



PREFEITURA MUNICIPAL DE LEME - SP
SECRETARIA MUNICIPAL ADMINISTRAÇÃO

PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO - PDTI

AUTORIA	Márcio Leandro Felizatti
VERSÃO DO DOCUMENTO	1.1
DATA DESSA VERSÃO	29/12/2020

INTRODUÇÃO

Atualmente vivemos em um mundo altamente globalizado, caracterizado por constantes transformações, inundando-se regularmente por novos produtos, serviços e descobertas.

Isto tem feito com que as organizações também da gestão pública se preocupassem 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: agilidade nos processos, na estrutura, na comunicação e na eliminação da burocracia.

Na atual “Era da Atualização e Informação”, o uso estratégico da tecnologia da informação e a administração dos recursos de informática podem e devem melhorar o atendimento da população e o desenvolvimento sustentável deste 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 em crescimento da atuação do poder público exercendo assim um forte domínio sobre os interesses da população.

O Plano Diretor de Tecnologia da Informação foi desenvolvido a partir de levantamento e análise da situação organizacional e tecnológica, realizado em 2018. O levantamento da situação tecnológica contemplou:

- I. Análise do Parque Computacional;
- II. Análise da arquitetura de sistemas;
- III. Análise da infraestrutura de redes;
- IV. Identificação dos recursos de hardware, software básico e aplicativos;
- V. Estudo de documentos da área de informática.

Nos últimos anos, a área de informática da Prefeitura Municipal de Leme, vem enfrentado por vários processos de reorganização, realinhamento

tecnológico e de infraestrutura física do parque computacional, para gerar condições para cumprir sua missão e seu plano estratégico.

O mercado tecnológico indica como tendências aplicáveis à atuação dos Órgãos Públicos, no decorrer dos anos, redes com alta velocidade, interoperabilidade de aplicações, maior produtividade, sistemas de gerência de bancos de dados de grande capacidade de armazenamento, segurança da informação, alto nível de conectividade e interação com novas linhas de atuação através de canais virtuais e governo eletrônico.

Para que as recomendações propostas pelo PDTI sejam viáveis, é de suma importância a disponibilização de um orçamento anual para investimento em Tecnologia da Informação, compatível com as necessidades equiparando-se assim ao mesmo patamar da evolução tecnológica dos demais órgãos Municipais, Estadual e Federal.

O PDTI deverá ser avaliado a cada biênio e ajustado para melhor atendimento dos serviços prestados pela área de TI.

Os aspectos táticos e operacionais decorrentes do PDTI serão definidos em etapa posterior, em conjunto com representantes das secretarias da Prefeitura do Município de Leme.

Além de alcançar as metas estabelecidas neste PDTI é válido ressaltar a importância em estreitar o relacionamento da Coordenadoria de Atendimento e Suporte Técnico de Informática com as diversas secretarias da Prefeitura desta municipalidade.

Esta proposta consiste em prorrogar este PDTI pelo período de um ano, até a data de 31 de dezembro 2021.

OBJETIVO

Apresentar propostas que auxiliem na instauração de um processo de melhoria continua nos itens de software, hardware, administração da rede, infraestrutura, banco de dados e proteção da informação, apontando soluções para os problemas identificados que estejam limitando o alcance das metas da Prefeitura de Leme, por meio da Coordenadoria de Atendimento e Suporte Técnico de Informática.

O PDTI será o documento norteador para elaboração do planejamento e execução de todas as ações da tecnologia da informação. A fase do planejamento consiste em definir as ações que serão tomadas para atendimento às necessidades levantadas a partir do diagnóstico da situação atual da área de TI da Prefeitura Municipal de Leme.

CAPÍTULO I - PLANEJAMENTO ESTRATÉGICO

1. REFERENCIAIS ESTRATÉGICAS 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 do Município de Leme, contribuindo para a melhoria na prestação de serviços ao cidadão e ao desenvolvimento da municipalidade.”

1.2 VISÃO

“Integração dos serviços e formulação das tendências de tecnologia da informação na gestão do Município de Leme.”

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 do *Município de Leme*”.

Com vista aos objetivos estratégicos do município, este Plano Diretor de Tecnologia da Informação 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 EQUIPE PARTICIPANTE

Nome	Cargo	Área
CLAUDEMIR BORGES	PREFEITO MUNICIPAL INTERINO	GABINETE
SECRETARIADO MUNICIPAL	PREFEITURA MUNICIPAL	TODAS SECRETARIAS
Coordenador: Gerson Joest, Analista de sistema: Márcio Leandro Felizatti, Técnicos em Informática: Eduardo Henrique Drezano Pinto, Emerson Ricardo Gallo, Guilherme Aranha, Julio Henrique Moura, Marcio Vinicius Pereira Silva, Rebeca de Souza Sardinha, Robson Manoel Antonio Felipe, Thalles Stellet Sanchez Sobral, Vitor Hugo Monteiro Privatto, Vitor Roberto Bertini Junior, William Fernando Francisco	EQUIPE DE INFORMÁTICA	TECNOLOGIA DA INFORMAÇÃO
Controle Interno	Controle Interno	Controle Interno

1.5 PARTES INTERESSADAS

Nome	Órgão	Cargo
GABINETE DO PREFEITO	PREFEITURA MUNICIPAL	PREFEITO
SECRETARIADO MUNICIPAL	PREFEITURA MUNICIPAL	TODAS SECRETARIAS
SETOR DE TECNOLOGIA DA INFORMAÇÃO	PREFEITURA MUNICIPAL	ANALISTA DE SISTEMA

1.6 METODOLOGIA APLICADA

ITIL ISO 20000

O **ITIL - Information Technology Infrastructure Library** é um modelo de referência para gerenciamento de processos de TI muito no conceito da atualidade.

Essa metodologia foi criada pela secretaria de comércio do governo inglês, a partir de pesquisas realizadas por consultores, especialistas e doutores, para desenvolver as melhores práticas para gestão de TI nas empresas públicas e privadas.

O foco desse modelo é descrever os processos necessários para gerenciar a infraestrutura de TI eficientemente e eficazmente de modo a garantir os níveis de serviço acordados com os clientes internos e externos.

Características do ITIL:

- I. Modelo de referência para processos de TI não proprietário;
- II. Adequado para todas as áreas de atividade;
- III. Independente de tecnologia e fornecedor;
- IV. Baseado nas melhores práticas;
- V. Um modelo de referência para a implementação de processos de TI;
- VI. Checklist testado e aprovado; Prefeitura

1.7 ORGANOGRAMA ESTRUTURAL DA GERÊNCIA DE TECNOLOGIA

DA INFORMAÇÃO E COMPETÊNCIAS



1.8 SECRETÁRIO DE ADMINISTRAÇÃO

Competência: Assessorar o Chefe do Executivo em assuntos de sua unidade; Planejar, organizar, coordenar e controlar a execução das atividades do Setor, providenciando os meios para que as mesmas sejam realizadas; Zelar pelo material e/ou equipamento pertencentes ao Setor; Elaborar relatório periódico sobre as atividades de sua unidade;

Atender ao público em assuntos de competências de sua unidade; Manter elevada a moral de seus subordinados e a colaboração entre os servidores municipais.

1.9 RESPONSÁVEIS PELA TECNOLOGIA DA INFORMAÇÃO

Competência: Distribuir, orientar e coordenar os serviços do Setor; Supervisionar a execução das atividades do Setor (Suporte à Desktops, Notebooks e Periféricos, Conectividade a Rede Local (LAN), Gerenciamento dos Servidores, Firewall e outros equipamentos de infraestrutura. Conectividade a Internet (WAN), Conectividade à Rede Wireless (WLAN), Correio Eletrônico, Antivírus dos Servidores, Filtro de Conteúdo Web, Cópias de Segurança (Backup e Restore), Serviços de Armazenamento Centralizado, Gerenciamento de sistemas relacionados a página on-line; Informar e encaminhar processos submetidos à sua apreciação; Elaborar relatórios periódicos das atividades do Setor; Requisitar, receber e controlar material de consumo permanente ou equipamentos; Sugerir medidas de melhoria dos serviços e aperfeiçoamento das rotinas; Fornecer elementos para a

elaboração da previsão orçamentária; Zelar pela disciplina e controlar a frequência e pontualidade de seus subordinados; Zelar pelo material e/ou equipamento pertencentes ao Setor e pela conservação da limpeza e higiene da mesma; Elaborar trabalhos específicos que lhe sejam determinados.

1.10 SUPORTE TÉCNICO

Competência: Suporte aos Desktops, Notebooks e Periféricos, Movimentação de Equipamentos de TI, Conectividade a Rede Local (LAN), Conectividade a Internet (WAN), Conectividade à Rede Wireless (WLAN), Correio Eletrônico, Antivírus de Estações de Trabalho, Filtro de Conteúdo Web, Cópias de Segurança (Backup e Restore), Serviços de Armazenamento Centralizado, Gerenciamento e Suporte à Servidores, Gerenciamento de sistemas relacionados a página on-line; Zelar pelo material e equipamento pertencentes ao patrimônio público; Assessorar os servidores na execução de serviços relacionados a informática; Elaborar documentos, formulários; Acompanhar e dar manutenção aos programas municipais relacionados a internet; Gerenciar softwares adquiridos pela municipalidade. Executar trabalhos específicos que lhe sejam determinados.

2. OBJETIVOS

Os objetivos estratégicos da Coordenadoria de Atendimento e Suporte Técnico de Informática, devidamente alinhados aos objetivos estratégicos da gestão municipal, apresentam-se como tangíveis dentro de um prazo de 03 (três) anos, de 2021-2022. Porém, a volatilidade do segmento de tecnologia da informação exige manutenção constante do plano haja vista a possibilidade de mudanças de tendências.

Item	Objetivo
1.	Atualizar as condições de trabalho da equipe de tecnologia da informação através do fornecimento de cursos de especialização para os funcionários atuais.
2.	Assegurar o ganho de desempenho na conectividade entre unidades remota internamente na rede local.

3.	Atualização do Setor de TI e demais setores, com modernização de equipamentos de tecnologia da informação.
4.	Consolidar a infraestrutura dos demais setores com novas aquisições, readequações e upgrades estruturais.
5.	Promover a segurança lógica da rede através de segmentações físicas, lógicas, controle de acesso a rede lógica e soluções de armazenamento seguro.
6.	Promover segurança por meio de políticas, planos, documentações e reorganização formal das rotinas de trabalho da unidade de tecnologia da informação.
7.	Aprimorar processos e sistemas de atendimento a usuários de tecnologia da informação por meio de sistemas de Service Desk e acesso físico.
8.	Implantar novos sistemas corporativos para automatizar rotinas de trabalho e reduzir custos operacionais
9.	Promover a inclusão digital e social por meio de programas municipais.

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. 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).

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

2. VISÃO GERAL

O ambiente de tecnologia da informação da gestão municipal da Prefeitura do Município de Leme, é composto dos seguintes ativos:

Ativos	Quantidade
Servidores Físicos - Prefeitura	8
Servidores Físicos-comodato	2
Switches (não gerenciados)	7
Estações de Trabalho	1919
Impressoras	1077
multifuncionais	319
No-breaks	6
Links (Fibra 100mb sla 99,8%)	1
Usuários (AD)	321
Rádios - Pontos de Acesso	18
Rádios - Clientes	85

3. INFRAESTRUTURA

As próximas seções deste documento apresentam as disposições físicas e lógicas do ambiente de tecnologia da informação da Prefeitura de Leme, assim como a

identificação de deficiências e necessidades de adaptações e reformulações consideradas de grau médio e alto para um ambiente tão dependente de tecnologia da informação.

3.1 ESTAÇÕES DE TRABALHO E SERVIDORES

O conjunto de 1919 (um mil, novecentas e dezenove) estações de trabalho da Prefeitura de Leme, englobam estações de trabalho com sistema operacional Linux, Microsoft Windows XP, 7, 8, 8.1 e 10. O parque de servidores é composto de (03) três unidades na plataforma Microsoft Windows Server 2008 R2 (servidor de domínio, aplicação e web server) , (02) dois servidores Linux XenServer (virtualização) e (01) um servidor Microsoft Windows 2012 R2 Server (banco de dados).

3.2 ESTRUTURAS DE REDE DA PREFEITURA DE LEME

LOCAL	DEFICIÊNCIA	GRAU DE RISCO	NECESSIDADE DE ADAPTAÇÃO OU REFORMULAÇÃO
SALA DOS SERVIDORES	Cabeamento e Segurança	Médio	Adequação para uma sala mais segura, revisão na parte elétrica, reorganização através de conduites, melhoria na forração do teto para evitar goteiras,
SETOR DE TI	Reorganização Cabos, Fiação Elétrica, Porta de Segurança	Baixo	Substituir atual porta da sala para uma com segurança adequada.
PAÇO MUNICIPAL	Revisão de rede	Baixo	Revisar toda rede elétrica e cabeada instalada atualmente no local.

4. SISTEMAS PRÓPRIOS E TERCEIRIZADOS UTILIZADOS PELA PREFEITURA DO MUNICÍPIO DE LEME.

Os sistemas utilizado pela Prefeitura do Município de Leme é terceirizado através de licitação e a empresas prestadoras dos serviços são a Governança Brasil SA - GovBr e a Vivver Sistemas.

Utilizado pela Prefeitura do Município de Leme é terceirizado através de licitação e a empresa prestadora do serviço é a GovBr, cuja plataforma possui os seguintes módulos implantados no servidor local:

- I. Administração de Receitas (AR)
- II. Compras e Materiais (CM)
- III. Contabilidade Pública (CP)
- IV. Gestão de Pessoas (GP)
- V. Licitações e Contratos (LC)
- VI. Procuradoria (PC)
- VII. Patrimônio Público (PP)
- VIII. Responsabilidade Fiscal (RF)
- IX. Tesouraria (ST)
- X. Tramitação de Processos (TP)

O sistema utilizado pela Secretaria de Saúde é terceirizado também e a empresa prestadora do serviço é a Vivver Sistemas, a plataforma possui os seguintes módulos implantados em servidor local:

- I. Ambulatório
- II. Faturamento

- III. Farmácia e Almoxarifado
- IV. Laboratório
- V. Regulação
- VI. Informação Geográfica
- VII. Vigilância Epidemiológica
- VIII. Ouvidoria
- IX. RH
- X. Tratamento Fora do Domicílio (TFD)
- XI. CMCE
- XII. PPI
- XIII. Vacina
- XIV. Gestor (Relatórios)
- XV. Informação de ESF
- XVI. Administração

5. SEGURANÇA

Atualmente a Prefeitura Municipal de Leme utiliza como segurança de firewall, Proxy e monitoramento nos acessos os softwares pfSense e EndianCE. Quanto à utilização de antivírus, os servidores principais utilizam antivírus ESET File Security, as estações que utilizam o software Microsoft Essentials Security ou Windows Defender contido na versão do Windows 10.

5.1 BACKUP

Os Backups são realizados manualmente, e com alguns processos automáticos.

São armazenadas em ferramentas disponíveis, através do servidor.

6. PESSOAS E PROCESSOS

Os atuais prestadores de serviço da Prefeitura do Município de Leme, no segmento de tecnologia da informação, são:

Empresa	Objeto
GOVBR - Governança Brasil	Sistema de Gestão Pública para os Serviços oferecidos pela Prefeitura Municipal de Leme
VIVVER SISTEMAS	Sistema de Gestão da Secretaria Municipal de Saúde
TELEFONICA	Provedora de Internet

Em relação ao atendimento de suporte reativo, se o problema for lógico em nível de software, é realizado o acesso remoto para sua resolução. Em relação ao atendimento de suporte preventivo, há política definida para atualização dos softwares e sistemas operacionais das estações de trabalho e servidores.

7. PROJETOS

7.1 INFRAESTRUTURA FÍSICA E LÓGICA DA REDE

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

acomodação de equipamentos de tecnologia da informação.

7.1.1 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 do Município de Leme necessita de atualização em sua infraestrutura de rede física para assegurar mais estabilidade e escalabilidade na comunicação de dados, além de preparar sua infraestrutura 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;
- Reformular toda a estrutura de cabeamento de dados;

7.1.2 REDE LÓGICA CABEADA

A infraestrutura lógica da rede é parte essencial para a manutenção da disponibilidade, integridade e confidencialidade dos dados. A rede de dados da Prefeitura Municipal de Leme deverá ser reformulada, por meio de um projeto técnico.

7.2 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 deseje 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. A Prefeitura Municipal de Leme, constantemente através de seus firewall consegue:

- 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 do Município de Leme;
- Promover maior desempenho no acesso à Internet, com segurança apropriada e capaz de detectar ataques modernos;
- Aperfeiçoar o uso de conectividade Internet entre as secretarias apenas para tráfego útil ao desempenho das rotinas de trabalho;

7.2.1 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 Municipal de Leme.

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, incitar 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.

Os 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 da Prefeitura Municipal, sem validação e inspeção.

A solução de segurança de perímetro Internet baseada em firewall considera-se as seguintes premissas:

- Controlar e segmentar fisicamente o tráfego entre as redes internas, rede DMZ, Internet, Prefeitura Municipal de Leme e redes locais remotas (Secretarias);
- Implantar uma rede desmilitarizada (DMZ) onde serão acomodados servidores com serviços publicados para a Internet;
- Integrar funcionalidades de UTM (Unified Threat Management) como IPS/IDS, Anti-spam, Antivírus, Anti-spyware e Controle de Conteúdo Web;
- Estabelecer tunelamento VPN com outras soluções através do protocolo IPS ou SSL;
- Atuar preferencialmente em modo Ativo/Passivo para assegurar persistência e manutenção da conectividade em situações de falhas;
- Permitir o gerenciamento centralizado de todas as camadas, com funcionalidades de UTM aplicada as regiões de segurança monitoradas.

7.2.2 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.

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 fácil.

Facilitando 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 a 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 (Clientes);
- Integração com serviço de Diretório e RADIUS;
- Controle de acesso integrado ao End-Point;
- Independentemente da plataforma utilizado pelo computador.

7.2.3 CONTROLE DE ACESSO A REDE

Uma solução de Controle de Acesso a 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 avaliação de vulnerabilidades e retificação assistida, além de isolar computadores e usuários suspeitos. Com isso, para a solução de controle de acesso a 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;

7.3 SERVIDORES, ARMAZENAMENTO E BACKUP

Identificação: Máquina 1

Fabricante	IBM	
Modelo	System x3550 M3	
Processador	2 processadores Intel64 Family 6 Model 44 Stepping 2 GenuineIntel ~1592 Mhz	
Memória	64 GB	
Hard Disk		
Qtd	Tamanho	Tipo
4	146 GB	SAS
S.O.	Microsoft Windows Server 2008 R2	
Serviços:	Área de trabalho remota Serviço de Domínio do Active Directory Servidor DNS Servidor Web IIS: TP Net Cetil (Tramitação de protocolo)	
Identificação: Máquina 2		
Fabricante	IBM	
Modelo	System x3550 M3	
Processador	2 processadores Intel64 Family 6 Model 44 Stepping 2 GenuineIntel ~1592 Mhz	
Memória	64 GB	
Hard Disk		
Qtd	Tamanho	Tipo
3	300 GB	SSD SAS
S.O.	Linux	
Serviços:	Banco de dados VIVVER	
Identificação: Máquina 3		
Fabricante	IBM	
Modelo	System x3550 M3	
Processador	2 processadores Intel64 Family 6 Model 44 Stepping 2 GenuineIntel ~1592 Mhz	
Memória	48 GB	
Hard Disk		
Qtd	Tamanho	Tipo
4	500	SAS
S.O.	Microsoft Windows Server 2008 R2	
Serviços:	Servidor de Aplicação - CETIL	
Identificação: Máquina 4		
Fabricante	IBM	
Modelo	System x3550 M3	
Processador	2 processadores Intel64 Family 6 Model 44 Stepping 2 GenuineIntel ~1592 Mhz	
Memória	48 GB	
Hard Disk		
Qtd	Tamanho	Tipo
4	500 GB	SAS
S.O.	Debian	

Serviços:	Servidor UNMS	
Identificação: Máquina 5		
Fabricante	IBM	
Modelo	System x3550 M3	
Processador	2 processadores Intel64 Family 6 Model 44 Stepping 2 GenuineIntel ~1592 Mhz	
Memória	48 GB	
Hard Disk		
Qtd	Tamanho	Tipo
4	500 GB	SAS
S.O.	Microsoft Windows Server 2008 R2	
Serviços:	Servidor de Aplicação - CETIL	
Identificação: Máquina 6		
Fabricante	Dell Inc.	
Modelo	PowerEdge 6950	
Processador	4 processadores AMD64 Family 15 Model 65 Stepping 3 AuthenticAMD ~990 Mhz	
Memória	64 GB	
Hard Disk		
Qtd	Tamanho	Tipo
1	180	SCSI
1	280	SCSI
S.O.	Microsoft Windows Server 2008 R2	
Serviços:	HYPER-V	
Identificação: Máquina 7		
Fabricante	HP	
Modelo	ProLiant DL380G6	
Processador	2 processadores Intel Xeon E5645 2,40Ghz	
Memória	48 GB	
Hard Disk		
Qtd	Tamanho	Tipo
8	500 GB	SAS
S.O.	XenServer	
Serviços:	Virtualização:	
Identificação: Máquina 8		
Fabricante	HP	
Modelo	ProLiant DL380 Gen9	
Processador	1 processador Intel Xeon 08C E5-2630v4	
Memória	64 GB	

Hard Disk		
Qtd	Tamanho	Tipo
2	1 TB	SATA
8	300 GB	SAS
S.O.	Microsoft Windows Server 2012 R2	
Serviços:	SQL server	

7.4.1 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 garante 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.

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.

7.4.2 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 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

7.5.1 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.

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:

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

7.5.2 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 Municipal de Leme sejam contemplados numa solução de continuidade, que busca o menor custo operacional possível.

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.

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.

CONSIDERAÇÕES FINAIS

A falta de investimentos em hardwares, softwares, equipamentos, sistemas operacionais, gerenciadores de banco de dados, além da ausência de procedimentos formais, conduz a um ambiente desprovido de padrões e vulnerável.

Não há sistemas e equipamentos 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 que a despeito das deficiências acima descritas, apesar das limitações orçamentárias, há uma preocupação aparente na reversão do quadro atual, que se inicia com a conclusão deste PDTI.

Após a leitura e análise deste documento, consideramos o mesmo **HOMOLOGADO** e apto para orientar nossas metas quanto ao uso de nossos recursos de tecnologia e informação de nossa instituição.

Leme/SP, 04 de janeiro de 2021.
