares documentados.

A.11.3 Responsabilidades dos usuários

Objetivo: Prevenir o acesso não autorizado dos usuários e evitar o comprometimento ou roubo da informação e dos recursos de processamento da informação.

	Controle	GAP	Justificativa
A.11.3.1	Uso de senhas	SIM	Necessário documentar.
A.11.3.2	Equipamento de usuários sem monitoração	SIM	
A.11.3.3	Política de mesa limpa e tela limpa	NÃO	Não existe política definida.

A.11.4 Controle de acesso à rede

Objetivo: Prevenir acesso não autorizado aos serviços de rede.

	Controle	GAP	Justificativa
A.11.4.1	Política de uso dos serviços de rede	NÃO	Não existe política definida.
A.11.4.2	Autenticação para conexão externa do usuário	SIM	Precisa ser melhorado e documentado.
A.11.4.3	Identificação de equipamento em redes	SIM	Precisa ser melhorado.
A.11.4.4	Proteção e configuração de portas de diagnóstico remotas	SIM	Precisa ser melhorado.
A.11.4.5	Segregação de redes	NÃO	Inexistência de VLAN's.
A.11.4.6	Controle de conexão de rede	SIM	Precisa ser melhorado e Documentado.
A.11.4.7	Controle de roteamento de redes	SIM	Pode ser melhorado, pois hoje está sendo feito através do Firewalls.

A.11.5 Controle de acesso ao sistema operacional

Objetivo: Prevenir o acesso não autorizado aos sistemas operacionais.

	Controle	GAP	Justificativa
A.11.5.1	Procedimentos seguros de entrada no sistema (log-on)	SIM	
A.11.5.2	Identificação e autenticação de usuário	SIM	
A.11.5.3	Sistema de gerenciamento de senha	SIM	
A.11.5.4	Uso de utilitários de sistema	SIM	O uso destes utilitários depende de direito de acesso de administrador.
A.11.5.5	Desconexão de terminal por inatividade	SIM	Bloqueio automático das estações exigindo usuário e senha para liberação
A.11.5.6	Limitação de horário de conexão	N/A	

A.11.6 Controle de acesso à aplicação e à informação

Objetivo: Prevenir o acesso não autorizado à informação contida nos sistemas de aplicação.

	Controle	GAP	Justificativa
A.11.6.1	Restrição de acesso à informação	PARCIAL	Os controles de acesso são implementados, no entanto, não existe Política de Controle de Acesso documentada.
A.11.6.2	Isolamento de sistemas sensíveis	NÃO	Não existe isolamento de sistemas críticos.

A.11.7 Computação móvel e trabalho remoto

Objetivo: Garantir a segurança da informação quando se utilizam a computação móvel e recursos de trabalho remoto.

	Controle	GAP	Justificativa
A.11.7.1	Computação e comunicação móvel	NÃO	Não existe Política de Computação Móvel documentada. Os notebooks não possuem solução criptográfica instalada.
A.11.7.2	Trabalho remoto	N/A	

Tabela 12 - Aquisição, desenvolvimento e manutenção de sistemas de informação

A.12 Aquisição, desenvolvimento e manutenção dos sistemas de informação			
A.12.1 Requisitos de segurança de sistemas de informação *Objetivo:* Garantir que a segurança é parte integrante dos sistemas de informação.			
	Controle	**GAP**	**Justificativa**
A.12.1.1	Análise e especificação dos requisitos de segurança	NÃO	Os requisitos de segurança não são avaliados antes da aquisição ou Desenvolvimento de aplicações.
A.12.2 Processamento correto de aplicações *Objetivo:* Prevenir a ocorrência de erros, perdas, modificações não autorizadas ou mau uso de informações em aplicações.			
	Controle	**GAP**	**Justificativa**
A.12.2.1	Validação dos dados de entrada	PARCIAL	Todos os sistemas em uso fazem validações básicas dos dados entrados, no entanto, acredita-se que algumas das verificações da norma não sejam realizadas. A criação de procedimentos de validação/homologação de sistemas é recomendada.
A 12.2.2	Controle do processamento interno	PARCIAL	Todos os sistemas em uso fazem validações básicas dos dados entrados, no entanto, acredita-se que algumas das verificações da norma não sejam realizadas. A criação de procedimentos de validação/homologação de sistemas é recomendada.
A 12.2.3	Integridade de mensagens	PARCIAL	Mensagens enviadas por sistemas automatizados poderiam ser assinadas digitalmente.
A 12.2.4	Validação de dados de saída	PARCIAL	Os dados de saída das aplicações são validados pelos operadores dos sistemas, no entanto, não existe um procedimento formal para esta atividade.

A.12.3 Controles criptográficos			
Objetivo: Proteger a confidencialidade, a autenticação ou a integridade das informações por méis criptográficos.			
	Controle	**GAP**	**Justificativa**
A.12.3.1	Política para o uso de controles criptográficos	NÃO	Uma política para o uso de controles criptográficos não se encontra definida.
A.12.3.2	Gerenciamento de chaves	NÃO	Não há gerenciamento de chaves uma vez que recursos criptográficos não se encontram em uso.
A.12.4 Segurança dos arquivos do sistema			
Objetivo: Garantir a segurança de arquivos de sistemas.			
	Controle	**GAP**	**Justificativa**
A.12.4.1	Controle de software operacional	PARCIAL	Os procedimentos precisam ser documentados.
A.12.4.2	Proteção dos dados para teste de sistemas	NÃO	Não existe separação de ambientes de testes, homologação e produção. O processo está sendo formalizado.
A.12.4.3	Controles de acesso ao código-fonte de programa	NÃO	
A.12.5 Segurança em processos de desenvolvimento e de suporte			
Objetivo: Manter a segurança de sistemas aplicativos e da informação.			
	Controle	**GAP**	**Justificativa**
A.12.5.1	Procedimento para controle de mudanças	NÃO	Os procedimentos para gestão de mudanças são inexistentes.
A.12.5.2	Análise crítica técnica das aplicações após mudanças no sistema operacional	NÃO	Os procedimentos de monitoramento para concretizar uma mudança de ambiente são inexistentes.
A.12.5.3	Restrição sobre mudanças em pacotes de software	PARCIAL	Existem controles implantados pelo terceiro, mas é necessário melhorar este nível de controle.
A.12.5.4	Vazamento de informações	NÃO	Não existem controles implantados.
A.12.5.5	Desenvolvimento terceirizado de software	PARCIAL	Melhorar e documentar os procedimentos de acompanhamento no desenvolvimento de softwares por terceiros.

A.12.6 Gestão de vulnerabilidades técnicas			
Objetivo: Reduzir riscos resultantes da exploração de vulnerabilidades técnicas conhecidas.			
	Controle	**GAP**	**Justificativa**
A.12.6.1	Controle de vulnerabilidades técnicas	NÃO	Não existem softwares de apoio às atividades implantadas, no entanto, os procedimentos precisam ser documentados.

Tabela 13 - Gestão de incidentes de segurança da informação

A.13 Gestão de incidentes de segurança da informação			
A.13.1 Notificação de fragilidades e eventos de segurança da informação			
Objetivo: Assegurar que fragilidade e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil.			
	Controle	**GAP**	**Justificativa**
A.13.1.1	Notificação de eventos de segurança da informação	NÃO	Inexistência de procedimento formal.
A.13.1.2	Notificando fragilidades de segurança da informação	NÃO	Inexistência de procedimento formal.
A.13.2 Gestão de incidentes de segurança da informação e melhorias			
Objetivo: Assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes de segurança da informação.			
	Controle	**GAP**	**Justificativa**
A.13.2.1	Responsabilidades e Procedimentos	NÃO	Processo não formalizado.
A.13.2.2	Aprendendo com os incidentes de segurança da informação	NÃO	Processo não formalizado.
A.13.2.3	Coleta de evidências	NÃO	Processo não formalizado.

Tabela 14 - Gestão da continuidade do negócio

A.14 Gestão da continuidade do negócio			
A.14.1 Aspectos da gestão de continuidade do negócio, relativos à segurança da informação *Objetivo:* Não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso.			
	Controle	**GAP**	**Justificativa**
A.14.1.1	Incluindo segurança da informação no processo de gestão da continuidade de negócio	NÃO	Plano de Continuidade de Negócios não foi elaborado.
A.14.1.2	Continuidade de negócios e análise/avaliação de risco	NÃO	Plano de Continuidade de Negócios não foi elaborado.
A.14.1.3	Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação	NÃO	Plano de Continuidade de Negócios não foi elaborado.
A.14.1.4	Estrutura do plano de continuidade do negócio	NÃO	Plano de Continuidade de Negócios não foi elaborado.
A.14.1.5	Testes, manutenção e reavaliação dos planos de continuidade do negócio	NÃO	Plano de Continuidade de Negócios não foi elaborado.

Tabela 15 - Conformidades

A.15 Conformidades			
A.15.1 Conformidade com requisitos legais *Objetivo:* Evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação.			
	Controle	**GAP**	**Justificativa**
A.15.1.1	Identificação da legislação vigente	NÃO	Processo não formalizado.
A.15.1.2	Direitos de propriedade intelectual	NÃO	Processo não formalizado.
A.15.1.3	Proteção de registros organizacionais	NÃO	Processo não formalizado.
A.15.1.4	Proteção de dados e privacidade da informação pessoal	NÃO	Processo não formalizado.

A.15.1.5	Prevenção de mau uso de recursos de processamento da informação	NÃO	Processo não formalizado.
A.15.1.6	Regulamentação de controles de criptografia	NÃO	Processo não formalizado.
A.15.2 Conformidade com normas e política de segurança da informação e conformidade técnica *Objetivo:* Garantir a conformidade dos sistemas com as políticas e normas da organização de segurança da informação.			
A.15.2.1	Conformidade com as políticas e normas de segurança da informação	NÃO	Processo não realizado.
A.15.2.2	Verificação da conformidade técnica	PARCIAL	Sendo executado durante o projeto de Diagnóstico de TI.
A.15.3 Considerações quanto à auditoria de sistemas de informação ***Objetivo:*** Maximizar a eficácia e minimizar a interferência no processo de auditoria dos sistemas de informação.			
A.15.3.1	Controles de auditoria de sistemas de informação	NÃO	Procedimentos ainda não definidos.
A.15.3.2	Proteção de ferramentas de auditoria de sistema de informação	NÃO	Procedimentos ainda não definidos.

9.4. Conclusão

A NBR ISO/IEC 27001 contém 133 controles que foram avaliados para identificar a sua necessidade no ambiente da Prefeitura Municipal de Tijucas do Sul. Destes controles, apenas 07 (sete) foram considerados como não aplicáveis. Um resumo da situação geral dos controles é apresentado de forma geral no gráfico abaixo:

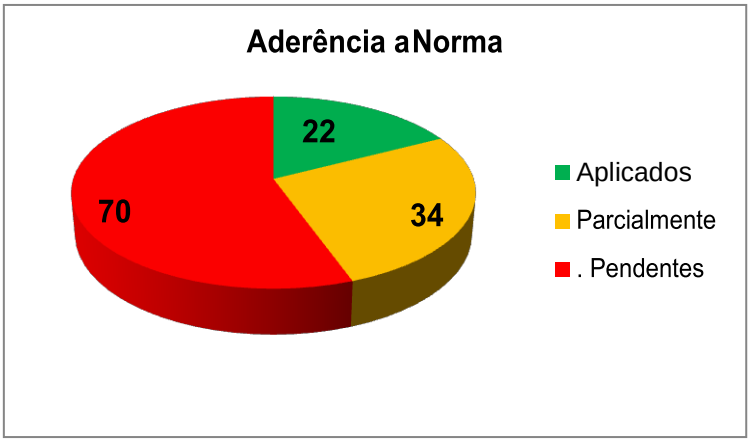


Figura 76 - Resultado da GAP Análise

O resultado representado na figura acima equivale percentualmente a:

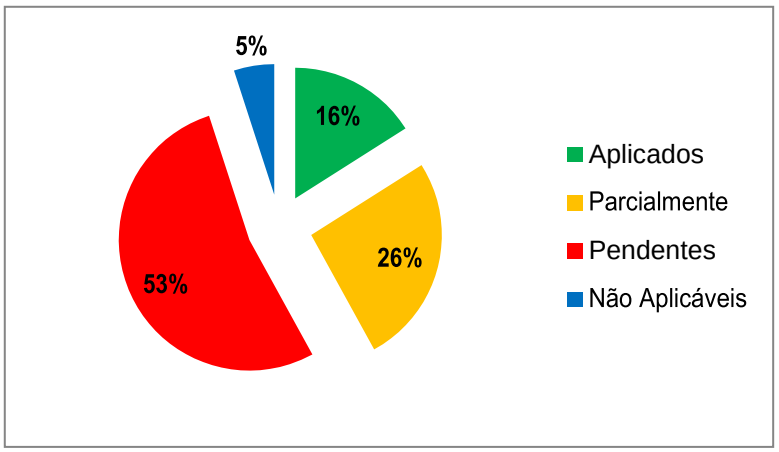


Figura 77 - Percentual de Aderência

CAPÍTULO III – PLANO DE AÇÃO DE TECNOLOGIA DA INFORMAÇÃO

1. INTRODUÇÃO

Este plano de ação complementa o “Diagnóstico de Tecnologia da Informação”, por meio de descrições detalhadas do ambiente, e permitiu a elaboração de uma proposta para endereçar os pontos frágeis do ambiente de tecnologia da informação.

O “Plano de Ação” consiste em uma proposta para melhoria do ambiente atual, considerando um horizonte de 03 (três) anos, e o respectivo plano de ação para a implantação do projeto.

Vale ressaltar que a seção de diagnóstico apresentou recomendações pontuais, listadas isoladamente para cada recurso computacional analisado. Já este Plano de Ação endereça as inúmeras recomendações pontuais de tecnologia da informação decorrentes das fraquezas encontradas, por meio de projetos classificados conforme sua prioridade, complexidade e níveis de investimento.

Os projetos apresentados justificam-se na medida em que, apesar de todos os esforços despendidos pela equipe de tecnologia da informação da Prefeitura para manter o ambiente de TI operacional e atualizado, diversos equipamentos já se encontram em situação iminente de obsolescência.

Tal situação, aliada ao fato de que a Prefeitura vem tornando seus negócios cada vez mais dependentes da tecnologia da informação, indica a necessidade de uma intervenção rápida na direção da atualização do parque tecnológico.

Deixar de executar e investir nas ações ora propostas irá expor a Prefeitura à sérias ameaças como: perda de informações, paralisações não programadas dos sistemas e gargalos de desempenho, além de estagná-la em direção ao desenvolvimento e crescimento dos serviços prestados.

2. CLASSIFICAÇÃO

Cada projeto sugerido neste plano de ação será classificado conforme os seguintes critérios:

- Prioridade;
- Complexidade;
- Investimento.

3. PRIORIDADE

Prioridade Baixa – São atividades que não necessitam de intervenção imediata ou por possuírem processos que, embora não sendo os ideais atendam ao menos parte das

necessidades inerentes à atividade ou por serem processos novos os quais, embora tenham alto potencial para agregação de valor, não são vitais à empresa. No entanto, sua relevância recomenda que a empresa mantenha em mente a necessidade de sua implantação em médio prazo.

Prioridade Média – Compreende atividades que, embora não sejam tão prioritárias quanto às enquadradas no item anterior, devem ser alvo de esforços consistentes na direção de sua implantação assim que for possível, basicamente em função das mesmas razões mencionadas anteriormente, mas que apresentam menor impacto.

Prioridade Alta – Compreende atividades que devem ser realizadas prioritariamente em função da situação precária encontrada, ou em função da baixa complexidade para implantação face ao retorno esperado, ou ainda em função da importância do projeto para o direcionamento estratégico da Tecnologia da Informação como um todo.

4. COMPLEXIDADE

Complexidade Baixa – Projetos e atividades com baixo grau de complexidade não demandam mão-de-obra com elevado grau de especialização, podendo ser executadas na maioria das vezes por técnicos da própria equipe de Tecnologia da Informação da Prefeitura e que, por conseguinte, têm prazos curtos para execução, geralmente inferiores a 45 dias.

Complexidade Média – Tarefas de nível médio de complexidade demandam maior conhecimento técnico e planejamento, requerendo o envolvimento de profissionais mais experientes e com maior vivência, podendo ou não necessitar de contratação de terceiros. São projetos de escopo mais ampliados que normalmente necessitam de um cronograma de execução entre 45 e 120 dias.

Complexidade Alta – Projetos de alto grau de complexidade são projetos elaborados e de longo prazo, que normalmente são executados em etapas e necessitam do envolvimento de profissionais altamente especializados e qualificados em seu processo de concepção e gerência. Em função de sua complexidade, normalmente possuem prazos de execução dilatados, acima de 120 dias, e necessitam de serviços de terceiros.

5. INVESTIMENTO

Investimento Baixo – Investimento com custo total inferior ou igual a R$ 30.000,00;

Investimento Médio – Investimento com custo total entre R$ 30.001,00 e R$ 150.000,00;

Investimento Alto – Investimento com custo total superior a R$ 150.001,00.

Estes dados foram considerados empiricamente, tomado como base o teto orçamentário anual da Unidade de Tecnologia da Informação de uma prefeitura de mesmo porte. Isto posto, são apresentados como projetos de atualização e modernização da estrutura de Tecnologia da Informação da Prefeitura:

Tabela 6 - Legenda de Investimentos

Coluna	Descrição
PRI	Prioridade para execução: Alta, Média ou Baixa
COM	Complexidade de implementação: Alta, Média ou Baixa
INV	Investimento estimado: Alta, Média ou Baixa

Tabela 7 - Relação de Projetos

Item	Projeto	PRI	COM	INV
1	Rede Física e Cabeamento	Alta	Média	Alta
2	Rede Lógica Cabeada	Alta	Média	Média
3	Rede Sem Fio Indoor	Alta	Baixa	Baixa
4	Firewall de Perímetro Internet	Alta	Média	Baixa
5	Proxy Web e Controle de Conteúdo	Alta	Média	Baixa
6	Controle de Acesso à Rede (NAC)	Média	Alta	Média
7	Solução de Cópias de Segurança (Backup)	Alta	Média	Baixa
8	Atualização de Servidores e Estações	Alta	Média	Alta
9	Solução de Armazenamento (Storage)	Alta	Alta	Média
10	Inventário	Média	Alta	Baixa
11	Monitoramento	Alta	Alta	Baixa
12	Correlacionado de Eventos	Média	Alta	Alta
13	Sistema de Colaboração	Alta	Média	Baixa
14	Política de Segurança	Alta	Alta	Baixa

15	Plano de Continuidade	Alta	Alta	Baixa
16	Internet para Todos	Alta	Alta	Alta
17	Solução de Segurança Monitoramento Urbano (CFTV)	Alta	Alta	Alta

6. PREMISSAS PARA PROPOSIÇÕES

O projeto de uma nova solução, para a qual os fornecedores deverão apresentar as suas propostas, deve-se tomar como base de desenvolvimento as seguintes premissas:

- **Requisitos do Negócio:** A arquitetura da solução foi concebida de modo a atender as atuais e futuras demandas da Prefeitura, salvo o surgimento de novas demandas não previstas durante a fase de elaboração do projeto.
- **Escalabilidade:** Os requisitos mínimos de hardware devem ser calculados tendo como meta suportar o crescimento das atuais aplicações e de novas demandas pelos próximos quatro anos, salvo mudanças radicais no mercado de tecnologia da informação.
- **Continuidade:** Os requisitos mínimos de hardware e software devem ser especificados tendo como base avaliações e tendências do mercado de TI para os próximos quatro anos.
- **Redundância:** Elementos críticos da solução deverão preferencialmente estar configurados em redundância, provendo alta-disponibilidade entre os nós que o compõem.
- **Especificação Técnica:** Equipamentos como hardware devem ser apresentados com especificação técnica detalhada, tais como:
- Tecnologia e Plataforma de Hardware;
- Finalidade/Função do Hardware;
- Níveis e Indicadores de Desempenho (CPU, Memória, Discos, Controladoras, Barramento Interno, Rede, etc.);
- Níveis de Redundância Interna;
- Escalabilidade;
- Compatibilidade (Ambiente do Cliente e Soluções de Mercado);
- Continuidade Tecnológica;
- Condições de Garantia e Suporte.

- **Garantia e Suporte:** Os hardwares ou softwares adquiridos devem incluir garantia e suporte pelo período de três anos, no mínimo.
- **Compatibilidade**: Os hardware e softwares adquiridos deverão ser compatíveis com padrões e especificações abertas do mercado, além do legado atual da Prefeitura.

7. PROJETOS

7.1. Infraestrutura Física e Lógica da Rede

Uma infraestrutura física de tecnologia da informação adequada é fundamental para garantir a eficiência dos serviços providos por sistemas automatizados, oferecendo condições ideais de segurança e disponibilidade para acomodação de equipamentos de tecnologia da informação.

Diante da atual condição em que se encontra, deve ser dada atenção especial a reformulação do Data Center para que as ações propostas neste plano reflitam em mudanças efetivas e práticas.

Para este trabalho de reformulação do Data Center é prudente a contratação de consultoria especializada em projetos de implantação de Data Centers para que possam ser avaliadas as condições mínimas aceitáveis.

7.2. Rede Física e Cabeamento

A estrutura de comunicação de uma organização é fundamental para a melhoria de processos administrativos e redução de custos operacionais. A Prefeitura necessita de atualização tecnológica em sua infraestrutura de rede física para assegurar mais estabilidade e rigor metodológico na comunicação de dados, além de preparar sua infra-estrutura para as novas tecnologias de comunicação emergentes.

Com o crescimento das plataformas de transmissão de dados, crescimento do quadro de agentes públicos e aumento da demanda por serviços eletrônicos, passou-se a exigir um constante aumento, tanto na abrangência, quanto na capacidade da rede atual, mostrando assim, uma deficiência do sistema existente e expondo a necessidade de uma

nova infraestrutura planejada. Este projeto deverá satisfazer, no mínimo, os seguintes objetivos:

- Garantir segurança física dos equipamentos de tecnologia da informação e consequentemente, a proteção física contra acesso indevido;
- Garantir o condicionamento adequado dos equipamentos de tecnologia da informação para o provimento de suas funções;
- Prevenir desastres no ambiente de tecnologia da informação causados por fenômenos naturais ou falhas humanas;
- Estender o espaço disponível para os funcionários dentro da Unidade de Tecnologia da Informação;
- Reformular toda a estrutura de cabeamento de dados vertical e horizontal;

O Data Center e a rede cabeada da Prefeitura deverão passar por uma reestruturação levando-se em consideração as seguintes premissas:

- Reformular o posicionamento da sala do Data Center ampliando a área de trabalho da Unidade de Tecnologia da Informação, mantendo-se as mesmas dimensões atuais;
- Comportar um sistema de refrigeração com múltiplas unidades de ar-condicionado com capacidade combinada de refrigeração para manter a temperatura e umidade nas condições ideais dos equipamentos, com unidades redundantes suficientes e monitoramento online via rede;
- Prover um sistema de gerador elétrico dimensionado para controlar todas as cargas do Data Center;
- Acomodar ao menos 02 (dois) racks com sistema de ventilação para ativos de rede e servidores no Data Center, reorganizando e adaptando o cabeamento vertical e horizontal atualmente existente;
- Acomodar os sistemas de estabilização e nobreaks em uma sala separada do Data Center para evitar a geração de interferência por parte de campos elétricos;
- Implantar sistema de vídeo monitoramento IP com câmeras IP dentro do Data Center;

- Implantar um sistema de detecção de fumaça e combate a incêndios com monitoramento por software e geração de alertas sonoro, via e-mail e mensagens SMS;
- A sala deverá dispor de piso elevado com ao menos 180 mm de profundidade para passagem de cabeamento horizontal;
- Ampliar e readequar a estrutura de cabeamento horizontal e vertical da estrutura predial em etapas, porém em um projeto escalar e levando em consideração os gargalos existentes atualmente;

7.2.2. Rede Lógica Cabeada

A infraestrutura lógica da rede é parte essencial para a manutenção da disponibilidade, integridade e confidencialidade dos dados. O atual parque de ativos de tecnologia da informação e a topologia da rede de dados não fornecem as condições mínimas necessárias para o provimento de serviços de tecnologia, por deficiência de desempenho, funcionalidades e tolerância a falhas.

Por isso julga-se emergencialmente necessária a reformulação da infraestrutura de rede lógica, através da substituição total dos ativos de rede e formulação das disposições lógicas ideais por meio de segmentação, roteamento, controle de acesso, autenticação e monitoramento.

A rede de dados da Prefeitura deverá ser reformulada, por meio de um projeto técnico considerando-se a topologia abaixo e as seguintes premissas:

- Não deverá ser reaproveitado nenhum componente do atual parque de equipamentos de borda e core de rede;
- O core da rede deverá atender com no mínimo 48 pontos de rede Gigabit para servidores e ativos;
- As bordas deverão atender no mínimo 192 pontos de rede Gigabit Ethernet para estações de trabalho e impressoras;
- Deve ser priorizada conexões de uplink com fibra-ótica multimodo entre o core da rede e os switches de borda;

7.3. Rede Sem Fio Indoor

As redes sem fio “são soluções normalmente aplicadas onde uma infraestrutura de cabeamento convencional (cobre ou fibra óptica) não pode ser utilizada”[1]. Este tipo de rede pode atender a diversos pontos de acesso com a mesma, ou até melhor eficiência que as redes cabeadas. Podendo, em alguns casos apresentar, incondicionalmente, melhor custo/benefício principalmente devido as restrições físicas e orçamentárias.

A flexibilidade da rede sem fio possibilita a mudança de layout uma vez que, quando é necessário modificar uma rede cabeada, é necessário um esforço muito maior, pois há a necessidade de estudo da distância entre os ativos, comprimento de cabos e espaço físico disponível. O projeto da rede sem fio indoor deverá satisfazer, no mínimo, os seguintes objetivos:

- Prover conectividade flexível de baixo custo e de alta segurança para computadores dispostos em locais sem infraestrutura de rede cabeada;
- Reduzir a necessidade de readequação do cabeamento da rede de dados em virtude de mudanças de layout;
- Garantir acesso à Internet para notebooks e demais aparelhos portáteis utilizados em salas de treinamento, em auditórios e salas de secretários e prefeito;
- Garantir a utilização de um ponto de acesso entre redes e usuários distintos sem interferência.

A implantação de rede sem fio corresponderá a cobertura de rede sem fio em áreas onde não há enlaces de rede cabeada, em locais onde a infraestrutura física predial não comporta a expansão de cabos para rede de dados e onde se pretende atender a necessidade de acesso de visitantes. A proposta de implantação da rede sem fio da Prefeitura por meio da disseminação de sinal de rádio frequência apresenta as seguintes premissas:

- Serão cobertas áreas como salas de treinamento, auditórios e salas de secretários e prefeito;

[1] http://www.brzcode.com.br/p/servicos-solucoes/-wireless (acesso em 25/06/2020)

- A infraestrutura deverá ser capaz de ser ampliada para demais áreas e locais da Prefeitura;
- Salas como auditórios e salas de treinamento deverão apresentar total independência para o acesso à Internet, sem qualquer conectividade com a rede da Prefeitura;
- Todas as estações de trabalho ou notebooks que desejam ingressar na rede sem fio deverão possuir de interface sem fio 802.11 a/b/g/n (Dual-Band);
- Será necessário o levantamento de locais para fixação dos equipamentos, alimentação elétrica e conectividade com a rede cabeada;
- Os pontos de acesso deverão contar com tecnologia PoE para sua energização, a fim de otimizar a implantação e realocação dos pontos de acesso;
- Será necessária a realização de Site Survey para avaliação do posicionamento ideal dos pontos de acesso;
- Todos os equipamentos deverão ser administrados por meio de uma console única e centralizada;
- A solução deve garantir priorização de acesso aos colaboradores da rede local onde ocorram múltiplos acessos;
- Todos os equipamentos deverão ser administrados por meio de uma console única e centralizada por meio de protocolos seguros (SSL e SSH);
- Os equipamentos devem suportar configuração de perfis de usuários e dispositivos móveis com regras de firewall.

7.4. Segurança Física e Lógica

Vivemos em um mundo globalizado, com o espaço geográfico fragmentado, porém fortemente articulado pelas redes, onde a informação, independente do seu formato, é um dos maiores patrimônios de uma organização moderna, sendo vital para quaisquer níveis hierárquicos e dentro de qualquer instituição que deseja manter-se competitiva no mercado. Considerada um ativo importantíssimo para a realização do negócio a informação deve ser protegida e gerenciada.

Nos últimos anos as tecnologias de informação e comunicação têm evoluído de forma rápida, fazendo com que as organizações tenham maior eficiência e rapidez nas tomadas de decisão, devido a este fato as chances de uma empresa não usar sistemas de informação tornou-se praticamente nula. Neste contexto a importância de se utilizar mecanismos de segurança é vital para a sobrevivência.

Diante da ausência de soluções adequadas de segurança, faz-se necessário a implantação de um conjunto de soluções de segurança que atendam os seguintes objetivos:

- Prevenir ataques à rede corporativa com proteção para o acesso de sistemas corporativos publicados para a Internet;
- Controlar o fluxo de entrada e saída de tráfego de dados entre as redes remotas (secretarias), a Internet, e a rede interna da Prefeitura;
- Promover maior desempenho no acesso à Internet, com segurança apropriada e capaz de detectar ataques modernos;
- Otimizar o uso de conectividade Internet entre as secretarias apenas para tráfego útil ao desempenho das rotinas de trabalho;

7.4.2. Firewall de Perímetro Internet (UTM)

Quando a rede corporativa é conectada à Internet, garantir a segurança contra intrusos passa a ser de importância vital. O método mais efetivo é utilizar um sistema de firewall entre a rede local e a Internet. O firewall certifica que toda comunicação entre a rede corporativa e a Internet esteja em conformidade com a política de segurança definida pela Prefeitura.

Para efetivamente prover uma segurança real, o firewall necessita identificar e controlar o fluxo de informações que passa através dele, para que a partir de uma tomada de decisão possa permitir, rejeitar, encriptar ou logar as tentativas de comunicação.

Um sistema de firewall necessita obter, armazenar, recuperar e manipular informações derivadas de todas as camadas de comunicação e de outras aplicações. Firewalls são responsáveis pela tarefa de cuidar para que o tráfego não desejado ou não autorizado com origem em uma rede "promíscua", como é o caso da Internet, não atinja o

segmento de rede privado (Prefeitura) sem validação e inspeção.

A solução de segurança de perímetro Internet baseada em firewall deverá ser implantada por meio de um projeto técnico considerando-se as seguintes premissas:

- Controlar e segmentar fisicamente o tráfego entre as redes internas, rede DMZ, internet, Prefeitura e redes locais remotas (secretarias);
- Implantar uma rede desmilitarizada (DMZ) onde serão acomodados os servidores com serviços publicados para a internet;
- Integrar funcionalidades de UTM (Unified Theat Management) como IPS/IDS, Anti-spam, Anti-vírus, Anti-spyware e Controle de Conteúdo Web;
- Estabelecer tunelamento VPN com outras soluções através do protocolo IPSec ou SSL;
- Atuar preferencialmente em modo Ativo/Passivo para assegurar persistência e manutenção da conectividade em situações de falhas;
- Assegurar “Zero Downtime“ durante o Failover de um dos membros do cluster de alta-disponibilidade;
- Garantir a replicação automática das configurações entre os membros do cluster de alta-disponibilidade;
- Permitir o gerenciamento centralizado de todas as camadas, com funcionalidades de UTM aplicada às regiões de segurança monitoradas.
- Permitir a configuração integrada do serviço de diretório local com a funcionalidade de Single Sign-On;

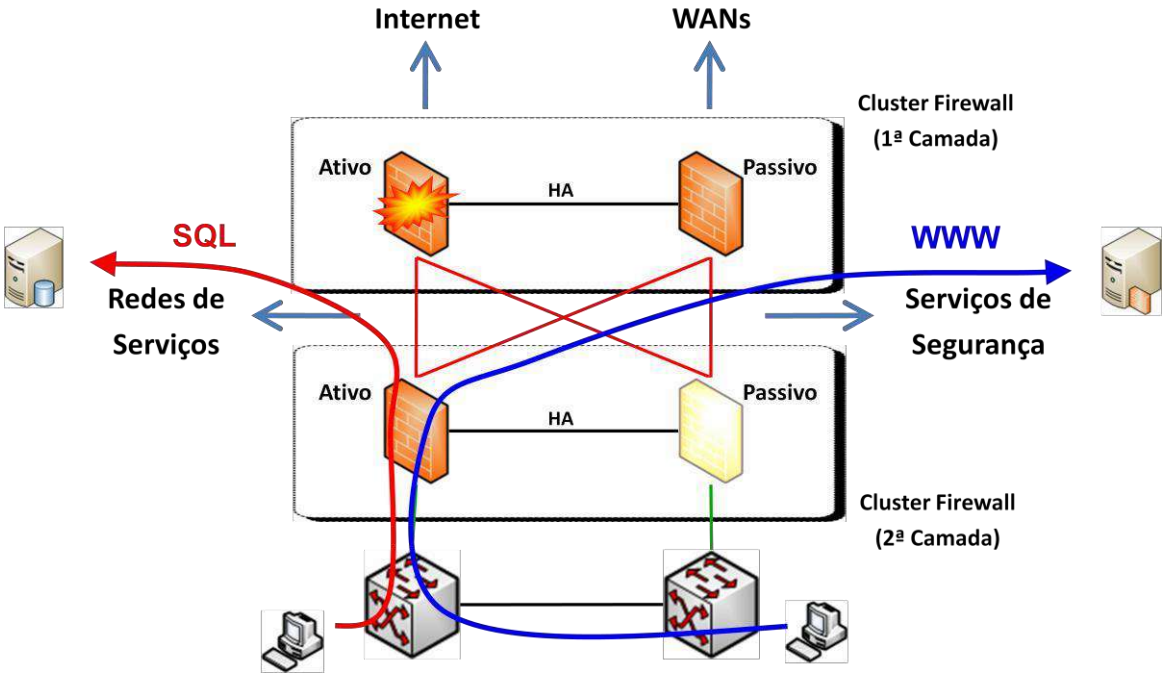


Figura 78 - Topologia de Firewall de Perímetro

7.4.3. Acesso Remoto Seguro

No atual ambiente, onde funcionários estão sempre em movimento, a capacidade de acessar informações essenciais a partir de qualquer lugar não é um luxo, mas uma necessidade. Porém, conectar-se à Prefeitura a partir de um café, hotel ou aeroporto nem sempre é um procedimento seguro. Os criminosos on-line estão sempre em busca de novas maneiras de roubar informações confidenciais, como senhas.

Atualmente existem soluções simples de implantar e gerenciar, que oferecem acesso remoto seguro aos recursos da rede para funcionários e prestadores de serviço de forma simples. Facilitando com isso, a implementação do acesso remoto seguro esse tipo de solução ajuda a maximizar o ROI, diminuir os custos de TI e aumentar a segurança da rede. A solução de segurança de acesso remoto seguro deverá ser implantada por meio de um projeto técnico considerando-se as seguintes premissas:

- Acesso remoto seguro com criptografia SSL;
- Acesso remoto assistido para suporte via web;

- Acesso à aplicações, correio eletrônico e arquivos;
- Acesso granular baseado no perfil do usuário/grupo;
- Integração com solução de autenticação forte;
- Sem a necessidade de um cliente de VPN (Clientles);
- Integração com serviço de Diretório e RADIUS;
- Controle de acesso integrado ao End-Point;
- Independe da plataforma utilizado pelo computador.

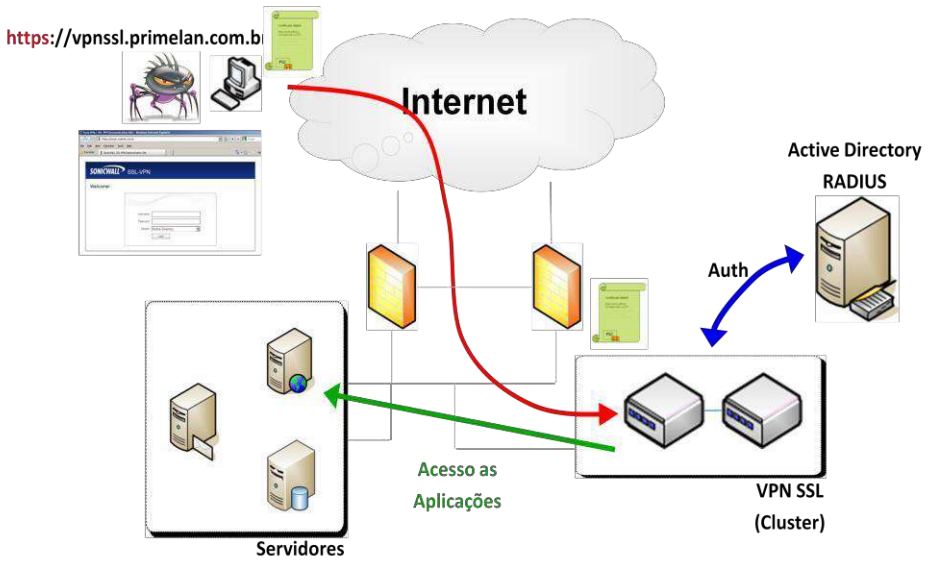


Figura 79 Acesso Seguro

7.4.4. Proxy Web e Controle de Conteúdo

Uma solução de controle de conteúdo web gerencia e controla o uso da Internet em ambientes corporativos, impedindo o acesso dos funcionários a sites considerados inapropriados ou potencialmente perigosos para a Prefeitura. Sua base de dados é constantemente atualizada e leva em conta usos e costumes do acesso a sites tanto no Brasil quanto no mundo.

Integrado ao controle de conteúdo, uma solução proxy web consiste em manter,

em uma área de acesso rápido, informações já acessadas por outros usuários, evitando assim, a retransmissão destas informações e deixando-as disponíveis ao usuário num tempo bem menor. Também conhecido como Web Cache, este tipo de solução é capaz de otimizar a utilização da Internet em até 40%, aproximadamente.

A solução de controle de conteúdo e proxy web integradas, devem ser implantadas por meio de um projeto técnico considerando-se as seguintes premissas:

- A solução deve apresentar funcionalidades de Proxy Reverso para serviços web publicadas na rede interna e na rede DMZ;
- A solução deve ser acomodada com conectividade lógica para a rede DMZ e rede Interna, sob a forma de servidor virtual ou físico;
- A solução deverá contemplar funcionalidades de controle de conteúdo web e não somente análise de URLs;
- Todas as aplicações publicadas e suportadas pelos seus fabricantes deverão ser publicadas por meio da solução Proxy;
- A solução deverá promover a proteção online contra ameaças no tráfego web mais recentes;
- A solução deverá prevenir a utilização de aplicações peer-to-peer, tráfego
- streaming, jogos e Instant Messaging;
- A solução deverá ser capaz de bloquear computadores comprometidos colocando-os em quarentena e também bloquear downloads;
- Deverá gerar relatórios customizados, alertas e notificações de administração da solução;
- Deverá permitir a definição de políticas baseadas em perfis de grupos e usuários.

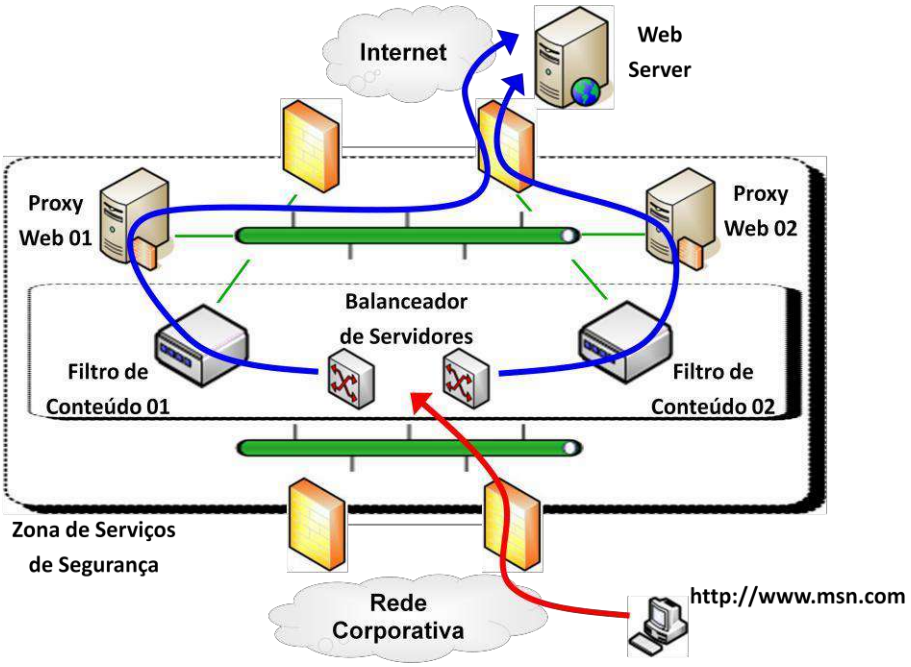


Figura 80 - Topologia de Proxy e Controle de Conteúdo

7.4.5. Controle de Acesso à Rede (NAC)

Uma solução de Controle de Acesso à Rede atua na pré e pós-conexão dos ativos na rede corporativa permitindo aos administradores de TI implementar uma condição que garanta que somente os usuários autorizados tenham acesso à devida informação, no local certo e na hora certa. Os dados ficam protegidos contra acesso indevido, visto que somente pessoas e/ou computadores expressamente autorizados possuem acesso. A solução pode ainda realizar a avaliação de vulnerabilidades e retificação assistida, além de isolar computadores e usuários suspeitos. Para a solução de controle de acesso à rede lógica considerando-se as seguintes premissas:

- Prover autenticação, autorização, conformidade e remediação para usuários de dispositivos em rede;
- Analisar continuamente as ameaças à rede corporativa oriundas de pessoas e máquinas conectadas;

- Manter a capacidade de rastreabilidade e auditorias de todas as conexões na rede;
- Provisionar as aplicações e servidores de forma segura e baseada no perfil de fluxos gerados;
- Isolar dispositivos suspeitos e bloquear dispositivos indesejados, garantindo conformidade dos dispositivos conectados à rede;
- Reduzir a superfície de ameaças geradas por dispositivos conectados internet à rede interna;

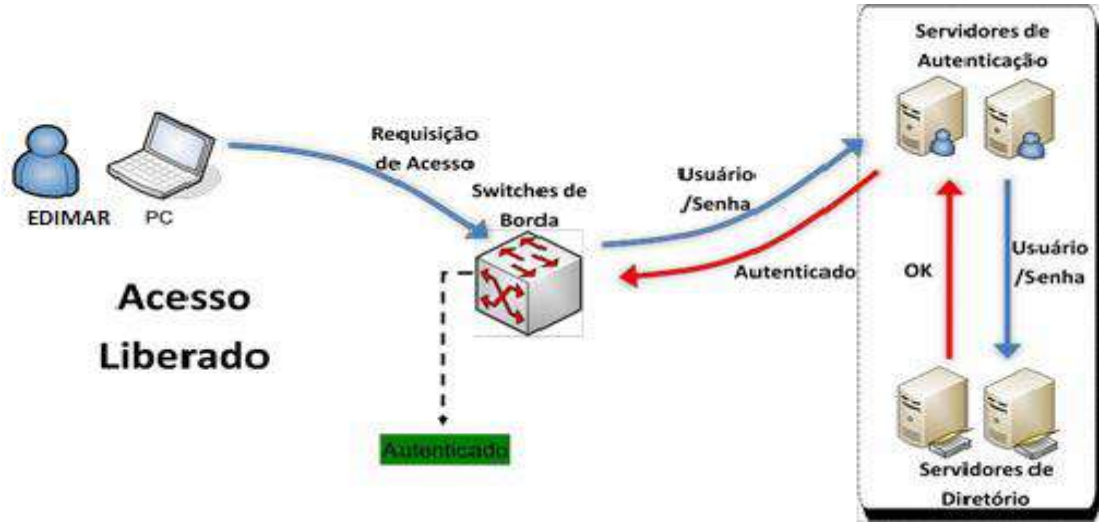


Figura 81 - Topologia de Acesso à Rede com Segurança

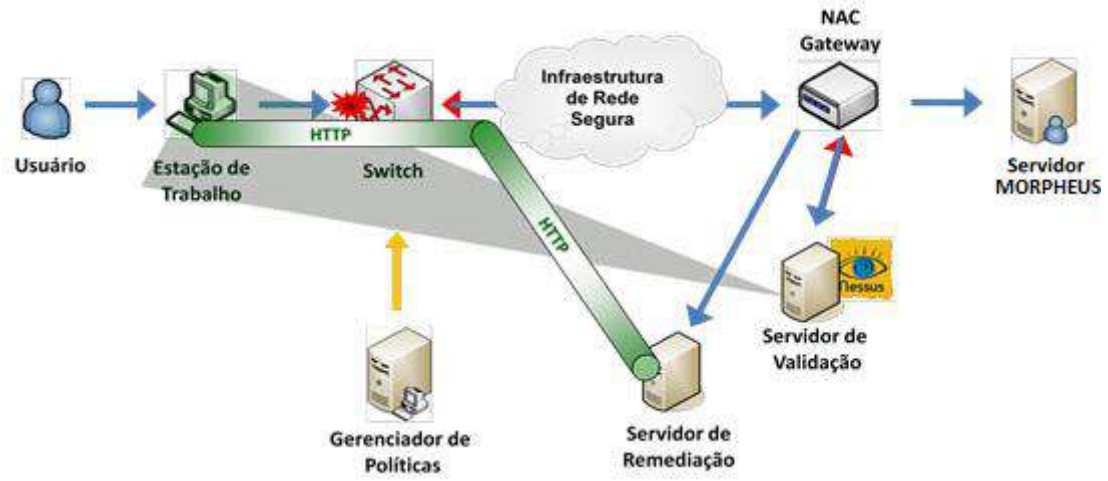


Figura 82 - Fluxo de Comunicação Seguro

7.4.6. Solução de Cópias de Segurança (Backup)

Atualmente os sistemas corporativos requerem soluções de backup cada vez mais velozes, flexíveis e confiáveis, preparadas para atender uma multiplicidade de plataformas. Essa necessidade de garantir a integridade e a segurança da informação é tão grande que os profissionais de redes não podem contar apenas com simples sistemas de armazenamento, necessitando utilizar recursos mais eficientes como os sistemas de backup corporativo. Este projeto deverá satisfazer, no mínimo, os seguintes objetivos:

- Promover a segurança dos dados por meio da disponibilidade de cópias de segurança;
- Implantar processos de controle e gerenciamento pró-ativo de cópias de segurança;
- Assegurar o retorno de arquivos e sistemas de negócio dentro de prazos e condições aceitáveis;
- Dentro do projeto técnico para atendimento as necessidades da prefeitura deverão constar como premissas:
- Fornecimento de hardware e software adequados para as necessidades emergentes da Prefeitura;
- A solução deverá atender tanto a sistemas operacionais Windows quanto Linux para no mínimo 9 servidores;
- Deverá levar em consideração a realização de backups que somam um volume de até 15 Tb sem compreensão;
- A solução em software deverá ser fornecida com agentes para Ambiente de Diretóio, Banco de Dados, Virtualização, File Server e Sistemas Operacionais;
- A solução deverá envolver uma Tape Library ou uma Auto Loader, não podendo ser

atendido com apenas uma Tape Drive;

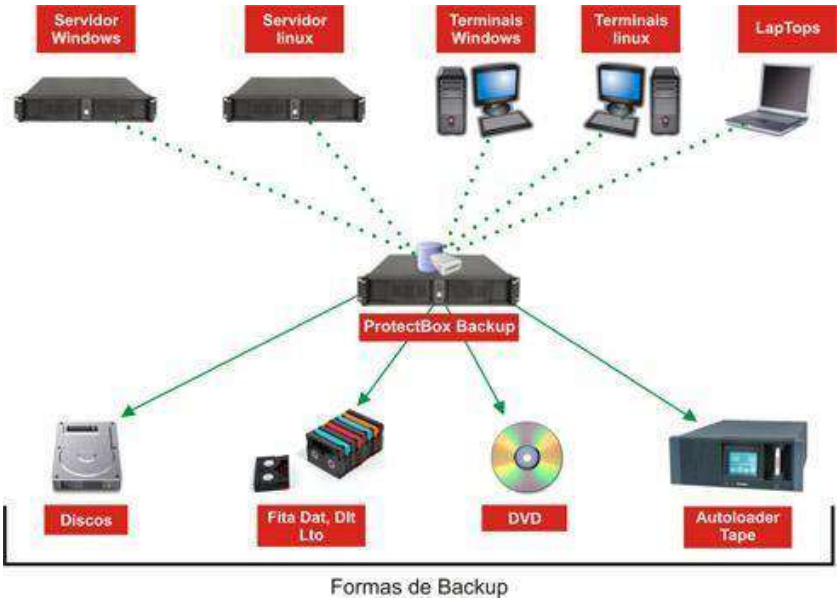


Figura 83 - Segurança Backup

7.5. Servidores, Estações e Armazenamento

7.5.1. Atualização de Servidores e Estações

Objetiva a reestruturação e homogeneização do parque de servidores e estações de trabalho através da aquisição ou aluguel destes ativos. Com isso, a Prefeitura contará diretamente com suporte/garantia, que por consequência estarão atrelados aos novos equipamentos. Essa estratégia diminuirá, e muito, o tempo de reposição de peças e indisponibilidade dos pontos de atendimento à população, por exemplo.

Outro fator importante é a estratégia de consolidação dos servidores em ambiente virtualizado, onde se origina do particionamento que divide um único servidor físico em múltiplos servidores lógicos. Depois que o servidor físico é dividido, cada servidor lógico pode rodar um sistema operacional e aplicativos de maneira independente, trazendo diretamente os seguintes benefícios:

- Aumento de serviço com um número menor de servidores físicos, economizando o custo total de hardware, eletricidade e manutenção;

- Menos servidores físicos para monitorar;
- Menor complexidade da infraestrutura física;
- Permite operar múltiplos sistemas a partir de uma única infraestrutura tecnológica.

Figura 84 - Consolidação de Servidores (Virtualização)

7.5.2. Solução de Armazenamento (Storage)

Hoje, as empresas enfrentam mais desafios relacionados ao storage do que jamais se viu antes. Enquanto isso, o storage vem se tornando cada vez mais complexo no data center. Para a maioria das empresas, o conceito de storage deixou de ser apenas algo relacionado à infraestrutura de TI e passou a interessar os gerentes de nível mais alto de toda a organização. A importância do storage aumentou por diversos motivos, entre eles a consolidação de recursos de tecnologia, redução de custos, conformidade com as novas leis regulatórias e com a natureza sempre presente do atual modelo de aplicativos para o cliente, ativo 24 horas por dia, todos os dias. A demanda de storage continua crescendo, por isso, as empresas de TI são chamadas a fazer mais com muito menos. Este projeto deverá satisfazer, no mínimo, os seguintes objetivos:

- Otimizar a utilização de recursos de armazenamento evitando desperdício;
- Assegurar tolerância a falhas para sistemas de missão crítica;
- Atender a demanda crescente por armazenamento não-volátil;

- Proporcionar maior desempenho para sistemas corporativos;
- Reduzir a complexidade de gestão de espaço em discos e reduzir o potencial de falhas;
- Conceder, mediante controle permissionário, local para armazenamento centralizado de arquivos de ordem corporativa.

A solução de armazenamento deverá assumir as seguintes premissas:

- A solução de hardware/software deverá atender a convergência de tecnologia SAN e NAS no mesmo equipamento;
- A solução deve compreender a implantação de uma rede de armazenamento (Storage) com protocolo de comunicação ISCSI;
- Os bancos de dados atualmente armazenados em discos locais de servidores devem ser migrados para o Storage, assim como as bases de dados;
- A solução deverá atender com pelo menos 14 (nove) TB para acomodação de bancos de dados, arquivos, virtualização, backups e snapshots;
- Arquivos corporativos deverão ser armazenados no storage e controlados por meio de permissões baseadas em grupo.

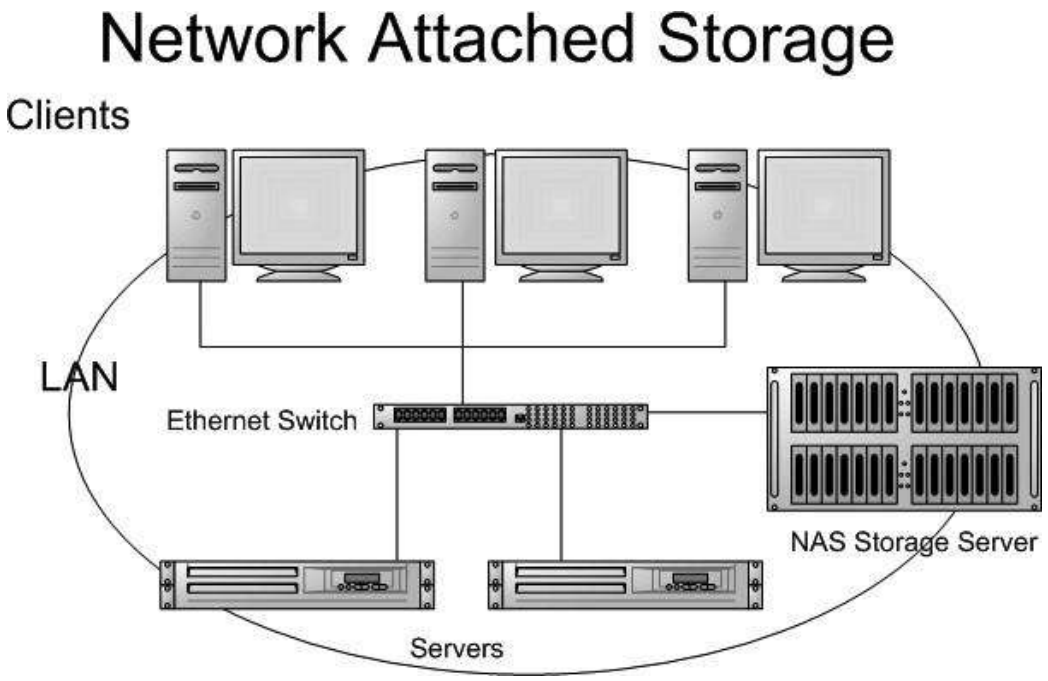


Figura 85 - Topologia de Storage

7.6. Monitoramento, Gerenciamento e Inventário

7.6.1. Inventário

Uma solução de inventário é projetada para atender a demanda de diversos ambientes de rede. Ela deve reunir dados abrangentes de software e hardware de qualquer computador executando qualquer sistema operacional e também de ativos de rede. Uma variedade de opções de distribuição e coleção de dados garantem que a solução trabalhe em qualquer ambiente.

Para ajudar a maximizar o investimento, a solução deve ir além de uma simples obtenção de dados. Ao fornecer um console de gerenciamento, diretivas para alertá-lo sobre informações críticas, e relatórios com qualidade profissional, a solução também devem incluir as ferramentas necessárias para transformar dados de inventário em informações úteis.

A solução deve fornecer inventário abrangente para computadores e ativos de rede, incluindo número de série, inventário de hardware, inventário de auditoria de software, máquina virtual, e informações de usuário/contato quando aplicável. Assim, a solução de

inventário deverá considerar as seguintes premissas para desenvolvimento do projeto:

- Deve apresentar precisão em relatórios para apoio na tomada de decisões a partir de dados concretos, com um inventário abrangente de sistemas em servidores e estações de trabalho;
- A solução deverá incluir inventário tanto para servidores e estações de trabalho quanto ativos de rede como switches, Access Points, roteadores e appliances de segurança;
- O projeto de inventário deve identificar e coletar informações de hardware e configurações específicas em servidores através da normalização, consolidação e segurança dos dados em um repositório central e da geração de relatórios com informações detalhadas sobre os ativos.

7.6.2. Monitoramento

Monitorar um ambiente de rede é uma das preocupações mais constantes entre empresas e organizações. Dispor de ferramentas que façam esse controle é fundamental para facilitar o trabalho e identificar imediatamente algum tipo de erro providenciando assim uma ação efetiva.

Um dos aspectos destacados nesse tipo de solução é opção por controle através de gráficos e relatórios, além de alertas pelos quais o administrador pode ter a opção de ser avisado se acontecer qualquer instabilidade na rede, proporcionando um acompanhamento em tempo real dos eventos. A solução de monitoramento deverá considerar as seguintes premissas para desenvolvimento do projeto:

- Solução preferencialmente corporativa para provimento de monitoramento básico de ativos de rede via SNMP;
- Permitir monitoramento básico para switches, roteadores e servidores, verificando o estado do equipamento (ligado/desligado), taxa de transferência das interfaces, throughput do equipamento e processamento;
- Capacidade de envio de alertas sonoros, SMS e e-mails quanto anomalias forem detectadas;
- Capacidade de geração de gráficos sumarizados e relatórios detalhados com

histórico das ocorrências relacionadas a um ativo.

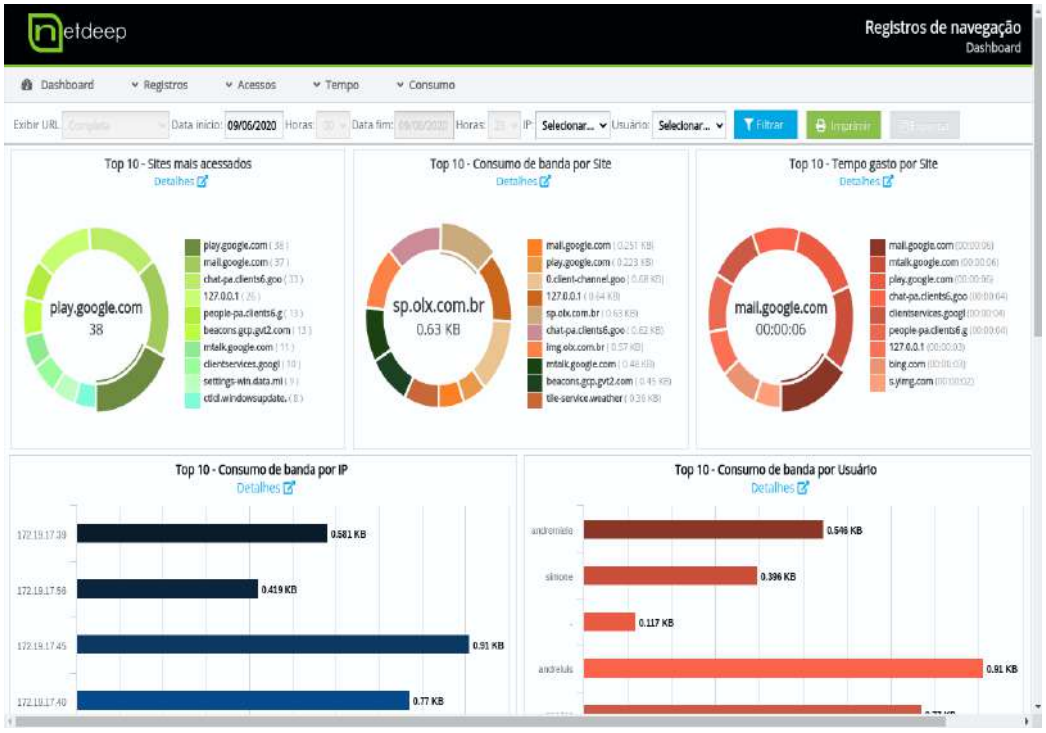


Figura 86 - Monitoramento Firewall

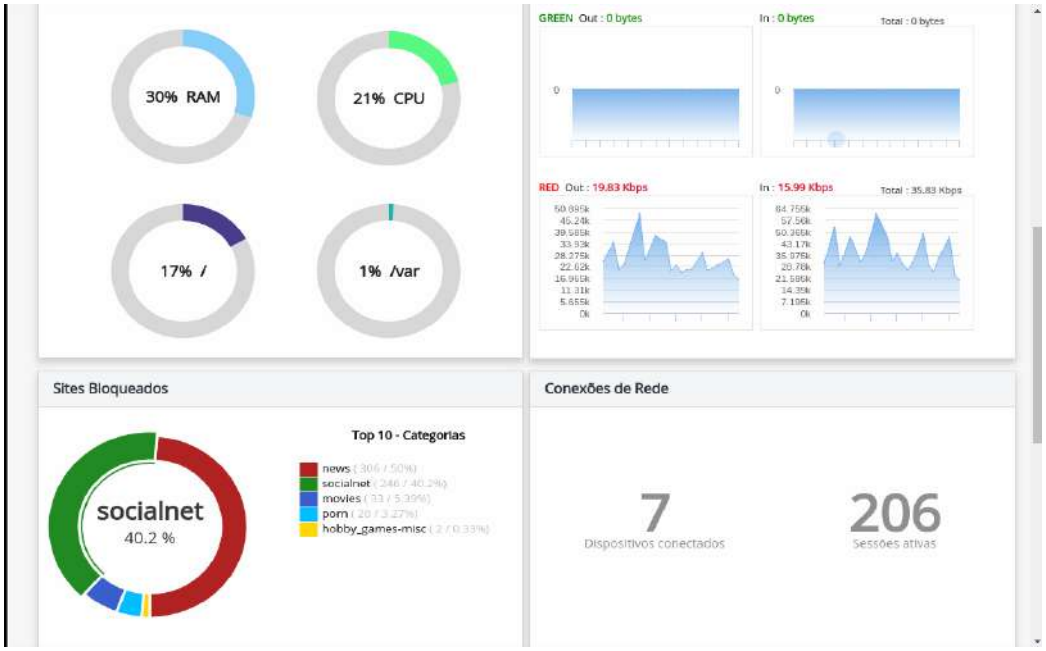


Figura 87 - Monitoramento Firewall

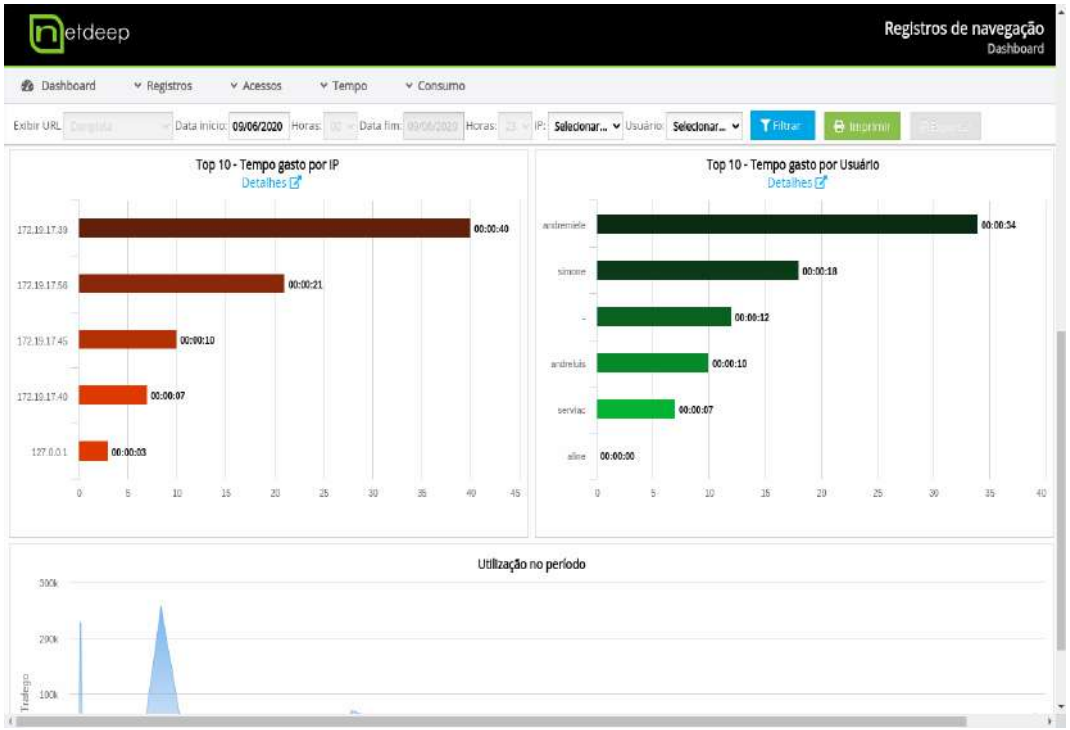
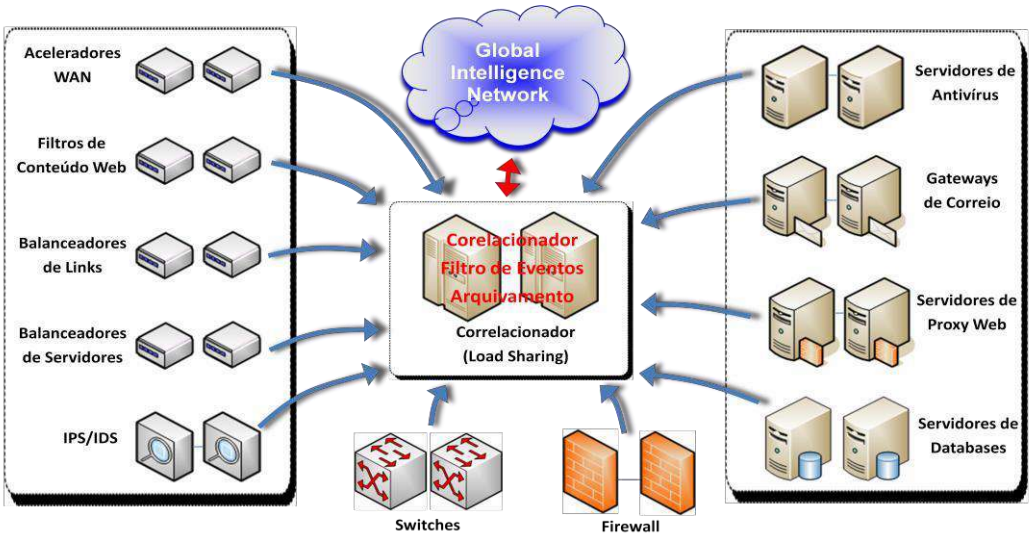


Figura 88 - Monitoramento

7.6.3. Correlacionador de Eventos

Quando ocorre uma falha em algum dos equipamentos existentes em uma rede, vários eventos são gerados, alguns provenientes de equipamentos interligados ao que falhou. Devido ao grande número de eventos gerados pelos vários equipamentos, a localização da falha torna-se uma tarefa difícil de ser realizada. Para diminuir o número de eventos, existe a técnica de correlação que consiste na interpretação conceitual de múltiplos alarmes, levando à atribuição de um novo significado aos alarmes originais, gerando um novo alarme.

O objetivo da correlação é diminuir a quantidade de alarmes transferidos dentro do sistema de gerência de rede, aumentando o conteúdo semântico dos alarmes resultantes. O correlacionado possui um módulo responsável em receber e correlacionar os eventos, o



correlator. O correlacionador utiliza o canal de notificação para propagar os alarmes correlacionados entre vários gerentes, para isso basta o gerente se conectar ao canal existente no correlacionador. Para evitar os eventos que não são de interesse, são utilizados filtros do serviço de notificação.

Figura 89 - Correlacionador de Eventos

7.7. Sistemas Corporativos

7.7.1. Sistema de Colaboração

O software de correio eletrônico surgiu com o objetivo de auxiliar a comunicação e a troca de informações entre as pessoas. Anteriormente ao surgimento do correio eletrônico, os documentos e mensagens eram distribuídos de maneira menos ágil, comparando-se com o trabalho realizado pelos correios ou por outros meios tradicionais.

Cada usuário deste sistema possui um endereço eletrônico conhecido como e-mail e através de programas de computadores que são clientes de e-mail e de servidores de correio eletrônico o usuário recebe e envia mensagens. Desta maneira, com a expansão dos serviços de web, o correio eletrônico tornou-se uma ferramenta muito difundida nas empresas e instituições.

As soluções de colaboração são ainda mais versáteis. Ela foi desenvolvida para responder às necessidades específicas de grupos de trabalho como gestão de projetos, criação colaborativa de documentação e conhecimento, gestão de intervenções e outras,

podendo ser integrado a todos os níveis com a sua plataforma tecnológica atual e com o modelo de trabalho da sua equipe. Integra-se também com sistemas de gestão de identidades, de messaging, de gestão de recursos e outros para permitir à sua organização a partilha de competências, recursos e serviços com parceiros.

7.8. Processos e Políticas

7.8.1. Política de Segurança

O principal propósito de uma política de segurança é informar aos usuários e equipes as suas obrigações para a proteção da tecnologia e do acesso à informação. A política deve especificar os mecanismos através dos quais estes requisitos podem ser alcançados. Outro propósito é oferecer um ponto de referência a partir do qual se possa adquirir, configurar e auditar sistemas computacionais e redes, para que sejam adequados aos requisitos propostos. Portanto, uma tentativa de utilizar um conjunto de ferramentas de segurança na ausência de pelo menos uma política de segurança implícita não faz sentido.

Uma política de uso apropriado (Appropriate - ou Acceptable - Use Policy - AUP) pode também ser parte de uma política de segurança. Ela deveria expressar o que os usuários devem e não devem fazer em relação aos diversos componentes do sistema, incluindo o tipo de tráfego permitido nas redes. A AUP deve ser tão explícita quanto possível para evitar ambiguidades ou maus entendimentos.

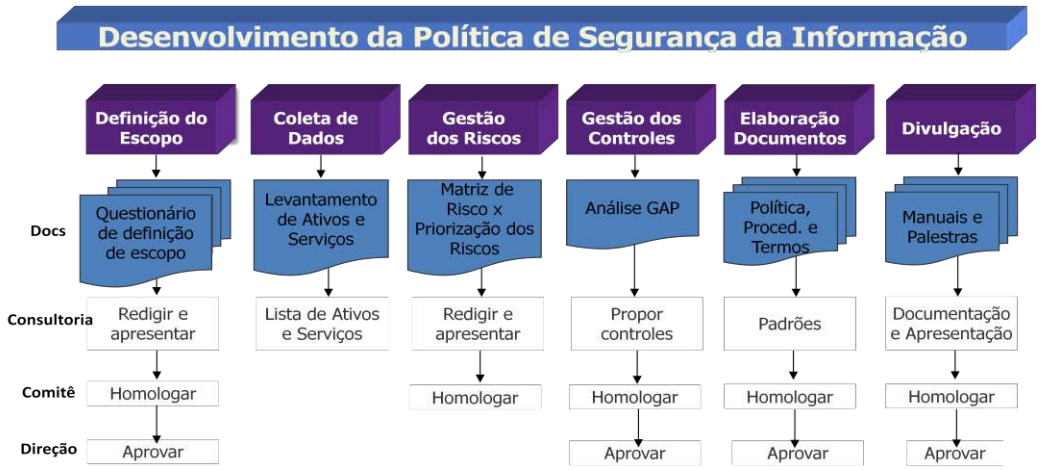


Figura 90 - Fases da Política de Segurança

Para que uma política de segurança se torne apropriada e efetiva, ela deve ter a aceitação e o suporte de todos os níveis de empregados dentro da organização. É especialmente importante que a gerência corporativa suporte de forma completa o processo da política de segurança, caso contrário haverá pouca chance que ela tenha o impacto desejado. As características de uma boa política de segurança são:

1. Ela deve ser implementável através de procedimentos de administração, publicação das regras de uso aceitáveis, ou outros métodos apropriados.
2. Ela deve ser exigida com ferramentas de segurança, onde apropriado, e com sanções onde a prevenção efetiva não seja tecnicamente possível.
3. Ela deve definir claramente as áreas de responsabilidade para os usuários, administradores e gerentes.

7.8.2. Plano de Continuidade de Negócio

A elaboração deste plano envolve todas as atividades necessárias para garantir que todos os processos de negócios críticos da Prefeitura sejam contemplados numa solução de continuidade, que busca o menor custo operacional possível. Existe uma necessidade de ter um Responsável Técnico (RT) no Setor de Tecnologia da Informação da Prefeitura Municipal De Tijucas Do Sul, que seja Servidor de Carreira do Munícipio para que a continuidade do PDTIT seja sempre prioridade na Administração Pública Municipal e que a validação seja via Decreto Municipal. Não é permitido terceiros de outras secretárias assumirem responsabilidade de Técnicas não estando alocado no Setor Tecnologia de Informação, dessa forma evitando desvio de função , problemas técnicos sérios e processos via Ministério Público Paraná .

Para tanto, é levantada toda a infraestrutura de tecnologia da informação e são mapeadas todas as ameaças que podem determinar uma interrupção de atividades. A

adoção de metodologia de continuidade de negócios padrão internacional por consultores de comprovada experiência no assunto, garantem a implantação de um plano eficaz e economicamente viável.

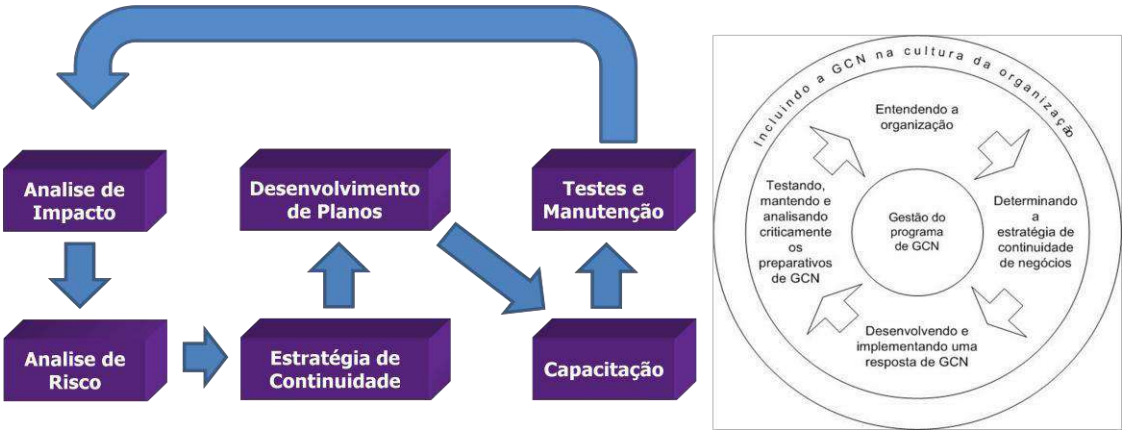


Figura 91 - Ciclo do Plano de Continuidade de Negócios

Os benefícios de um plano de continuidade se resumem a:

- Identificação proativa dos impactos de uma interrupção operacional;
- Resposta eficiente às interrupções, minimizando o impacto à organização;
- Capacidade de gerenciar os riscos que não podem ser segurados;
- Demonstra uma resposta possível por meio de um processo de testes;
- Proteger a marca, a reputação e a imagem da organização;
- Manter conformidade com suas obrigações legais e regulamentações.

Um plano de continuidade deve oferecer:

- Garantia de continuidade operacional de todos os processos críticos de negócios;
- Mitigação dos riscos de todas as ameaças de interrupção;
- Desenho da topologia de todos os recursos de Disaster Recovery;

- Previsão dos custos e investimentos para implementação do plano;
- Dimensionamento dos postos de trabalho de contingência;
- Documentação e treinamento de todos os procedimentos de contingência e continuidade;

- Recomendação do plano de testes de contingência.

7.9. Inclusão Digital

7.9.1. Internet para todos

Como em qualquer atividade ligada às telecomunicações, todas as iniciativas relacionadas aos projetos de Cidade Digital devem levar em conta o cumprimento das normas estabelecidas pela Agência Nacional de Telecomunicações (Anatel). A este órgão, cabe regulamentar os assuntos vinculados ao setor, o que inclui administrar o uso do espectro de radiofrequência.

Para usar telecomunicações em sua localidade, seja internamente, na interligação dos órgãos municipais, seja oferecendo serviços como acesso à Internet à comunidade, a prefeitura pode recorrer às operadoras tradicionais de telefonia fixa ou móvel. Mas nem sempre isto é possível ou viável economicamente.

As condições muitas vezes não são vantajosas ou o município sequer está na rota de atendimento comercial das operadoras, porque elas não vislumbram, ali, possibilidade de retorno financeiro que justifique seus investimentos. Nesse caso, os gestores públicos podem buscar alternativas como contratar serviços de terceiros ou criar uma solução própria.

O poder municipal pode contratar os serviços de uma empresa, pública ou privada, que já tenha a licença de Serviço de Comunicação Multimídia (SCM). Tal licença permite que as empresas contratadas pelos municípios cobrem pelos serviços prestados, sendo uma opção disponível, por exemplo, para as prefeituras que contam com um órgão

municipal de informática, desde que tal órgão seja uma empresa.

A prefeitura também pode obter na Anatel uma licença de Serviço Limitado Privado (SLP), na su-modalidade Serviço de Rede Privado. As normas relativas a essa opção foram aprovadas pela Anatel em março de 2007, especificamente para atender às demandas das municipalidades.

Esta alternativa surgiu dos estudos e análises técnicas feitas por especialistas da Anatel. Eles constataram que, em função do avanço da tecnologia sem fio, muitas prefeituras já vinham instalando sistemas de telecomunicação em frequência de radiação restrita, ou seja, dentro de limites pré-estabelecidos, para oferecer a seus cidadãos não somente acesso à Internet, mas também a uma série de serviços municipais de forma online, via computadores ou totens de atendimento.

A licença do Serviço Limitado Privado (SLP) não tem custo, mas há algumas restrições: está condicionada à gratuidade do acesso e é válida apenas para os serviços da prefeitura e dentro do território municipal.

Para mais informações sobre o SLP, pode-se acessar diretamente o portal da Anatel (www.anatel.gov.br), e clicar em Informações Técnicas > Comunicação via Rádio > Serviço Limitado e selecionando a opção Serviço Limitado Privado.

CONSIDERAÇÕES FINAIS

A ausência de verbas para investimentos em TI da Prefeitura provocou algumas deficiências estruturais significativas que ao longo da gestão foram feitas as correções para funcionamento da organização como um todo. Mas a Administração e o Setor de DTI buscaram soluções para resolver um erro crônico de gestões passadas, dessa maneira foi investido em conhecimento chamamento de um Técnico de Tecnologia da Informação mais Voluntariado para que a estrutura fosse erguida, montada e efetivada. Há uma

padronização de hardwares, softwares, equipamentos, sistemas operacionais, gerenciadores de banco de dados, softwares de automação de escritório, além dos procedimentos formais.

Mas não há sistemas e equipamento os redundantes para provimento de serviços de missão crítica, além de uma equipe técnica enxuta e responsável por uma enorme quantidade de atividades associadas à unidade de tecnologia da informação. Por outro lado, observa-se o crescimento acima descrito, apesar das limitações orçamentárias, mas mesmo assim houve um avanço significativo e transformação na área de Tecnologia de Informação na atual Gestão Municipal.

REFERÊNCIAS:

https://www.tjpr.jus.br/documents/15390/6234939/TCE-PR%20Cartilha_Governanca_em_TI_15-FINAL-vs_2018-01.pdf/cb26b8b7-fc94-3836-8c7a-e34d1125d048 (acesso em 11/01/2023)

https://mppr.mp.br/ (acesso em 11/01/2023)

https://www1.tce.pr.gov.br/conteudo/canal-de-comunicacao-caco-orientacoes-gerais/263/area/251 (acesso em 11/01/2023)

https://1doc.com.br/governo/sobre/funcionalidades/ (acesso em 17/01/2023)

https://jucis.df.gov.br/como-salvar-em-pdf-a/ (acesso em 17/01/2023)

https://portal.utfpr.edu.br/servidores/servicos-servidor/sei/manuais/manual-para-impressao-de-documentos-em-pdf-a-com-ocr.pdf (acesso em 17/02/2023)

https://www.cnm.org.br/comunicacao/noticias/municipios-podem-participar-de-proposta-para-fortalecer-eficiencia-energetica-em-predios-publicos (acesso em 17/22023)

http://cidadeseficientes.cbcs.org.br/ (acesso em 23/02/2023)

https://www.aen.pr.gov.br/Noticia/Copel-oferece-R-30-milhoes-para-projetos-de-eficiencia-energetica-submissoes-vao-ate-marco (acesso em 27/02/2023)

https://www.copel.com/site/copel-distribuicao/eficiencia-energetica/audiencia-publica-de-eficiencia-energetica/ (acesso em 27/02/2023)

Elaborado e Executado por:

Edimar Tiago Souza
CRA-PR:200474
Técnico em Tecnologia da Informação
edimar.souza@tijucasdosul.pr.gov.br

_____

Homologado em __/__/___

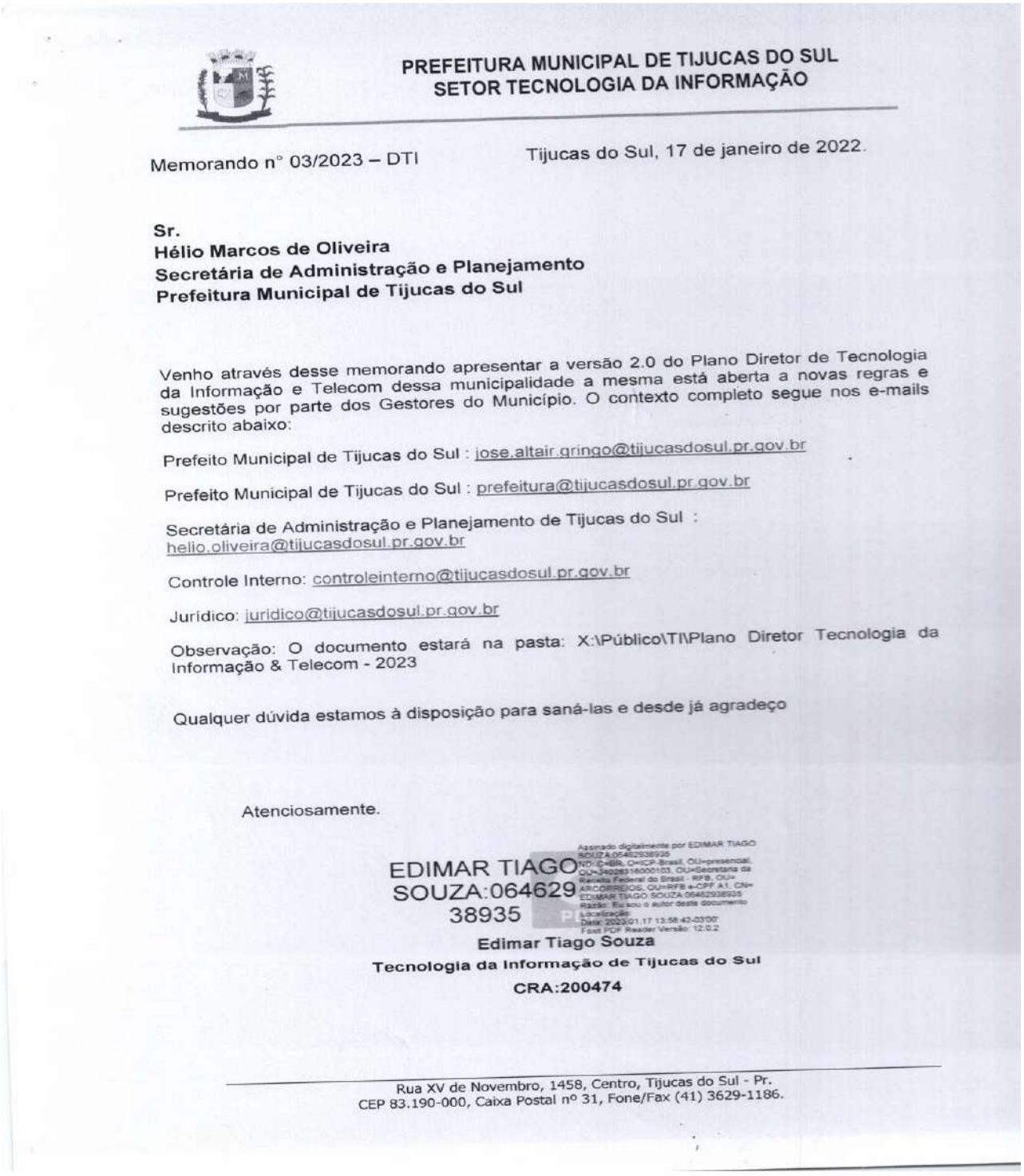
_____
Prefeitura Municipal de Tijucas do Sul

_____
Secretaria de Administração e Planejamento

_____
Advogado do Município de Tijucas do Sul

_____
Controladoria Geral do Município

Figura 92 – Memorando versão 2.0



PREFEITURA MUNICIPAL DE TIJUCAS DO SUL
SETOR TECNOLOGIA DA INFORMAÇÃO

Memorando n° 03/2023 – DTI Tijucas do Sul, 17 de janeiro de 2022.

Sr.
Hélio Marcos de Oliveira
Secretária de Administração e Planejamento
Prefeitura Municipal de Tijucas do Sul

Venho através desse memorando apresentar a versão 2.0 do Plano Diretor de Tecnologia da Informação e Telecom dessa municipalidade a mesma está aberta a novas regras e sugestões por parte dos Gestores do Município. O contexto completo segue nos e-mails descrito abaixo:

Prefeito Municipal de Tijucas do Sul : jose.altair.gringo@tijucasdosul.pr.gov.br

Prefeito Municipal de Tijucas do Sul : prefeitura@tijucasdosul.pr.gov.br

Secretária de Administração e Planejamento de Tijucas do Sul : helio.oliveira@tijucasdosul.pr.gov.br

Controle Interno: controleinterno@tijucasdosul.pr.gov.br

Jurídico: juridico@tijucasdosul.pr.gov.br

Observação: O documento estará na pasta: X:\Público\TI\Plano Diretor Tecnologia da Informação & Telecom - 2023

Qualquer dúvida estamos à disposição para saná-las e desde já agradeço

Atenciosamente.

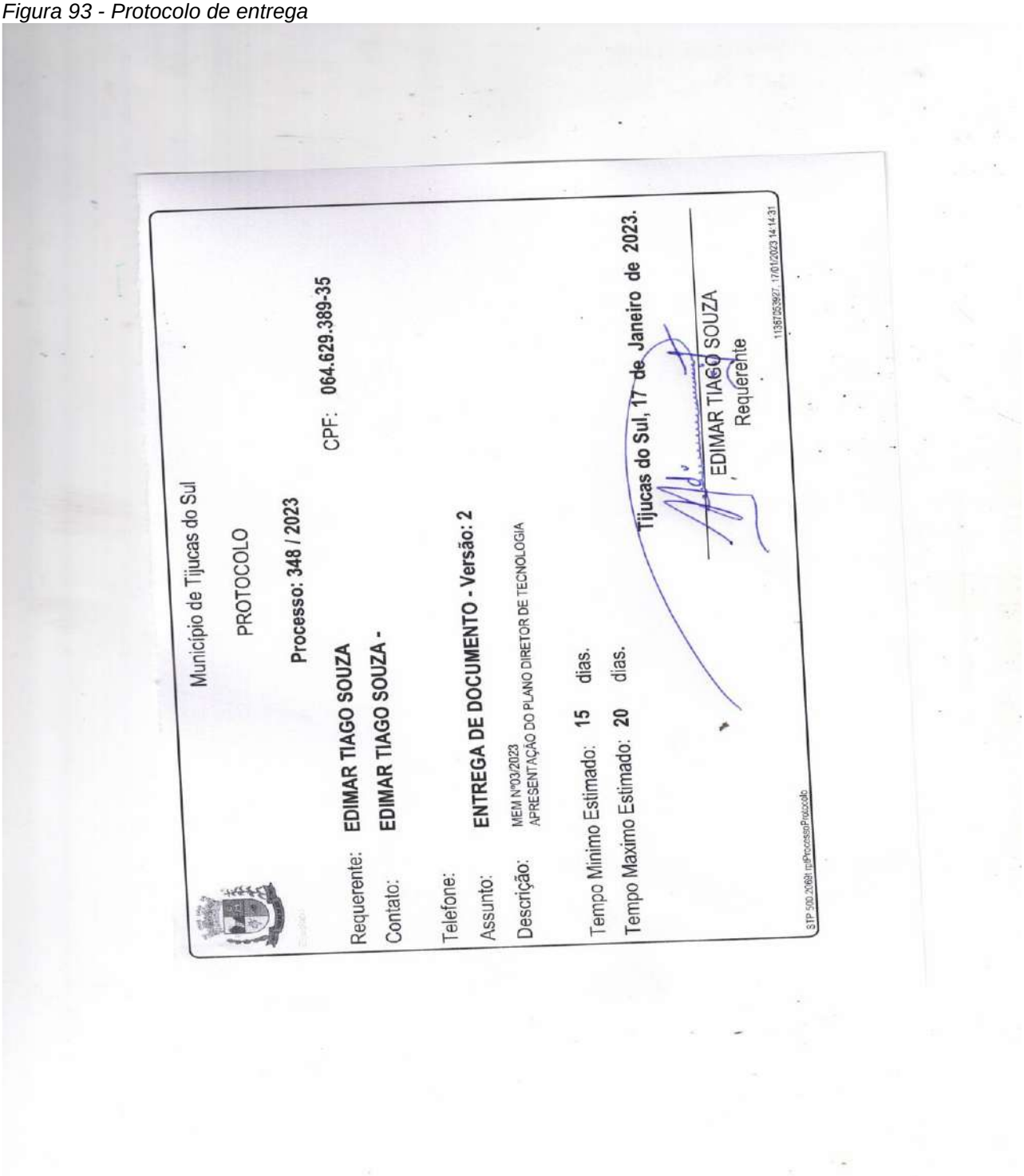
EDIMAR TIAGO SOUZA:06462938935

Assinado digitalmente por EDIMAR TIAGO SOUZA:06462938935
ND: C=BR, O=ICP-Brasil, OU=presencial, OU=34028316000103, OU=Secretaria da Receita Federal do Brasil - RFB, OU=ARCORREIOS, OU=RFB e-CPF A1, CN=EDIMAR TIAGO SOUZA:06462938935
Razão: Eu sou o autor deste documento
Localização:
Data: 2023.01.17 13:58:42-03'00'
Foxit PDF Reader Versão: 12.0.2

Edimar Tiago Souza
Tecnologia da Informação de Tijucas do Sul
CRA:200474

Rua XV de Novembro, 1458, Centro, Tijucas do Sul - Pr.
CEP 83.190-000, Caixa Postal nº 31, Fone/Fax (41) 3629-1186.

Figura 93 - Protocolo de entrega



Município de Tijucas do Sul

PROTOCOLO

Processo: 348 / 2023

Requerente: **EDIMAR TIAGO SOUZA** CPF: **064.629.389-35**

Contato: **EDIMAR TIAGO SOUZA -**

Telefone:

Assunto: **ENTREGA DE DOCUMENTO - Versão: 2**

Descrição: MEM Nº03/2023
APRESENTAÇÃO DO PLANO DIRETOR DE TECNOLOGIA

Tempo Minimo Estimado: **15** dias.

Tempo Maximo Estimado: **20** dias.

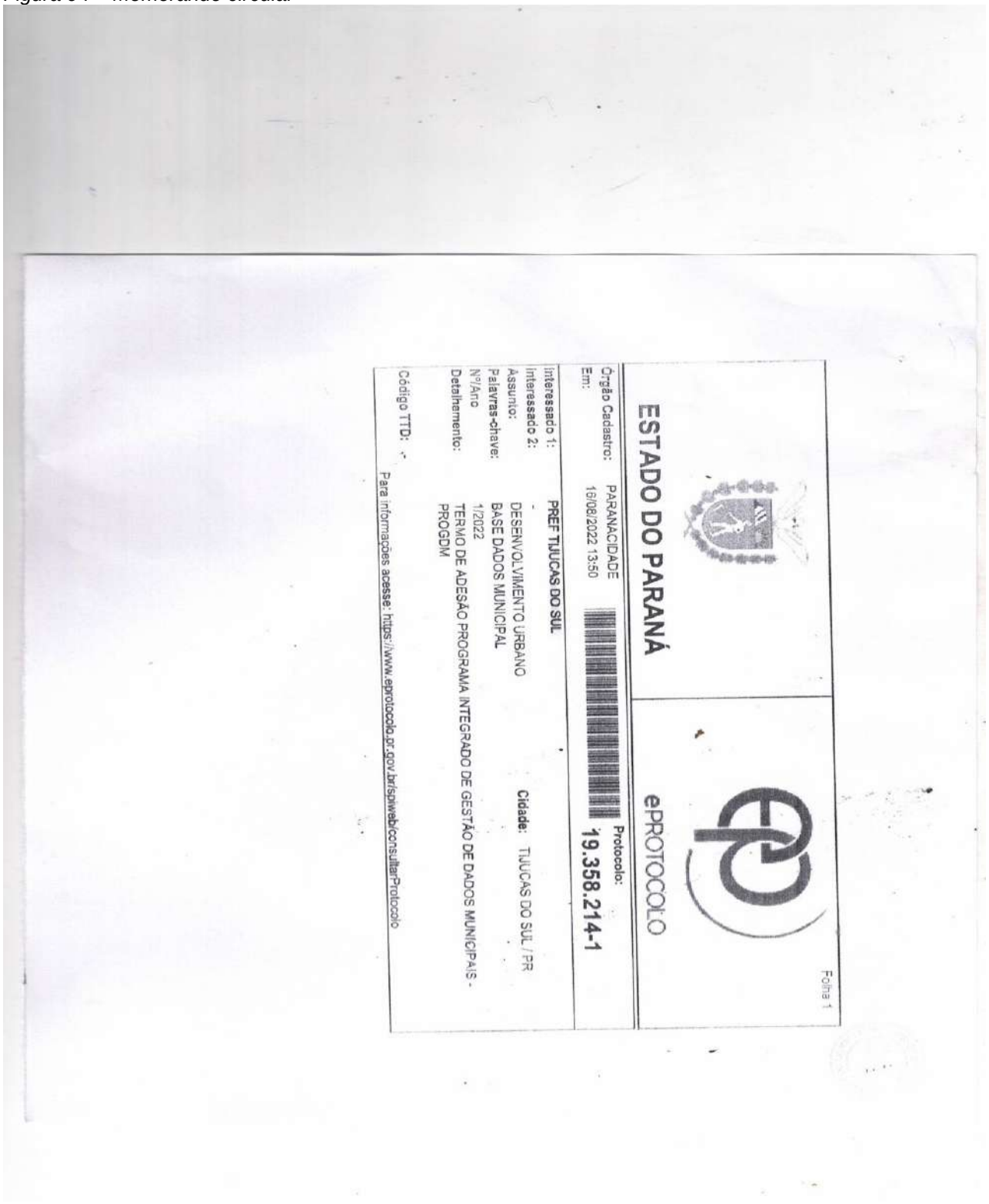
Tijucas do Sul, 17 de Janeiro de 2023.

EDIMAR TIAGO SOUZA
Requerente

STP-500.2068.rptProcessoProtocolo

113617053927 - 17/01/2023 14:14:31

Figura 94 – Memorando circular



ESTADO DO PARANÁ

ePROTOCOLO

Folha 1

Órgão Cadastro: PARANACIDADE
Em: 16/08/2022 13:50

Protocolo: 19.358.214-1

Interessado 1: PREF TIJUCAS DO SUL
Interessado 2: -
Assunto: DESENVOLVIMENTO URBANO
Palavras-chave: BASE DADOS MUNICIPAL
Nº/Ano 1/2022
Detalhamento: TERMO DE ADESÃO PROGRAMA INTEGRADO DE GESTÃO DE DADOS MUNICIPAIS - PROGDM

Cidade: TIJUCAS DO SUL / PR

Código TTD: -

Para informações acesse: https://www.eprotocolo.pr.gov.br/spiweb/consultarProtocolo