

QUANTITATIVOS E ORÇAMENTO DE REFERÊNCIA

Lote	Cód. Sistema	Cód. CATSER	Item	Descrição do Serviço	Unid	Quantidade Mensal Estimada	Valor Unitário	Valor Total Mensal
1	INFRAESTRUTURA DE COMUNICAÇÃO PARA INTERLIGAÇÃO DAS UNIDADES:							
	53679	25135	1	Infraestrutura de Comunicação com capacidade 01 Gbps, instalado no DC da contratada, com dupla abordagem em fibra óptica até o Centro Administrativo. (NS01)	un	01		
	53678	25135	2	Infraestrutura de Comunicação com capacidade 100 Mbps Full Duplex (NS02)	un	65		
	62438	25135	3	Infraestrutura de Comunicação com capacidade 20 Mbps Full Duplex (NS03)	un	85		
	CONEXÃO À INTERNET:							
	59222	26484	4	Link de Acesso Internet Dedicada com velocidade de 500 Mbps Full Duplex	un	01		
	FIREWALL:							
	53682	27014	5	Firewall Marca: _____ Modelo: _____	un	01		
	INFRAESTRUTURA PARA REDE WIFI INTERNO:							
	53680	26522	6	Ponto acesso Wifi Indoor Marca: _____ Modelo: _____	un	440		
				VALOR GLOBAL MENSAL R\$				
				VALOR GLOBAL ANUAL R\$				

TERMO DE REFERÊNCIA DOS SERVIÇOS

1. OBJETO	3
2. OBJETIVO	3
3. JUSTIFICATIVAS	4
3.1. Interligação das Unidades do Município	4
3.2. Conexão à Internet	4
3.3. Firewall	4
3.4. Serviços de WIFI	4
4. DA CONTRATAÇÃO UNIFICADA	4
4.1. Integração com a MPLS da Secretaria de Educação	5
5. REQUISITOS TÉCNICOS MÍNIMOS	5
5.1. Infraestrutura de comunicação para interligação das unidades	5
5.1.1. A infraestrutura a ser disponibilizada deverá suportar as seguintes tecnologias embarcadas:	5
5.1.2. Qualidade de Serviço (QoS – Quality of Service)	6
5.1.3. Níveis de Serviço (NS)	6
5.1.4. Classes de Serviço (CoS – Classes of Service):	6
5.1.5. Conexão das unidades e pontos da prefeitura na infraestrutura de comunicação:	7
5.1.6. Características dos Roteadores a serem fornecidos:	7
5.2. Conexão Dedicada à Internet	9
5.2.1. Características gerais	9
5.2.2. Testes e validações	9
5.3. Appliance Firewall para Gerenciamento da Internet	9
5.3.1. Características Gerais e Capacidade	9
5.3.2. Especificações Gerais	10
5.3.3. Filtro de pacotes	11
5.3.4. IPS (Intrusion Prevention System)	12
5.3.5. Gateway Antivírus	12
5.3.6. Solução de Proxy – Filtro Web	13
5.3.7. VPN (Virtual Private Network)	15
5.3.8. Logging e Relatórios	15
5.4. Infraestrutura para rede WIFI interna	16
5.4.1. Características mínimas do WIFI:	16
5.4.2. Características da infraestrutura fornecida:	17
5.5. Condições de fornecimento dos Serviços	17
6. QUANTIFICAÇÃO	18
6.1. Infraestrutura de comunicação para interligação das Unidades	18
6.2. Conexão à Internet:	18
6.3. Firewall:	19
6.4. Infraestrutura para rede WIFI indoor:	19
7. CARACTERÍSTICAS DA EXECUÇÃO DOS SERVIÇOS	19
7.1. Características gerais:	19
7.2. Cronograma de Entrega dos Serviços	20
7.3. Painel de Transparência dos Serviços	22
7.4. Central de atendimento 24x7x365	22
7.5. Segurança	23
7.6. Encerramento do Contrato	23

8 NÍVEIS MÍNIMOS DE SERVIÇO / SLA	23
8.1. Conexão Dedicada à Internet:	23
8.2. Firewall:	24
8.3. Infraestrutura de comunicação para interligação das Unidades	24
8.4. Infraestrutura para rede WIFI interno:	26
9 FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR	27
10. QUALIFICAÇÃO TÉCNICA	27
11. OBRIGAÇÕES DA CONTRATADA	28
12. OBRIGAÇÕES DA CONTRATANTE	29
13 SUBCONTRATAÇÃO	30
14. MODELO DE GESTÃO DE CONTRATO	30
15. DO PAGAMENTO	31
16 REAJUSTAMENTO DO PREÇO	32
17 DA PROTEÇÃO DE DADOS	32
18. DOTAÇÃO ORÇAMENTÁRIA	32

1. OBJETO

Contratação de empresa para locação de Infraestrutura de Rede para Comunicação, visando a Interligação de Unidades, Conexão de Internet, Firewall e WIFI, para a Prefeitura Municipal de Santa Cruz do Sul.

2. OBJETIVO

Promover uma infraestrutura de tecnologia da informação robusta e integrada que suporte de forma eficiente as operações diárias da Prefeitura de Santa Cruz do Sul. A interligação das unidades permitirá uma comunicação fluida e rápida entre os diversos departamentos, otimizando processos administrativos e facilitando o acesso a informações essenciais. A conexão dedicada e de alta velocidade à internet garantirá que todos os serviços online da prefeitura sejam executados sem interrupções, proporcionando maior agilidade no atendimento ao cidadão e na execução de tarefas internas.

Além disso, a implementação de um sistema de Firewall fortalecerá a segurança da rede corporativa municipal, protegendo dados sensíveis contra acessos não autorizados e possíveis ciberataques. O serviço de WIFI permitirá uma conectividade mais abrangente, beneficiando tanto os funcionários quanto os cidadãos que utilizam os espaços públicos administrados pela prefeitura. Com essa infraestrutura tecnológica aprimorada, espera-se aumentar a eficiência operacional, melhorar a segurança dos dados e oferecer um serviço público de qualidade superior à população de Santa Cruz do Sul.

As quantidades para implantação dos itens 2, 3 e 6, que serão realizados conforme demanda, atenderão às futuras necessidades, devido ao crescimento da demanda de tecnologia nos serviços à população e para a futura capacidade de atender aos pontos das escolas municipais, os quais estão previstos atualmente no contrato específico da Educação (097/PGM/2022), mas que em maio de 2026 deixará de vigor. Isso permitirá uma gestão eficiente e econômica dos recursos tecnológicos, adaptando-se às necessidades dinâmicas da administração municipal.

3. JUSTIFICATIVAS

3.1. Interligação das Unidades do Município

Prover solução para tráfego de dados, voz e imagens, bem como internet de forma segura e centralizada, interligando as unidades da Prefeitura Municipal de Santa Cruz do Sul localizadas nos endereços definidos em anexo deste Termo de Referência.

3.2. Conexão à Internet

A Conexão à Internet com qualidade e velocidade está alinhado às necessidades dos usuários/servidores no desempenho de suas atividades. Por exemplo, o acesso aos sistemas e aplicações da Prefeitura, páginas de pesquisa, sites de fornecedores, telefonia, e-mails, serviços disponibilizados aos cidadãos, prestação de contas, transparência, etc.

3.3. Firewall

O Firewall tem por objetivo proteger externamente acessos indevidos à rede local das unidades da Prefeitura, além implementar uma camada de segurança no acesso a conteúdos indevidos por usuários e dispositivos internos que podem ser vítimas de vírus, links e programas maliciosos sem o devido conhecimento dos usuários.

Além disso, o Firewall também garantirá o gerenciamento de acesso aos conteúdos, filtrando aplicações indesejadas e permitindo os acessos destinados às aplicações voltadas às atividades críticas do município.

3.4. Serviços de WIFI

Necessidade de conexão sem fio e segura para os usuários e dispositivos, com gerência centralizada, SSIDs separados de uma possível rede de conexão ao público e em conformidade com a legislação vigente, como o Marco Civil da Internet e LGPD.

4. DA CONTRATAÇÃO UNIFICADA

A contratação global se justifica pela interdependência técnica e operacional entre esses componentes, que juntos compõem uma estrutura fundamental de conectividade da rede corporativa municipal, e a separação desses serviços em diferentes contratos poderia comprometer a padronização, a eficiência da gestão, a compatibilidade entre soluções e a responsabilização do fornecedor em caso de falhas conjuntas.

Dessa forma, a contratação unificada assegura maior eficácia na execução, facilita o gerenciamento técnico e administrativo, e contribui para a continuidade dos serviços públicos digitais prestados à população.

O objeto desta contratação contempla os seguintes serviços de tecnologia da informação:

- **Interligação das Unidades:** Instalação de enlaces dedicados para a interligação das unidades municipais, garantindo alta disponibilidade e baixa latência na transmissão de dados entre os setores localizados em diversos pontos no município. Implementação de uma rede MPLS (Multiprotocol Label Switching) integrada e segura que suporte a comunicação eficiente e ininterrupta entre todas as unidades administrativas.
- **Conexão à Internet:** Fornecimento de um link dedicado de alta velocidade, full duplex, que assegure a operação contínua e eficiente de todos os serviços online da prefeitura.

- **Sistema de Firewall:** Implementação de um sistema de Firewall de última geração para monitorar e controlar o tráfego de dados na rede corporativa. Proteção contra ameaças cibernéticas e acessos não autorizados, assegurando a segurança dos dados sensíveis da prefeitura.
- **Infraestrutura de WIFI:** Instalação de pontos de acesso WIFI nos locais necessários, proporcionando conectividade sem fio de alta qualidade. Benefício tanto para os funcionários quanto para os cidadãos que utilizam os espaços públicos administrados pela prefeitura.

Embora os componentes da solução estejam separados em itens distintos, é imprescindível, do ponto de vista técnico, que a solução como um todo seja provida de maneira integrada por um único fornecedor pois, em um cenário de múltiplos fornecedores, a implantação da solução dependerá da execução efetiva dos contratos associados. A inexecução de um ou mais contratos poderá acarretar em atraso na implantação da solução por tempo imensurável. O parcelamento também poderia trazer prejuízos para a Administração devido à complexidade de gerir diversos contratos interdependentes. Por estas razões, e visando à eficiência da contratação, opta-se pelo não parcelamento.

4.1. Integração com a MPLS da Secretaria de Educação

Atualmente, a Secretaria Municipal de Educação (SEE) mantém ativa uma rede MPLS por meio do Contrato nº **097/PGM/2022**, vigente até maio de 2026, a qual está interligada à rede corporativa do Município. Essa infraestrutura é utilizada para conectar as unidades educacionais da rede pública municipal, bem como garantir-lhes acesso à Internet.

No âmbito desta contratação, o novo fornecedor deverá integrar a sua solução ofertada à rede MPLS atualmente operada pela SEE, por meio do link de 500 Mbps (NS01E) previsto para ser ativado por demanda no respectivo contrato. Nessa modalidade, a contratada assumirá o fornecimento de serviços de Internet dedicada e Firewall para as unidades educacionais, mantendo-se a rede de transporte contratada pela SEE (MPLS e pontos WIFI).

O modelo de precificação adotado (por unidade conectada) deverá prever essa flexibilidade e será detalhado na proposta técnica.

5. REQUISITOS TÉCNICOS MÍNIMOS

5.1. Infraestrutura de comunicação para interligação das unidades

a) Deverá ser fornecida infraestrutura de comunicação de fibra óptica e/ou rádio frequência digital possibilitando a conexão dedicada entre as unidades da Prefeitura com o BACKBONE da CONTRATADA. O ponto CONCENTRADOR (roteador de borda) da rede MPLS deverá estar localizado na infraestrutura da CONTRATADA, em seu Data Center ou Ponto de Presença (PoP), de onde partirá a interligação de todas as unidades da Prefeitura.

5.1.1. A infraestrutura a ser disponibilizada deverá suportar as seguintes tecnologias embarcadas:

- Tecnologia de transmissão MPLS (Multi Protocol Label Switching), conforme RFC (*) 3031.
- Utilização de redes privadas virtuais (VPN – Virtual Private Networks) sobre a tecnologia MPLS, de acordo com a RFC 2547.

c) A infraestrutura disponibilizada deverá permitir a topologia multiponto (comunicação entre as redes locais diretamente entre elas) ou em estrela (onde todo o tráfego entre as diversas redes locais depende de roteamento por meio de uma rede central).

d) Possibilitar o uso de VPN pela Prefeitura, com isolamento de tráfego do backbone da Contratada, sendo utilizados rótulos (labels) nos pacotes para roteamento exclusivo de suas VPNs.

* RFC (Request for Comments) é um documento técnico que serve para sugerir mudanças ou melhorias em sistemas de software ou em protocolos da Internet.

5.1.2. Qualidade de Serviço (QoS – Quality of Service)

a) A rede de dados deverá suportar QoS a fim de garantir um tratamento diferenciado para o tráfego de cada classe de serviço que operar sobre a rede:

b) QoS sobre MPLS/VPN deverá estar de acordo com as RFCs 3270 e 2983.

c) Priorização das classes de serviço (CoS – Classes of Service) críticas sensíveis à latência, de forma a otimizar o uso da rede, em caso de congestionamentos.

d) A classificação das diferentes CoS deverá seguir os padrões das RFCs 2474 e 2475 (Serviços Diferenciados), contendo 4 mecanismos básicos de diferenciação de tráfego: Classificação, Marcação, Policiamento e Filas.

5.1.3. Níveis de Serviço (NS)

Com vistas a garantir padrões mínimos de desempenho, disponibilidade e economicidade, estabelecem-se os seguintes níveis de serviço (NS), correspondentes ao SLA de velocidade de banda a ser contratada:

a) NS01 – Interligação de dados (MPLS) capacidade de 1 Gbit/s (gigabits por segundo), instalado no Data Center da contratada, interligado exclusivamente em fibra óptica (FO), em dupla abordagem com o Centro Administrativo 1 da Prefeitura, devendo cada rota possuir trajetos físicos independentes e pontos de entrada distintos no prédio, de forma a garantir a redundância e a continuidade do serviço em caso de falha ou rompimento em um dos percursos.

b) NS02 – Interligação de dados (MPLS) capacidade de 100 Mbit/s (megabit por segundo), instalado no Data Center da contratada, podendo ser interligado em fibra óptica (FO) ou rádio frequência digital (RD) com as unidades da Prefeitura.

c) NS03 – Interligação de dados (MPLS) capacidade de 20 Mbit/s (megabit por segundo), instalado no Data Center da contratada, podendo ser interligado em fibra óptica (FO) ou rádio frequência digital (RD) com as unidades da Prefeitura.

5.1.4. Classes de Serviço (CoS – Classes of Service):

A infraestrutura de rede deverá ser compatível com:

a) RFC 2597 e 2598, diferentes CoS serão definidas, possibilitando a diferenciação entre o tráfego, para a implementação de QoS.

b) Prioridades e níveis de serviços, os diferentes tipos de tráfego da rede serão classificados em no mínimo 4 (quatro) CoS:

b1) Multimídia: aplicações sensíveis a retardo (delay) e variações de retardo (jitter), exigindo priorização de tráfego.

b2) Voz: aplicações críticas para a Prefeitura, exigindo entrega garantida, latência mínima e tratamento prioritário.

b3) Dados Prioritários: aplicações com grande volume de dados importantes, porém sem a necessidade de um tempo de resposta reduzido. Embora possam representar conteúdo importante, essas aplicações podem esperar por disponibilidade de recursos da rede, em horários com menor volume de transações, para serem efetuadas.

b4) Dados: todo tráfego não atribuído às três classes anteriores, sua finalidade é permitir uma alocação menor de recursos para os tráfegos não previstos ou ainda não identificados como tráfegos prioritários ou críticos. É preciso garantir que tal tráfego possa fluir se houver recursos disponíveis na rede, sem afetar negativamente as demais classes.

5.1.5. Conexão das unidades e pontos da prefeitura na infraestrutura de comunicação:

a) Deverá ser fornecida infraestrutura de rede que permita a conexão das redes locais das unidades e pontos de serviço da Prefeitura, interligando o equipamento roteador da rede local a uma porta de entrada exclusiva na infraestrutura de rede da contratada.

b) Cada local conectado à infraestrutura deverá receber uma identificação única, a ser utilizada tanto pela Prefeitura como pela Contratada.

c) A nomenclatura a ser utilizada na identificação de cada local deverá refletir a respectiva unidade, a ser definida em conjunto pela Prefeitura e pela Contratada.

d) A infraestrutura para interligação das unidades deverá ser através do meio de acesso descrito neste termo de Termo de Referência.

e) A infraestrutura de comunicação deverá ser fornecida dentro do ponto CONCENTRADOR, diretamente em fibra (1000Base-X) ou RJ45 (1000Base-T), ou ainda seus equivalentes para 10 Gigabits.

f) É responsabilidade da Contratada toda a infraestrutura necessária para a comunicação entre o BACKBONE e as unidades, com exceção do fornecimento de energia elétrica para alimentação dos equipamentos nas dependências das unidades da Prefeitura.

g) É responsabilidade da Contratada disponibilizar a infraestrutura locada (inclusive cabos e equipamentos), todos padronizados e com identificação, até o local indicado em cada unidade da Prefeitura.

h) Não é responsabilidade da Contratada a instalação de cabeamento e a configuração de equipamentos da rede local (LAN) de cada unidade, para ligação entre computadores, impressoras e servidores do local.

i) A contratada deverá identificar de forma visual e permanente cada equipamento instalado nas dependências da contratante, contendo o código ou etiqueta do serviço entregue no respectivo equipamento.

5.1.6. Características dos Roteadores a serem fornecidos:

a) Os roteadores deverão ser todos da mesma marca e fabricante e deverão atender às especificações definidas neste Termo de Referência.

- b) A versão do sistema operacional de cada roteador deverá ser a mais atual que esteja disponível e que suporte todas as características especificadas neste Termo de Referência.
- c) Cada roteador deverá ser fornecido com todos os acessórios e programas necessários à sua instalação, operação e monitoramento, inclusive com licenças as quais forem necessárias.
- d) Todos os equipamentos deverão suportar o respectivo tráfego da banda ocupada, sem degradação do desempenho e do QoS.
- e) A configuração de memória DRAM, memória Flash e CPU, de forma qualitativa e quantitativa, deverão ser compatíveis com as características descritas neste Termo de Referência para todos os roteadores.
- f) Cada roteador deverá suportar todo tráfego com a banda ocupada sem exceder 70% (setenta por cento) de utilização de CPU e memória durante a utilização normal do circuito.
- g) Caberá à Contratada substituir qualquer roteador sempre que forem excedidos os limites de 85% (oitenta e cinco por cento) de utilização de CPU ou memória.
- h) A substituição ocorrerá mediante prévio acordo com a Prefeitura e sem qualquer ônus.
- i) Os roteadores deverão ter as seguintes características mínimas técnicas:
 - i1) Suportar o padrão IEEE 802.1p.
 - i2) Possuir porta LAN com detecção automática de velocidade e suporte aos padrões 802.3, 802.3u, 802.3q, 802.1d, 802.1s e 802.1w.
 - i3) Suportar a aplicação de QoS (Quality of Service) para tráfego de dados e multimídia (incluindo voz e vídeo), de forma a garantir a prioridade na transmissão de determinadas aplicações.
 - i4) Suportar a configuração de métodos de priorização de tráfego por tipo de protocolo, endereçamento IP ou serviços da pilha TCP/IP.
 - i5) Suportar a implementação de Listas de Controle de Acesso (ACLs).
 - i6) Suporte ao protocolo de gerenciamento SNMP nas versões 2 ou 3, e à especificação MIB-II, implementados em conformidade com as RFCs 1157, 1213 e 2570, respectivamente.
 - i7) Suportar as MIBs para QoS, permitindo a monitoração de parâmetros de QoS.
 - i8) Possuir capacidade de geração e armazenamento de logs de eventos.
 - i9) Possibilitar configuração remota segura, via SSH ou interface web com HTTPS.
 - i10) Implementar cliente NTP (Network Time Protocol), conforme RFC 1305 ou SNTP (Simple Network Time Protocol), conforme RFC 2030.
 - i11) Possuir interface para gerenciamento local, via console físico ou porta dedicada.
 - i12) Trabalhar com tensões de entrada de 110 VCA e 220 VCA, e detecção automática de tensão.
 - i13) Os roteadores deverão possuir no mínimo: 02 (duas) interfaces Gigabit Ethernet 10/100/1000 Mbps, com conector RJ-45 para conexão LAN e para WAN; ou 01 (uma) interface Gigabit Ethernet 10/100/1000 Mbps, com conector RJ-45 para conexão LAN, e 01 (uma) interface SFP (porta para transceptor óptico).

5.2. Conexão Dedicada à Internet

5.2.1. Características gerais

Deverá ser provida a Conexão à Internet com velocidade de 500 Mbps, o qual deverá ser instalado no DATA CENTER da CONTRATADA, e entregue juntamente ao FIREWALL, estando este alcançável a todas as unidades da Prefeitura, com objetivo de conectar a rede interna do município a rede mundial de computadores, com as seguintes características:

- a) Garantia de 100% (cem por cento) da velocidade contratada para Download e Upload;
- b) A banda deverá ser bidirecional (full-duplex);
- c) Fornecer endereçamento IP válido e fixo através de bloco IPv4 /28 (16 IP livres);
- d) Fornecer a configuração de resolução de DNS Reverso;
- e) Entregar o link já roteado em formato Ethernet;
- f) Os índices de latência e perdas de pacotes deverão ser de no máximo o especificado a seguir, salvo momentos em que o link esteja com a utilização de 100% da banda contratada (saturado), período em que os índices não serão considerados para fins de penalização.
- g) Em caso de Desastre, deverá ser ativado um link de internet no Data Center secundário com as mesmas características deste no prazo máximo de 1 hora.

5.2.2. Testes e validações

- a) Para evitar fatores externos que podem influenciar os resultados do teste de velocidade, somente uma máquina deverá estar ligada diretamente ao modem/roteador do fornecedor do link, através de um cabo de rede (não será utilizada rede sem fios), certificando-se que a mesma não esteja executando programas que ocupem a rede, CPU e memória.
- b) A ferramenta utilizada para aferição dos testes de velocidade será o SIMET (Sistema de Medição de Tráfego Internet), disponível na Web no endereço: <http://simet.nic.br>. Essa ferramenta é utilizada pelo INMETRO para avaliar a conexão brasileira, além de ser homologada pelo CGI (Comitê Gestor da Internet no Brasil).
- c) No fornecimento do link de acesso à Internet, manter a inexistência de qualquer tipo de bloqueio na comunicação. Permitindo assim a implementação de serviços, como videoconferência, VoIP, VPN, etc.

5.3. Appliance Firewall para Gerenciamento da Internet

Fornecer 1 equipamento de Appliance Firewall (hardware/software) dedicado para gerenciamento, controle e prevenção de ameaças na Internet, o qual deverá ser instalado no Data Center da CONTRATADA, ou excepcionalmente da CONTRATANTE, estando este conectado a todas as unidades interligadas da Prefeitura, de acordo com as seguintes características:

5.3.1. Características Gerais e Capacidade

- a) Suporte para no MÍNIMO:
 - a1. 10 Gbps de taxa de transferência de Firewall (Throughput).
 - a2. 1 Gbps de taxa de transferência para VPN.

a3. 2 Gbps de taxa de transferência para IPS.

a4. 2 Gbps de taxa de transferência para Antivírus.

b) Suporte para no MÍNIMO 4.000.000 conexões simultâneas e 120.000 novas conexões/segundo.

c) Deve ter capacidade para operar com pelo menos 5 (cinco) segmentos de redes distintas fisicamente através de portas, classificadas e configuradas por zonas WAN, LAN, DMZ, VPN e WIFI, conforme a necessidade.

d) Deve possuir capacidade de criar e gerenciar VLANs.

e) Deve possuir arquitetura de armazenamento baseada em SSD.

f) Deve permitir a conexão simultânea de vários administradores.

g) Deve possuir capacidade de backup das configurações, de forma automatizada, no dispositivo físico (appliance) e remoto.

h) Deve possuir capacidade de envio do backup remoto através de FTP, SFTP, SCP, SMTP, etc.

i) Deve possuir suporte à administração via comunicação segura, HTTPS, SSH e console, devendo os protocolos inseguros (ex: Telnet, HTTP) estarem desabilitados por padrão.

j) Deve possuir acesso à interface de configuração e administração via web em português, com total capacidade sobre os recursos e funcionalidades existentes.

k) Deve possuir garantia e atualizações periódicas do software durante a vigência do contrato de prestação de serviços.

l) Deverá existir o serviço de Disaster Recovery do Firewall, garantindo que, pelo menos, a cada 24 horas, o conteúdo integral do mesmo e as configurações do serviço estejam replicados em armazenamento secundário. E em caso de Desastre, o tempo máximo de disponibilidade para assumir serviço no armazenamento secundário deve ser conforme definido no SLA/Níveis mínimos de serviço.

m) Deve possuir dimensões de 1U, para instalação em rack.

n) Deve possuir alimentação elétrica via fonte AC/DC de 100 a 240 V.

o) Deve permitir instalação dupla de fonte de alimentação

p) Deve possuir interface exclusiva para gerência.

5.3.2. Especificações Gerais

a) A solução proposta deve fornecer logs e relatórios.

b) A solução proposta deve cumprir as normas da FCC (Federal Communications Commission);

c) A solução proposta deve funcionar como servidor proxy HTTP autônomo com Firewall integrado, Antivírus, filtragem de conteúdo, IPS.

d) A solução proposta deve suportar a configuração política baseada em usuários para segurança e gerenciamento de internet.

e) A solução proposta deve fornecer os relatórios de appliance baseados no usuário, não só baseado em endereço IP.

- f) A solução proposta deve suportar administração via comunicação segura HTTPS, SSH e Console.
- g) A solução proposta deve ser capaz de exportar e importar backup de configurações, incluindo os objetos de usuário.
- h) A solução proposta deve suportar Route (Layer 3) / modo transparente (Layer 2).
- i) A solução proposta deve apoiar a integração com o Windows NTLM, Active Directory, LDAP, RADIUS ou banco de dados local para autenticação do usuário.
- j) A solução proposta deve suportar Parent Proxy com suporte a IP / FQDN.
- k) A solução proposta deve suportar NTP.
- l) A solução proposta deverá suportar a funcionalidade de unir usuário/ip/mac para mapear nome de usuário com o endereço IP e endereço MAC por motivo de segurança.
- m) A solução proposta deve suportar o tempo de inatividade do usuário, inativo/ocioso, após o qual o usuário será desconectado e precisará se autenticar novamente.
- n) A solução proposta deve suportar a criação de usuário baseada em ACL (Access Control List, ou Lista de Controle de Acesso) para fins de administração.
- o) A solução proposta deve suportar instalação de LAN by-pass no caso do appliance estar configurado no modo transparente.
- p) A solução proposta deve suportar SNMP v1, v2c e v3.
- q) A solução proposta deve suportar Balanceamento de carga (Load Balance) e distribuição de sinal em caso de falha (Failover) para múltiplos links e ISPs;
- r) A solução proposta deve suportar o roteamento explícito com base em origem, destino, nome de usuário, aplicação.
- s) A solução proposta deve suportar algoritmo round robin para Load Balance.
- t) A solução proposta deve fornecer opção para criar condição de Failover em ICMP, TCP ou UDP para detectar falha de conexão ISP.
- u) A solução proposta deve enviar e-mail de alerta ao administrador sobre a mudança do status de gateway.
- v) A solução proposta deve ter Balanceamento de Carga (Load Balance) do gateway, ativo/ativo (Round Robin), ativo/passivo e suporte a Failover.

5.3.3. Filtro de pacotes

- a) A solução proposta deve ser um standalone appliance com OS integrado.
- c) A solução proposta deve suportar stateful inspection com o usuário baseado one-to-one e dinâmico NAT, PAT.
- d) A solução proposta deve suportar a identidade do usuário como critérios de Origem/Destino IP/Subnet /group, porta de destino na regra de firewall.
- e) A solução proposta deve facilitar a aplicação de políticas unificadas de ameaças como AV/AS, IPS, filtro de conteúdo, políticas de largura de banda e política de decisão de roteamento baseado em regras de

firewall para facilidade de uso, também controles unificado de ameaças deve ser aplicado sobre o tráfego entre zona.

- f) A solução proposta deve suportar a arquitetura de segurança da zona multiusuário definida.
- g) A solução proposta deve ter predefinida aplicação baseado na porta/assinatura e também suportar a criação de aplicativo personalizado baseado na porta/número de protocolo.
- h) A solução proposta deve suportar inbound NAT com balanceamento de carga.
- i) A solução proposta deve suportar 802.1q suporte marcação VLAN.
- j) A solução proposta deve suportar roteamento dinâmico como RIP1, RIP2, ISPF, BGP4.
- k) O sistema proposto deve fornecer Mac Address (Endereço físico) regra de firewall baseada em fornecer OSI Layer 2 a Camada de aplicação 7.

5.3.4. IPS (Intrusion Prevention System)

- b) A solução proposta deve ter assinatura baseada em protocolo e sistema de prevenção de intrusão baseada em anomalia.
- c) A solução proposta deve ter mais de 3500 assinaturas de banco de dados.
- d) A solução proposta deve apoiar a criação da assinatura IPS personalizada.
- e) A solução proposta deve apoiar a criação de uma política múltipla IPS para a zona diferente, em vez de política geral em nível de interface.
- f) A solução proposta deve apoiar a opção de configuração para ativar/desativar categoria/assinatura para reduzir a latência de pacotes.
- g) A solução proposta deve ter o nome de usuário junto com IP em IPS alertas e relatórios.
- h) A solução proposta deve fazer automaticamente a atualização a partir do servidor de atualização.
- i) A solução proposta deve apoiar o bloqueio dos Anonymous Proxy HTTP aberto rodando na porta 80 ou qualquer outra porta e também deve apoiar cliente baseado em proxy aberto como o Ultrasurf.
- j) A solução proposta deve ser capaz de detectar e bloquear P2P aplicação baseada em mensageiro instantâneo como skype e conhecidos aplicativos de bate-papo como WLM, Rediffbol, Discord, etc
- k) A solução proposta deve gerar os alertas para ataques.
- l) A solução proposta deve gerar relatórios históricos baseados nos maiores alertas, maiores atacantes, principais vítimas.

5.3.5. Gateway Antivírus

- a) A solução proposta deve ter uma solução integrada de antivírus.
- c) A solução proposta deve funcionar como SMTP proxy não como MTA ou servidor de retransmissão.
- d) A solução proposta deve suportar a verificação SMTP, POP3, IMAP, FTP, HTTP, FTP através de protocolos HTTP.
- e) O banco de dados básico de assinatura de vírus da solução proposta deve incluir a lista de assinaturas e variantes completas, bem como de malware como phishing e spyware.

- f) A solução proposta deve ter facilidade para adicionar assinatura/disclaimer nos e-mails.
- g) A solução proposta deve apoiar o bloqueio dos arquivos dinâmicos/executáveis com base na extensão do arquivo.
- h) Para o tráfego SMTP, a solução proposta deve apoiar as seguintes ações para anexos infectados, suspeitos ou protegidos.
 - h1. Rejeitar e-mail.
 - h2. Entregar o correio sem anexo.
 - h3. Entregar e-mail original.
 - h4. Notificar o administrador.
- i) A solução proposta deve suportar várias políticas de antivírus para endereço de e-mail ou grupo de endereços, remetente/destinatário, configuração de notificação, quarentena, configuração e extensão do arquivo, em vez de definir a política única.
- j) A solução proposta deve atualizar a assinatura do banco de dados em uma frequência de menos de uma hora e ele também deve suportar atualização manual.
- k) Para o tráfego POP3 e IMAP, o sistema proposto deve retirar o anexo infectado e enviar notificação ao destinatário e administrador.
- l) A solução proposta deve analisar o tráfego HTTP baseado no nome de usuário, de origem/destino endereço IP ou URL baseada em expressão regular.
- m) A solução proposta deve fornecer a opção para ignorar a verificação de tráfego HTTP específico.
- n) A solução proposta deve apoiar em tempo real e modo de carga para verificação de vírus HTTP.
- o) A solução proposta deve fornecer histórico de relatórios com base no nome de usuário, endereço IP do remetente, destinatário e nome dos vírus.

5.3.6. Solução de Proxy – Filtro Web

- b) A solução proposta deve ser integrada com banco de dados local em vez de requisitar ao banco de dados hospedado remotamente.
- c) A solução proposta deve funcionar como proxy HTTP autônomo.
- d) A solução proposta deve ter pelo menos 80 categorias no banco de dados web e pelo menos 40 milhões de endereços URL.
- e) A solução proposta deve possuir as seguintes características:
 - e1. Deve ser capaz de bloquear URLs baseado em HTTPS com a ajuda de Certificados.
 - e2. Deve ser capaz de bloquear URL com base em expressão regular.
 - e3. Devem apoiar a lista de exclusão com base na expressão regular.
 - e4. Deve ter suporte para bloquear qualquer carregamento de tráfego HTTP.
 - e5. Deve ser capaz de bloquear sites em cache no Google com base na categoria.

- e6. Deve ser capaz de bloquear websites ou conteúdos hospedados em CDN (Content Delivery Network) como Akamai.
- e7. Deve ser capaz de identificar e bloquear as solicitações que chegam através de servidor proxy na base do nome de usuário e endereço IP.
- e8. Deve ser capaz de identificar e bloquear pedido de tradução de URL.
- f) A solução proposta deve suportar os recursos de bloqueio de controle de aplicativos.
- g) Deve ser capaz de bloquear aplicativos bate-papo conhecidos como Yahoo, MSN, AOL, Google, Rediff, Jabber, Discord, etc.
- h) Devem suportar o bloqueio de transferência de arquivos do aplicativo de chat conhecido e do protocolo FTP.
- i) A solução proposta deve bloquear HTTP ou HTTPS baseado na solicitação de proxy anônimo disponível na internet.
- j) A solução proposta deve oferecer opção de personalizar mensagem de acesso negado para cada categoria.
- k) A solução proposta deve ser compatível com definição de políticas de acesso e navegação segura, para proteger menores em ambientes como escolas e bibliotecas (por exemplo: CIPA-Children's Internet Protection Act).
- l) A solução proposta deve ter categorias específicas que reduzem a produtividade dos funcionários, a largura de banda dos sites e sites maliciosos.
- m) A solução proposta deve ser capaz de gerar relatórios com base no nome de usuário, endereço de IP, URL, grupos, categorias e tipo de categorias.
- n) A solução proposta deverá apoiar critérios de pesquisa em relatórios para encontrar os dados relevantes.
- o) A solução proposta deve apoiar a criação de uma política cíclica diária/semanal/mensal/anual para acesso à internet em usuários individuais/grupo de usuários.
- p) A solução proposta deve apoiar a criação de política de tempo de acesso à Internet para usuários individuais ou grupos.
- q) A solução proposta deve apoiar a criação de uma política de transferência de dados diária/semanal/mensal/anual para o usuário individual ou grupo.
- r) A solução proposta deve suportar a criação de uma política de transferência de dados cíclica diária/semanal/mensal/anual para o usuário individual ou grupo.
- s) A solução proposta deve ter gerenciamento de banda integrado.
- t) A solução proposta deve ser capaz de definir a largura de banda garantida e estourável por usuário/IP/Aplicação em base individual ou compartilhado.
- u) A solução proposta deve oferecer opção de configurar diferentes níveis de prioridade para aplicação crítica.

v) A solução proposta deve fornecer opção para definir a largura de banda diferente para agendamento diferente em uma única política e largura de banda deve mudar conforme cronograma on the fly.

w) A solução proposta deve fornecer categoria de gerenciamento de banda baseado em web e priorização.

5.3.7. VPN (Virtual Private Network)

a) A solução proposta deve ser VPNC básico de interoperabilidade e AES certificado de interoperabilidade.

b) A solução proposta deve suportar IPSec (Net-to-Net, Host-to-Host, ou client-to-site), L2TP e conexão VPN PPTP.

c) A solução proposta deve apoiar DES, 3DES, AES, Twofish, Blowfish, o algoritmo de Serpent encryption.

d) A solução proposta deve suportar chaves pré-compartilhadas e autenticação baseada em certificado digital.

e) A solução proposta deve apoiar as autoridades de certificação externa.

f) A solução proposta deve apoiar facilidade de exportação de configuração client-to-site para a configuração VPN sem problemas em Laptop/Desktop remoto.

g) A solução proposta deve apoiar os clientes VPN IPSec comumente disponíveis.

h) A solução proposta deve apoiar a autoridade local de certificados e devem suportar criar/renovar/Excluir certificado autoassinado.

i) A solução proposta deve suportar failover VPN para fins de redundância, quando mais de uma conexão está mesmo no grupo e uma conexão cair, deve mudar automaticamente para outra conexão e reduzir o tempo de inatividade.

j) A solução proposta deve pré-carregar certificados de terceiros, incluindo a VeriSign / Entrust.net / Microsoft e fornecer facilidade de upload de qualquer outra autoridade de certificação.

l) A solução proposta deve suportar Threat free túnel VPN Ipsec/L2TP/PPTP.

5.3.8. Logging e Relatórios

a) A solução proposta deve ter integrado nos relatórios do appliance.

b) A solução proposta deve apoiar modelos diferentes para visualizar os relatórios.

c) A solução proposta deve permitir salvar relatórios em formatos HTML, CSV e PDF.

d) A solução proposta deve suportar o registro de antivírus, Anti-spam, filtro de conteúdo, IPS, Firewall atividade no servidor syslog.

e) A solução proposta deve fornecer relatórios detalhados de todos os arquivos enviados via protocolo HTTP ou HTTPS. O relatório deve incluir nome de usuário/endereço IP/URL/nome/data e hora do arquivo.

f) A solução proposta deve fornecer relatórios de transferência de dados na base de aplicação, nome de usuário, IP address.

g) A solução proposta deve fornecer relatórios de conexão completos para o usuário, IP de origem, IP de destino, porta de origem, porta de destino ou protocolo.

h) A solução proposta deve ter facilidade de enviar relatórios sobre o endereço e-mail ou no servidor FTP.

- i) A solução do sistema proposto deve fornecer ou permitir criar relatórios regulatórios de conformidade.
- j) A solução proposta deve apoiar a facilidade de auditoria para rastrear todas as atividades realizadas pela appliance de segurança.
- k) A solução proposta deve apoiar vários servidores syslog para log remoto.
- l) A solução proposta deverá apresentar o registro de informações de todos os módulos do servidor syslog.
- m) A solução proposta deve ter opção configurável para enviar relatórios sobre o endereço de e-mail designado.
- n) A solução proposta deve ser capaz de fornecer relatórios detalhados sobre todos os e-mails que passam pelo Firewall.
- o) A solução proposta deve fornecer os relatórios de todas as tentativas bloqueadas feitas por usuários/IP Address.

5.4. Infraestrutura para rede WIFI interna

O Ponto de Conectividade WIFI é definido como um conjunto agrupado de serviços e equipamentos para prover conectividade à rede corporativa da Prefeitura (redes “funcionários” e “corporativo”), bem como visitantes mediante identificação e/ou credenciamento (rede “visitantes”), e deverá atender aos seguintes requisitos mínimos:

5.4.1. Características mínimas do WIFI:

- a) O equipamento deverá suportar a criação e operação de múltiplos SSIDs, sendo exigido o suporte a pelo menos 6 SSIDs conforme necessidade da contratante, cada um vinculado a uma VLAN distinta, para possibilitar a separação lógica de redes como, por exemplo, “visitantes”, “funcionários”, “corporativo”, “equipamentos”, etc.
- b) Deverá permitir a ocultação do SSID;
- c) Para a rede de Visitantes, deverá operar no modo hot-spot com portal de autenticação/identificação centralizada dos usuários, através de formulário de identificação com CPF, ou login integrado a outras redes sociais, como por exemplo, o Facebook.
- d) Os dados de credenciais dos Visitantes deverão ser armazenados em banco de dados em armazenamento da contratada, pelo período de 1 (um) ano, e acessíveis à equipe de TI do Município através de painel Web.
- e) Para a rede Administrativa, deverá suportar autenticação de camada 2, através dos protocolos EAP-TLS com integração com RADIUS, LDAP e Active Directory;
- f) Suportar o padrão de segurança WPA3;
- g) O sistema de Hot-Spot deverá realizar o controle da conexão com os seguintes parâmetros:
 - g.1) Controle de tempo de conexão por MAC dos equipamentos;
 - g.2) Controle de banda de cada conexão;
 - g.3) Controle de tempo de uso;
 - g.4) Portal de acesso customizado com logotipo e campos de inserção de dados;

- g.5) O sistema portal de autenticação (hot-spot) deve permitir a configuração e distribuição de comprovantes (vouchers) de autenticação dos usuários de forma temporária, por determinadas horas e/ou dias;
- h) Deve ser compatível com os protocolos SNMP v1, v2 e v3;
- i) O equipamento deve permitir, quando em uma VLAN, o isolamento entre os dispositivos dos usuários;
- j) Deve permitir configuração de obtenção de endereço IP de forma automática, através de DHCP;
- k) Deve possuir funcionalidades de Qualidade de Serviço (QoS);

5.4.2. Características da infraestrutura fornecida:

Fornecimento de Access Points Indoor do tipo "Teto/Parede" com as seguintes características:

- a) Infraestrutura locada (inclusive cabeamento e equipamentos), conforme necessidade da contratante, desde o ponto de entrada da conexão (fibra óptica ou rádio) até o local onde será instalado o roteador WIFI.
- b) Os cabos a serem instalados devem ser categoria CAT6 ou superior, e tipo LSZH ("Low Smoke Zero Halogen" ou em português "Baixa Emissão de Fumaça e Sem Halogênios", projetado para reduzir a produção de fumaça e gases tóxicos em caso de incêndio).
- c) Suporte aos protocolos WIFI 802.11a/b/g/n/ac/ax (WIFI 6), operando nas bandas de 2,4 GHz e 5 GHz, com tecnologia MIMO ou MU-MIMO 2x2 ou superior, e com recursos de eficiência como OFDMA e TWT (Target Wake Time).
- d) Suporte a alimentação por PoE;
- e) Capacidade de pelo menos 50 conexões simultâneas com intensidade mínima de -65 dBm em pelo menos 90% das áreas de uso previstas em cada unidade;
- f) Provisionamento de configurações dos equipamentos por sistema centralizado "controller" a ser fornecido pela CONTRATADA e com acesso à equipe de TI do Município;
- g) Deverá existir o serviço de Disaster Recovery do "Wifi Controller", garantindo que, pelo menos, a cada 24 horas, o conteúdo integral do mesmo e as configurações do serviço estejam replicados em armazenamento secundário. E em caso de Desastre, o tempo máximo de disponibilidade para assumir serviço no armazenamento secundário deve ser conforme definido no SLA/Níveis mínimos de serviço.
- h) A conexão à Internet será provida através do Link dedicado, item 4 deste Termo de Referência.

5.5. Condições de fornecimento dos Serviços

- a) A Contratada deverá efetuar a manutenção dos serviços, que inclui reposição dos equipamentos, peças e infraestrutura, como cabos, conectores, adaptadores, entre outros. Os equipamentos defeituosos, caso não possam ser reparados, deverão ser substituídos atendendo ao SLA contratado.
- b) Todas as soluções que contemplam os serviços acima deverão incluir Hardware, Software, Serviços de Instalação e Configuração, suporte técnico 24/7, isto é, durante as 24 (vinte e quatro) horas do dia nos 7 (sete) dias da semana.
- c) Os custos com deslocamentos e estadia de técnicos, transporte do equipamento serão integralmente assumidos pela empresa contratada.

d) A contratada deverá fornecer cronograma de implantação, conforme descrito no item 7.2. Cronograma de Entrega dos Serviços, contendo detalhes das atividades previstas com sugestões de prazos que serão validados pela equipe de TI.

e) Os serviços deverão ser providos por meio de infraestrutura física instalada nas dependências da contratada, da contratante ou em local indicado pela contratante, garantindo pleno funcionamento, monitoramento, gerenciamento e suporte técnico necessários para a operação dos recursos contratados.

f) Em todos os serviços, os logs de eventos devem ser armazenados por pelo menos 7 (sete) dias, e os relatórios de serviços/recursos utilizados por pelo menos 90 (noventa) dias.

6. QUANTIFICAÇÃO

A contratação será realizada sob a forma de empreitada por preço unitário, caracterizando-se como fornecimento contínuo e sob demanda, com pagamento proporcional ao consumo efetivamente realizado em cada período mensal de medição.

Os itens 1 (NS01 – Infraestrutura de Comunicação com capacidade de 1 Gbps), 4 (Link de Acesso à Internet Dedicada) e 5 (Firewall) serão contratados de forma fixa, com fornecimento contínuo e permanente durante a vigência do contrato.

Já os itens 2 (NS02 – 100 Mbps), 3 (NS03 – 20 Mbps) e 6 (WIFI Indoor) serão ativados e fornecidos por demanda, de acordo com a necessidade da contratante.

6.1. Infraestrutura de comunicação para interligação das Unidades

Item	Descrição do Serviço	Quantidade/Mês
1	Infraestrutura de Comunicação com capacidade de 01 Gbps Full Duplex, instalado no DC da contratada, com dupla abordagem em fibra óptica até Centro Administrativo Município. (NS01)	01
2	Infraestrutura de Comunicação com capacidade 100 Mbps Full Duplex (NS02)	65
3	Infraestrutura de Comunicação com capacidade 20 Mbps Full Duplex (NS03)	85

6.2. Conexão à Internet:

Item	Descrição	Quantidade/Mês
4	Conexão Internet Dedicada com velocidade de 500 Mbps Full Duplex	01

6.3. Firewall:

Item	Descrição	Quantidade/Mês
5	Firewall	01

6.4. Infraestrutura para rede WIFI indoor:

Item	Descrição	Quantidade/Mês
6	Ponto de WIFI indoor	440

7. CARACTERÍSTICAS DA EXECUÇÃO DOS SERVIÇOS

7.1. Características gerais:

7.1.1. Não poderão ser definidos pontos de concentração dos serviços que possam estabelecer estrangulamento das capacidades de transmissão de dados.

7.1.2. Os serviços prestados nos locais especificados inicialmente poderão sofrer alteração de endereço de acordo com a necessidade da Administração Pública no decorrer do período contratado.

7.1.3. É de responsabilidade da Contratada o fornecimento de todos os equipamentos e meios necessários para promover os serviços a serem disponibilizados completamente operacionais e com o custo já incluso no valor mensal a ser pago pela Prefeitura.

7.1.4. Cabe à contratada a instalação, configuração e manutenção/substituição dos equipamentos necessários para a operacionalização dos serviços.

7.1.5. Todos os serviços deverão estar disponíveis para operação durante as 24 (vinte e quatro) horas por dia, todos os dias do ano, com disponibilidade mínima de 99,00% (noventa e nove por cento) ao mês, quando não mencionados nas características específicas, excetuando-se quando a CONTRATADA informar janela de manutenção com pelo menos 3 (três) dias úteis de antecedência, e no período noturno entre 22h e 6h;

7.1.6. A contratada deverá fornecer um software em português, devidamente licenciado, para monitoramento gráfico do tráfego de cada conexão em tempo real contendo relatórios referente à sua utilização de cada circuito de dados e Internet.

7.1.7. Todos os circuitos de comunicação de dados e Internet deverão ser disponibilizados prevendo a possibilidade de expansão futura da velocidade de transmissão, para, pelo menos, o dobro da velocidade inicial contratada, não tendo assim limitações físicas para tal situação.

7.1.8. Fornecer todos os equipamentos necessários para o funcionamento dos serviços contratados, incluindo todos os custos referentes a atualizações tecnológicas, substituição de equipamentos e suporte técnico.

7.1.9. A contratada deverá comparecer através de seu representante em todas as reuniões e outras atividades de coordenação, planejamento, acompanhamento e avaliação que venham a ser convocadas previamente pela Prefeitura.

7.1.10. A contratada deverá realizar a instalação e configuração de todos os serviços on-site (nas dependências da Prefeitura) com técnicos identificados e mediante agendamento prévio junto a equipe de Tecnologia da Informação (TI) da Prefeitura e junto à Secretaria gestora do respectivo contrato.

7.1.11. A Contratada deverá prestar suporte para a equipe de TI da Prefeitura e os funcionários por ela indicados, de forma a habilitá-los ao pleno uso e gerência dos serviços contratados.

7.1.12. Durante a vigência do contrato deverão estar incluídas atualizações e garantia dos softwares necessários para os serviços prestados.

7.1.13. Nenhum dos modelos ofertados de WIFI Access Point e Firewall poderá estar listado no site do fabricante em listas de Fim de suporte ou de comercialização - EOL (end-of-life) e EOS (end-of-sale) - na data da proposta.

7.1.14. Fornecer suporte técnico, conforme os Níveis Mínimos de Serviço (SLA) deste Termo de Referência sem custo adicional.

7.1.15. Durante o período de vigência do contrato, a CONTRATADA deverá sugerir mudanças e melhorias na arquitetura da solução, quando identificada uma oportunidade a fim de reduzir custos e otimizar desempenho.

7.2. Cronograma de Entrega dos Serviços

7.2.1. A CONTRATADA deverá apresentar, até o 3º dia útil, após assinatura do contrato, um Plano de Implantação Detalhado, com datas específicas, atividades técnicas e responsáveis, que será aprovado pela equipe técnica da CONTRATANTE. Aprovado o referido Plano, será emitido o Termo de Autorização para Início da Implantação dos Serviços.

7.2.2. O prazo total para entrega e entrada em operação do ambiente completo é de até 90 (noventa) dias corridos, a contar da assinatura do Termo de Autorização para Início da Implantação dos Serviços.

7.2.3 O cronograma de ativação dos serviços deverá seguir os seguintes prazos na ordem dos itens conforme a seguinte relação:

Item	Prazo de Ativação*
Item 1. Infraestrutura de Comunicação com capacidade 1 Gbps Full Duplex (NS01) Item 4. Conexão Internet Dedicada Item 5. Firewall	Até 15 dias
Item 2. Infraestrutura de Comunicação com capacidade 100 Mbps Full Duplex (NS02)	Até 60 dias

Item 3. Infraestrutura de Comunicação com capacidade 20 Mbps Full Duplex (NS03)	
Item 6. Infraestrutura para rede WIFI interno	Até 90 dias
Itens a serem ativados para atender às unidades da Secretaria de Educação (SEE), até o vencimento do Contrato nº 097/PGM/2022, conforme a lista de unidades de entrega dos serviços: Item 2. Infraestrutura de Comunicação com capacidade 100 Mbps Full Duplex (NS02), Quantidade: 44 Item 3. Infraestrutura de Comunicação com capacidade 20 Mbps Full Duplex (NS03), Quantidade: 6 Item 6. Infraestrutura para rede WIFI interno, Quantidade: 248	Até 22 de Maio de 2026

(*) O prazo de ativação é contado a partir da expedição do Termo de Início dos Serviços de Implantação, sendo que os prazos citados acima não são cumulativos, sendo o prazo máximo de conclusão de todas as ativações solicitadas em até 90 dias. Os prazos de ativação poderão ser prorrogados mediante solicitação e justificativa formal da contratada e aceite da contratante.

7.2.3. Realizada a implantação, será emitido o Termo de Aceitação e Recebimento Definitivo dos Serviços.

7.2.4. Todos os marcos de entrega do Plano devem ser documentados com termos de aceite parcial, emitidos pela CONTRATANTE, como condição para o prosseguimento do cronograma.

7.2.5. O cronograma de entrega dos serviços deverá conter ao menos as seguintes etapas:

7.2.5.1. Reunião inicial de alinhamento técnico com a equipe da Prefeitura;

7.2.5.2. Entrega da infraestrutura contratada com acesso funcional à rede corporativa e à internet em cada uma das unidades;

7.2.5.3. Execução de testes de conectividade, performance e segurança, com acompanhamento da equipe técnica da Prefeitura;

7.2.5.4. Entrega dos acessos administrativos e documentação técnica do ambiente de monitoramento;

7.2.5.5. Início da operação assistida (com suporte técnico ativo para acompanhamento do funcionamento do ambiente);

7.2.5.6. Finalização da implantação e assinatura do Termo de Aceitação e Recebimento Definitivo dos Serviços pela CONTRATANTE.

7.2.6. Os serviços serão recebidos definitivamente por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço.

7.2.7. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

7.2.8. O prazo para início da contagem dos períodos de faturamento e pagamento da CONTRATADA somente terá início a partir da assinatura do Termo de Aceitação e Recebimento Definitivo dos Serviços pela CONTRATANTE, atestando que todos os serviços contratados foram entregues em conformidade com os

requisitos técnicos, funcionais e de segurança estabelecidos neste Termo de Referência.

7.3. Painel de Transparência dos Serviços

A contratada deverá fornecer um painel de transparência dos serviços prestados contendo todos os indicadores solicitados neste documento e possibilitar a consulta on-line, a qualquer tempo, de todas as solicitações (chamados), com detalhes de data/hora de abertura, classificações, ações executadas e prazos de atendimento.

7.4. Central de atendimento 24x7x365

7.4.1. A CONTRATADA deverá disponibilizar um centro de atendimento único para recebimento dos chamados de manutenção técnica, com chamadas telefônicas locais ou gratuitas (0800) e e-mail para recebimento de chamados, com fornecimento de número de protocolo para acompanhamento.

7.4.2. A CONTRATADA deverá fornecer e manter atualizada uma lista de recorrência ("escalation list"), com contatos internos para casos de demora no restabelecimento do serviço.

7.4.3. A CONTRATADA deverá disponibilizar acesso ao sistema de gerenciamento dos incidentes da rede contratada pela PMSCS, devendo ser possível acompanhar pelo menos as seguintes informações:

a) Identificação do nó da rede afetado, data de abertura e fechamento.

b) Histórico do incidente, com descrição das atividades executadas pela CONTRATADA.

7.4.4. A CONTRATADA deverá realizar o monitoramento pró-ativo dos pontos, atuando na resolução de incidentes sem abertura de chamado pela PMSCS.

7.4.5. A CONTRATADA deverá prestar manutenção preventiva da rede, efetuando testes de verificação de qualidade da conexão física e lógica, sempre que houver solicitação da PMSCS, sem custos adicionais.

7.4.6. A CONTRATADA deverá realizar a manutenção corretiva do hardware, no local onde os equipamentos estiverem instalados (on-site) de modo a manter os circuitos ativos, devendo substituir os equipamentos cujo conserto necessita ser realizado em laboratório por outro com as mesmas características do original.

7.4.7. Nas situações de falha na comunicação, a CONTRATADA deverá comprovar a tentativa de acesso ao seu roteador na localidade do incidente por meio de um "visto" dado por um funcionário identificado da PMSCS na localidade, se a unidade estiver fora do horário de funcionamento e sem um funcionário identificado da PMSCS, deverá entrar em contato com um membro da "equipe técnica de acompanhamento dos serviços" através de contato telefônico que será informado oportunamente.

7.4.8. Nos casos em que for inviável o acesso às dependências da PMSCS para a solução de incidentes, a CONTRATADA deverá demonstrar que verificou possíveis causas na sua infraestrutura, reunindo evidências técnicas dessas ações, com registros por e-mail para a PMSCS. Comprovado que a causa provável do problema necessita de intervenção física, será interrompida a contagem do prazo de resolução até o horário de início do expediente da respectiva dependência da PMSCS do próximo dia útil.

7.4.9. No caso dos enlaces do nó central, a PMSCS poderá providenciar acesso em horários extraordinários. Para tanto, a CONTRATADA deverá fornecer e manter atualizada uma lista de funcionários autorizados a realizar o atendimento.

7.4.10. Mensalmente, a CONTRATADA deverá enviar relatórios detalhados do seu sistema de monitoramento da infraestrutura de rede contratada, bem como dos chamados e incidentes do período de competência antes da data de pagamento, para conferência e realização dos descontos cabíveis.

7.5 Segurança

7.5.1. A CONTRATADA deverá guardar sigilo sobre dados e informações obtidos em razão da Execução dos serviços contratados ou da relação contratual mantida com a Prefeitura Municipal de Santa Cruz do Sul.

7.5.2. A CONTRATADA deverá assinar um Termo de Confidencialidade com a Prefeitura Municipal de Santa Cruz do Sul, como condição para assinatura do contrato, comprometendo-se a manter sob absoluto sigilo todas as informações às quais tiver acesso em razão da execução contratual. A obrigação de sigilo será estendida a todos os colaboradores e eventuais prestadores de serviço envolvidos na execução do contrato, sendo de responsabilidade da CONTRATADA garantir a sua observância. O descumprimento desta obrigação poderá ensejar penalidades contratuais, civis e administrativas, nos termos da legislação vigente.

7.6 Encerramento do Contrato

7.6.1 A CONTRATADA deverá manifestar-se por escrito com antecedência mínima de 180 (cento e oitenta) dias do término contratual, a intenção de não renová-lo, e justificativa.

8 NÍVEIS MÍNIMOS DE SERVIÇO / SLA

A CONTRATADA deverá garantir os níveis mínimos de serviço descritos neste item, de forma a assegurar a disponibilidade, desempenho, suporte técnico e segurança em cada um dos serviços da solução contratada.

8.1. Conexão Dedicada à Internet:

8.1.1. Por se tratar de um serviço com atuação centralizada, é a porta que provê acesso à rede mundial de computadores (Internet) para toda a rede corporativa da Prefeitura, os níveis mínimos de serviço deverão garantir alta disponibilidade, baixa latência e resposta rápida em caso de falhas. O atendimento deverá seguir os prazos definidos no seguinte SLA:

- Disponibilidade: 99,8% mensal (máximo de 86 minutos de indisponibilidade por mês).
- Largura de Banda Garantida: 100% da capacidade contratada (500 Mbps) em 95% do tempo, com tolerância de 10% de oscilação em picos de tráfego.
- Latência para Servidores Nacionais: Máximo de 60 ms.
- Perda de Pacotes: Máximo de 0,5% em condições normais.
- Tempo de Resposta:

	Atendimento	Resolução
Crítico (indisponibilidade total do link)	1 hora	4 horas
Moderado (degradação de desempenho)	3 horas	6 horas
Baixa Prioridade	6 horas	24 horas

- Penalidades:
 - Indisponibilidade acima de 86 minutos/mês: Multa de 3% do valor unitário mensal do respectivo item do contrato.
 - Não cumprimento da largura de banda mínima: Multa de 2% do valor unitário mensal do

respectivo item do contrato.

8.1.2. Indicadores técnicos de Níveis Mínimos de Serviço / SLA

a) Latência (milissegundos): consiste no tempo médio de trânsito (ida e volta – roundtrip) de um pacote de 64 bytes entre dois pontos. Esta não deverá ultrapassar 30 ms para o Ponto de Troca de Tráfego (PTT) mais próximo (vide <https://ix.br/>).

b) Perda de Pacotes (%): consiste na taxa de falha na transmissão de pacotes IP entre dois pontos. Esta não deve ultrapassar 2% (dois por cento) de perda para o para o Ponto de Troca de Tráfego (PTT) mais próximo (vide <https://ix.br/>).

8.2. Firewall:

8.2.1. Como serviço centralizado e crítico, responsável por proteger o tráfego entre a rede corporativa e a internet, o Firewall deve operar de forma contínua, com disponibilidade compatível com o SLA contratado e mecanismos eficazes de resposta a incidentes. A CONTRATADA deverá assegurar suporte especializado e pronta intervenção conforme os prazos indicados:

- Disponibilidade: 99,44% mensal (máximo de 242 minutos, equivalente a 4 horas de indisponibilidade por mês).
- Tempo de Atualização de Regras: Máximo de 4 horas após solicitação formal.
- Detecção e Mitigação de Ameaças: Resposta a incidentes de segurança (ex.: tentativas de intrusão) em até 30 minutos após detecção.
- Tempo de Resposta:

	Atendimento	Resolução
Crítico (falha total do Firewall)	1 hora	4 horas
Moderado (problemas de configuração)	4 horas	8 horas
Baixa Prioridade (consultas ou relatórios)	8 horas	24 horas

- Relatórios: Fornecimento de relatórios mensais de tentativas de intrusão, tráfego bloqueado e desempenho do firewall, entregues até o 5º dia útil do mês subsequente.
- Penalidades:
 - Indisponibilidade acima de 242 minutos/mês: Multa de 3% do valor unitário mensal do respectivo item do contrato.
 - Atraso na entrega de relatórios: Multa de 1% do valor unitário mensal do respectivo item do contrato.

8.3. Infraestrutura de comunicação para interligação das Unidades

8.3.1. Por se tratar de um serviço com atuação global e local, que conecta todas as unidades da Prefeitura à rede corporativa por meio de enlaces dedicados, os níveis mínimos de serviço deverão considerar a criticidade da comunicação centralizada entre os pontos, bem como o atendimento individualizado em cada localidade. Os prazos devem obedecer ao seguinte SLA:

- Disponibilidade: 99,00% mensal (máximo de 432 minutos, equivalente a 7 horas e 12 minutos, de indisponibilidade por mês).
 - Método de Cálculo: Percentual de tempo em que todos os circuitos MPLS estão operacionais, medido em minutos úteis (excluindo janelas de manutenção previamente agendadas).
- Latência: Máximo de 10 ms entre quaisquer duas unidades interligadas na rede MPLS (medido em condições normais de tráfego).
- Perda de Pacotes: Máximo de 0,1% em condições normais.
- Tempo de Resposta para endereços na SEDE MUNICIPAL (1º Distrito):

	Atendimento	Resolução
Crítico (indisponibilidade total de um circuito)	2 horas	4 horas
Moderado (degradação de desempenho)	4 horas	8 horas
Baixa Prioridade (consultas ou ajustes)	8 horas	24 horas

- Tempo de Resposta para endereços do INTERIOR:

	Atendimento	Resolução
Crítico (indisponibilidade total de um circuito)	4 horas	8 horas
Moderado (degradação de desempenho)	8 horas	16 horas
Baixa Prioridade (consultas ou ajustes)	16 horas	48 horas

- Janela de Manutenção: Agendada com antecedência mínima de 7 dias, realizada fora do horário comercial (preferencialmente entre 22h e 06h).
- Penalidades:
 - Indisponibilidade acima de 432 minutos/mês: Multa de 2% do valor mensal de uma unidade do respectivo item do contrato.
 - Não cumprimento de latência ou perda de pacotes: Multa de 1% do valor mensal de uma unidade do respectivo item do contrato.

8.3.2. Indicadores técnicos de Níveis Mínimos de Serviço / SLA:

a) A infraestrutura locada deverá ser capaz de possibilitar a comunicação com os seguintes indicadores de acordo com os requisitos mínimos abaixo:

- LAT – Latência (oneway): do NÚCLEO DO BACKBONE até cada PONTO DE COMUNICAÇÃO, medida através da ferramenta Ping considerando o tempo de ida e volta de um pacote.

O cálculo será feito através da fórmula:

- $LAT = TR / 2$, onde: TR é o tempo de resposta fornecido por ferramenta que meça o tempo de ida e retorno de pacote ICMP de 64 bytes de tamanho.
- PPct – Perda de pacotes: medida em percentual tomando como referência o volume total de pacotes entre um enlace fim a fim, entre interface LAN na origem até a interface LAN do destino.

A perda de pacotes será calculada por:

- $PPct = [(Npcts_Origem - Npcts_destino) / Npcts_origem] * 100$, onde: Npcts_Origem é o número de pacotes enviados, e Npcts_Destino é o número de pacotes no destino.

b) Sempre que constatado que os Indicadores Técnicos estão fora dos parâmetros definidos, o circuito em questão será considerado:

b.1) Infraestrutura Parcialmente indisponível quando:

- o percentual de perda de pacotes for igual ou superior a 2% (dois por cento), para cada período de 5 minutos de medição.
- a latência for excedida a 10 ms (dez milissegundos), para cada período de 5 minutos de medição.

b.2) Infraestrutura Totalmente indisponível quando:

- o percentual de perda de pacotes for igual ou superior a 5% (cinco por cento), para cada período de 5 minutos de medição.
- a latência for excedida a 20 ms (milissegundos), para cada período de 5 minutos de medição.

c) Em caso do congestionamento no link causado por excesso de tráfego, os períodos em que ocorreu o congestionamento serão desconsiderados.

d) Caso sejam constatadas as ocorrências simultâneas dos eventos a penalidade será aplicada uma única vez.

8.4. Infraestrutura para rede WIFI interno:

8.4.1. Por se tratar de um serviço com atuação local e distribuída, instalado individualmente em cada unidade da Prefeitura, os níveis mínimos de serviço devem contemplar a manutenção da conectividade sem fio, a substituição de equipamentos defeituosos e o suporte técnico in loco, conforme os prazos estabelecidos no SLA abaixo:

- Disponibilidade: 99,00% mensal (máximo de 432 minutos, equivalente a 7 horas e 12 minutos, de indisponibilidade por mês).
- Cobertura: Sinal WIFI com intensidade mínima de -65 dBm em 90% da área de uso prevista de cada unidade.
- Capacidade: Suporte a pelo menos 50 dispositivos conectados simultaneamente por ponto de acesso, com velocidade mínima de 10 Mbps por dispositivo em condições normais.
- Tempo de Resposta para endereços na SEDE MUNICIPAL (1º Distrito):

	Atendimento	Resolução
Crítico (indisponibilidade total de um ponto de acesso)	2 hora	8 horas
Moderado (degradação de desempenho)	6 horas	12 horas
Baixa Prioridade	8 horas	24 horas

- Tempo de Resposta para endereços no INTERIOR:

	Atendimento	Resolução
Crítico (indisponibilidade total de um ponto de acesso)	4 hora	16 horas
Moderado (degradação de desempenho)	12 horas	24 horas
Baixa Prioridade	16 horas	48 horas

- Penalidades:
 - Indisponibilidade acima de 432 minutos/mês por ponto de acesso: Multa de 1% do valor mensal de uma unidade do respectivo item do contrato.
 - Não cumprimento de cobertura ou capacidade: Multa de 2% do valor mensal de uma unidade do respectivo item do contrato.

9 FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

9.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo menor preço global do Lote.

9.2. O objeto da presente contratação — locação de infraestrutura de rede, internet dedicada, firewall e WIFI — enquadra-se como serviço comum, nos termos do inciso XIII do art. 6º da Lei nº 14.133/2021, pois seus padrões de desempenho e qualidade podem ser objetivamente definidos no edital por meio de especificações técnicas usuais de mercado, como largura de banda e níveis mínimos de serviço (SLA). Assim sendo, a modalidade adequada para a licitação é o pregão eletrônico, conforme art. 28, inciso II da referida lei.

10. QUALIFICAÇÃO TÉCNICA

10.1 Deverá ser apresentado, pelo menos um, atestado ou certidão de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, em nome do licitante, que comprove a aptidão para o desempenho de atividades compatíveis com o objeto desta licitação. Cada documento deve identificar o(s) técnico(s) responsável(is).

10.1.1 Os atestados ou certidões solicitadas deverão comprovar a execução de serviços compatíveis em características e quantidades equivalentes ou superiores às parcelas de maior relevância técnica ou valor significativo, que são:

10.1.1.1. Fornecimento de Acesso Internet Dedicada em um único local, com velocidade de 500 Mbps Full Duplex, referente ao item 6.2 deste Termo de Referência;

10.1.1.2. Fornecimento de infraestrutura de comunicação de 70 pontos para interligação de unidades (MPLS, L2L ou VPN), independente da velocidade atendida, referente a 50% do quantitativo total dos serviços listados no item 6.1 deste Termo de Referência;

10.1.2 Os atestados ou certidões de capacidade técnica deverão conter, no mínimo, as informações que a empresa inscrita no CNPJ e estabelecida em endereço a ser relatado, prestou os serviços exigidos em termos de capacidade técnica e que demonstra capacidade técnica adequada. Os atestados poderão ser

objeto de diligência por parte do Agente de Contratação ou da equipe técnica, com vistas a dirimir dúvidas em relação ao tipo de serviço prestado.

10.1.3 O Agente de Contratação poderá verificar a comprovação da execução das parcelas de maior relevância técnica ou valor significativo através da descrição dos serviços constantes nos atestados/certidões apresentados.

10.1.4 Poderão ser apresentados tantos atestados ou certidões quanto forem necessários, desde que comprovado o atendimento de todas as parcelas de maior relevância acima exigidas, observada a respectiva competência profissional.

10.2. Apresentar Termo de Autorização para exploração de SCM (Serviço de Comunicação Multimídia), outorgada pelo poder concedente (ANATEL), comprovando aptidão para o desempenho de atividade de transmissão de dados, incluindo dados, voz, imagem e vídeo.

10.3. Para fins de comprovação do Autonomous System e Ponto de Troca de Tráfego, deverá a Licitante apresentar:

10.3.1. o ASN (Número do Autonomous System) para comprovação de que a licitante é AS (Autonomous System), disponível em <https://registro.br/2/whois>;

10.3.2. a comprovação de que a licitante está conectada, direta ou indiretamente via provedor de trânsito, a pelo menos 3 (três) "Pontos de Troca de Tráfego" (PTT) nacionais (disponíveis em <http://ix.br/particip>) com o objetivo de melhorar a eficiência e distribuição do tráfego de Internet da Prefeitura.

11. OBRIGAÇÕES DA CONTRATADA

11.1. A CONTRATADA obrigará-se a fornecer o objeto a ela adjudicado, conforme especificações estabelecidas no Edital e em seus Anexos e na proposta apresentada, prevalecendo, no caso de divergência, as especificações e condições estabelecidas no Edital;

11.2. A CONTRATADA assumirá responsabilidade pela boa execução e eficiência dos serviços que efetuará, assim como pelo cumprimento dos elementos técnicos recebidos, bem como quaisquer danos decorrentes.

11.3. Responsabilizar-se pelo perfeito cumprimento do objeto do contrato, arcar com os eventuais prejuízos causados à Prefeitura de Santa Cruz do Sul ou a terceiros, provocados por ineficiência ou irregularidade cometida por seus empregados ou prepostos envolvidos na execução dos serviços, respondendo integralmente pelo ônus decorrente de sua culpa ou dolo na entrega do produto ou serviços, o que não exclui nem diminui a responsabilidade pelos danos que se constatarem, independentemente do controle e fiscalização exercidos pela Prefeitura de Santa Cruz do Sul;

11.4. Comunicar à Prefeitura de Santa Cruz do Sul, por escrito, quaisquer anormalidades, que ponham em risco o êxito e o cumprimento dos prazos de execução dos serviços, propondo as ações corretivas necessárias;

11.5. CONTRATADA não poderá alegar incapacidade de execução de parte ou todo do objeto contratado, bem como impossibilidade de ajuste e/ou adequação de performance técnica, qualquer que sejam os empecilhos, estando obrigada à execução dos ajustes e adequações necessárias para dirimi-los, sem ônus

para a Prefeitura de Santa Cruz do Sul. Excetuam-se os casos em que as falhas sejam provenientes da Prefeitura de Santa Cruz do Sul;

11.6. Dispor de mão de obra especializada, qualificada e em quantidade suficiente à perfeita prestação dos serviços, em seu nome e sob sua responsabilidade, sem qualquer solidariedade da Prefeitura de Santa Cruz do Sul, cabendo-lhe efetuar todos os pagamentos, inclusive os relativos aos encargos previstos na legislação trabalhista, previdenciária e fiscal, bem como de seguros e quaisquer outros decorrentes da sua condição de empregadora, assumindo ainda, com relação ao contingente alocado, total responsabilidade pela coordenação e supervisão dos encargos administrativos, tais como: controle, fiscalização e orientação técnica, controle de frequência, ausências permitidas, licenças autorizadas, férias, punições, admissões, demissões, transferências e promoções;

11.7. Responsabilizar-se por todos os custos com pessoal, diárias, passagens e comunicações necessárias à perfeita execução dos serviços objeto deste Termo de Referência;

11.8. Manter em dia todos os direitos pecuniários de seus colaboradores, tais como horas extras, adicionais noturnos, indenizações e outras vantagens, de forma que não sejam os trabalhos da Prefeitura de Santa Cruz do Sul prejudicados em função de reivindicações por parte dos colaboradores da CONTRATADA;

11.9. Assumir todas as despesas e ônus relativos ao pessoal e a quaisquer outras derivadas ou conexas com o Contrato, ficando ainda, para todos os efeitos legais, inexistente qualquer vínculo empregatício entre seus colaboradores e/ou preposto e a Prefeitura de Santa Cruz do Sul;

11.10. Informar à Prefeitura de Santa Cruz do Sul, para efeito de controle de acesso às suas dependências, o nome e o CPF dos colaboradores disponibilizados para a prestação de serviços.

11.11. Qualquer indenização que a prefeitura de Santa Cruz do Sul, porventura, venha pagar a terceiros em virtude de vazamentos de dados por falhas de segurança, relativos ao objeto contratado, será de inteira responsabilidade da CONTRATADA.

11.12. Manter, durante o período de vigência do contrato, todas as condições que ensejaram a contratação.

11.13. A fim de garantir a sustentação da Solução para a Administração Municipal durante e após a vigência contratual, em função de eventual interrupção do contrato por qualquer motivo ou futura transição contratual decorrente de nova licitação para o mesmo objeto, a CONTRATADA deve:

11.13.1. Assegurar ao CONTRATANTE, mediante cláusula contratual, o uso do produto sucessor em caso de descontinuidade do produto contratado;

11.13.2. Assegurar ao CONTRATANTE, mediante cláusula contratual, transferência de todas as obrigações contratuais ao sucessor em caso de venda da empresa CONTRATADA ou incorporação por novos controladores;

11.14. Cooperar com a apuração dos fatos relacionados a sinistros ou eventos danosos, mediante o fornecimento de informações técnicas, registros, relatórios e demais elementos necessários à correta análise do ocorrido;

11.15. Responsabilizar-se pelos prejuízos decorrentes de caso fortuito ou força maior, desde que reste demonstrado que a CONTRATANTE atuou com o devido zelo e segurança na guarda dos bens, inexistindo dolo ou culpa da Administração.

12. OBRIGAÇÕES DA CONTRATANTE

12.1. Comunicar formalmente à CONTRATADA, em prazo razoável, a ocorrência de dano, furto, roubo ou qualquer outro sinistro, tais como incêndio, inundação ou atos de vandalismo.

12.2. Realizar mensalmente o boletim de medição dos recursos utilizados, para fins de pagamento do que foi realmente utilizado.

12.3. Efetuar o pagamento da CONTRATADA de acordo com a forma de pagamento estipulada na licitação e no Contrato.

12.4. Promover o acompanhamento e a fiscalização do fornecimento/prestação dos serviços, sob os aspectos qualitativo e quantitativo, anotando em registro próprio as falhas e solicitando as medidas corretivas.

12.5. Rejeitar, no todo ou em parte, o objeto entregue pela CONTRATADA fora das especificações do contrato.

12.6. Observar para que durante a vigência do Contrato sejam cumpridas as obrigações assumidas pela CONTRATADA, bem como sejam mantidas todas as condições de habilitação e qualificação exigidas na licitação.

12.7. Aplicar as sanções administrativas, quando se fizerem necessárias.

12.8. Prestar à CONTRATADA informações e esclarecimentos que venham a ser solicitados.

12.9. Zelar, guardar e empregar os bens da CONTRATADA com diligência, observando as condições normais de uso, conservação e segurança;

12.10. Responsabilizar-se pelos danos decorrentes de atos praticados pela própria CONTRATANTE ou por seus agentes, quando caracterizados dolo ou culpa;

12.11. Responsabilizar-se pelos danos decorrentes de atos de terceiros ou de eventos da natureza quando evidenciada falha da CONTRATANTE quanto ao dever de guarda, segurança ou adoção de medidas razoáveis de prevenção, especialmente nos casos em que o evento era previsível ou evitável.

12.12. Demais condições constantes do edital de licitação.

13 SUBCONTRATAÇÃO

13.1 Será permitida subcontratação parcial exclusivamente para a execução da denominada "última milha" nas unidades localizadas no interior (fora da Sede Municipal – 1º Distrito). A subcontratação ficará limitada a 25% (vinte e cinco por cento) do somatório total do quantitativo previsto nos itens 2 (NS02) e 3 (NS03) deste Termo de Referência, prioritariamente às unidades do Interior, conforme relação de "unidades de entrega dos serviços" em anexo, na qual estão identificadas 27 (vinte e sete) unidades situadas fora da Sede Municipal (coluna LOCAL=Interior). A contratada permanecerá integralmente responsável pelo cumprimento das obrigações técnicas, prazos e níveis de serviço (SLA) estabelecidos, devendo informar previamente à Administração a justificativa e os endereços/unidades que serão atendidos por terceiros.

14. MODELO DE GESTÃO DE CONTRATO

14.1. O prazo da Contratação: **24 (vinte e quatro) meses**, contados a partir da assinatura do contrato, prorrogáveis por sucessivos períodos de 12 (doze) meses, respeitada a vigência máxima decenal (dez anos), conforme art. 105 e seguintes, da Lei nº 14.133, de 1º de abril de 2021.

14.2. A gestão e a fiscalização do objeto contratado serão realizadas conforme o disposto no Decreto Municipal 11.668/2023, que “Regulamenta a Lei Federal nº 14.133, de 1º de abril de 2021, no âmbito do município de Santa Cruz do Sul”.

14.3. O(s) Fiscal(is) e o gestor do contrato serão devidamente indicados no Termo de Contrato.

14.4. A fiscalização do contrato será exercida por representantes da CONTRATANTE, designados formalmente como fiscais técnicos e fiscais administrativos. Caberá aos fiscais técnicos acompanhar e verificar o cumprimento dos requisitos técnicos e operacionais da solução contratada, incluindo aspectos relacionados à performance, disponibilidade, segurança, continuidade dos serviços e conformidade com os níveis de serviço pactuados, além de gerar o boletim de medição mensal dos serviços. Já os fiscais administrativos serão responsáveis por monitorar a execução contratual sob os aspectos administrativos, como prazos, documentação, pagamentos e cumprimento das cláusulas contratuais. Ambos os fiscais poderão solicitar informações e documentos à CONTRATADA sempre que necessário para o adequado acompanhamento da execução contratual.

14.5. A fiscalização será exercida no interesse da Prefeitura Municipal de Santa Cruz do Sul – RS e não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por quaisquer irregularidades, e, na sua ocorrência, não implica corresponsabilidade do Poder Público ou de seus agentes e prepostos.

15. DO PAGAMENTO

15.1. Os pagamentos serão efetuados mensalmente, no prazo de até 10 (dez) dias corridos a contar do recebimento da Nota Fiscal/Fatura, observando os seguintes requisitos:

15.1.1. A CONTRATADA deverá apresentar até o quinto dia útil do mês subsequente, o relatório dos pontos ativados do mês anterior para a CONTRATANTE, a qual irá analisar e confirmar os quantitativos e valores através da expedição do Boletim de Medição.

15.1.2. Somente após o envio do Boletim de Medição para a CONTRATADA, é que esta poderá gerar a Nota Fiscal/Fatura.

15.1.3. Comprovação da regularidade fiscal e trabalhista da CONTRATADA, por meio da apresentação das certidões exigidas no edital, válidas na data do pagamento.

15.1.4. O prazo para início da contagem dos períodos de faturamento e pagamento da CONTRATADA somente terá início a partir da assinatura do Termo de Aceitação e Recebimento Definitivo dos Serviços pela CONTRATANTE, atestando que todos os serviços contratados foram entregues em conformidade com os requisitos técnicos, funcionais e de segurança estabelecidos neste Termo de Referência.

15.1.5. Nos casos em que houver aumento ou redução de pontos de conexão (NS02 ou NS03) ou WIFI no decorrer do mês, o cálculo da remuneração deverá ser realizado de forma proporcional ao número de dias

em que os pontos permaneceram ativados, tomando como base a data da efetiva ativação (no caso de aumento de pontos) ou a data de solicitação (no caso de desativação de pontos).

15.2. O pagamento será realizado com recursos orçamentários próprios da CONTRATANTE, em conta bancária indicada pela CONTRATADA.

15.3. O processo de pagamento será centralizado pela Secretaria de Administração e Gestão, em conjunto com as Secretarias de Educação e de Saúde, sendo estas duas últimas em razão da quantidade de endereços atendidos, respectivamente 52 e 48 de um total de 150 endereços, e da possibilidade de utilização de verbas vinculadas disponíveis.

15.4. O simples recebimento da Nota Fiscal/Fatura não implicará em sua aprovação automática, podendo ser devolvida à CONTRATADA para correções, suspensão ou ajustes, em caso de:

15.4.1. divergências entre os serviços prestados e os contratados;

15.4.2. pendências apontadas no Boletim de Medição;

15.4.3. aplicação de descontos decorrentes de multas ou penalidades previstas no Contrato.

15.5. Quando da emissão da Nota Fiscal, a CONTRATADA deverá descrever os serviços prestados de forma clara, obedecendo rigorosamente à descrição constante no Instrumento Contratual, incluindo o número da nota de empenho e endereço onde o serviço foi prestado.

15.6. Na hipótese de glosa de valores, decorrentes de descumprimento de SLA, prazos de atendimento, penalidades contratuais ou outras condições previstas neste Contrato, o valor glosado será deduzido automaticamente do valor a ser pago na fatura correspondente.

16 REAJUSTAMENTO DO PREÇO

16.1 O reajustamento de preço do contrato deverá se dar conforme as previsões contratuais e legais, através do Índice Nacional de Preços ao Consumidor Amplo, conforme o Decreto Municipal 11.668/2023.

17 DA PROTEÇÃO DE DADOS

17.1. Em atendimento ao art. 7º, da lei nº 13.709 (LGPD), referente ao tratamento de dados pessoais: A Lei Geral de Proteção de Dados será obedecida, em todos os seus termos, pela CONTRATADA, obrigando-se ela a tratar os dados da CONTRATANTE que forem eventualmente coletados, conforme sua necessidade ou obrigatoriedade.

17.2. Em atendimento ao art. 6º da lei nº 13.709 (LGPD), referente à observância de boa-fé e aos princípios a serem empregados no tratamento de dados: Conforme prevê a Lei Geral de Proteção de Dados, obriga-se a CONTRATADA a executar os seus trabalhos e tratar os dados da CONTRATANTE respeitando os princípios da finalidade, adequação, transparência, livre acesso, segurança, prevenção e não discriminação.

17.3. Em atendimento ao art. 60 da lei nº 13.709 (LGPD), referente à formulação de regras de boas práticas e de governança no tratamento de dados: A CONTRATADA obriga-se a garantir a confidencialidade dos dados coletados da CONTRATANTE por meio de uma política interna de privacidade, a fim de respeitar, por si, seus funcionários e seus prepostos, o objetivo do presente termo.

17.4. Em atendimento ao art. 15 da lei nº 13.709 (LGPD), referente ao término do tratamento de dados: Eventuais dados coletados pela CONTRATADA serão arquivados por esta somente pelo tempo necessário

para a execução dos serviços contratados. Ao seu fim, os dados coletados serão permanentemente eliminados, excetuando-se os que se enquadrarem no disposto no artigo 16, I da Lei Geral de Proteção de Dados.

18. DOTAÇÃO ORÇAMENTÁRIA

18.1. As despesas decorrentes deste procedimento licitatório correrão à conta da(s) seguinte(s) dotação(ões) orçamentária(s), constante(s) no Orçamento Programa para 2025:

Dotação: 2025/166 – PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL
Programa de Trabalho: 06.01.04.126.0002.2601 – MANUTENÇÃO DOS SISTEMAS DE TECNOLOGIA E INFORMAÇÃO
Elemento de Despesa: 3.3.90.40.00.00.00.00 – SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – PJ
Fonte de Recurso: 1500 – RECURSOS NÃO VINCULADOS DE IMPOSTOS
Destinação: 0000001 – RECURSO LIVRE
Rubrica Item: 3.3.90.13.00.00.00 – COMUNICAÇÃO DE DADOS E REDES EM GERAL

Secretaria de EDUCAÇÃO - Administrativo

Dotação: 2026/326 – PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL
Programa de Trabalho: 10.01.12.122.0002.2023 – MANUTENÇÃO DA SECRETARIA MUNICIPAL DE EDUCAÇÃO
Elemento de Despesa: 3.3.90.40.00.00.00.00 – SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – PJ
Fonte de Recurso: 1501 – OUTROS RECURSOS NÃO VINCULADOS
Destinação: 0000001 – RECURSO LIVRE
Rubrica Item: 3.3.90.40.13.00.00.00 – COMUNICAÇÃO DE DADOS E REDES EM GERAL

Dotação: 2026/333 – PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL
Programa de Trabalho: 10.01.12.122.0002.2287- CONSELHO MUNICIPAL DE EDUCAÇÃO
Elemento de Despesa: 3.3.90.40.00.00.00.00 – SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – PJ
Fonte de Recurso: 1501 – OUTROS RECURSOS NÃO VINCULADOS
Destinação: 0000001 – RECURSO LIVRE
Rubrica Item: 3.3.90.40.13.00.00.00 – COMUNICAÇÃO DE DADOS E REDES EM GERAL

Dotação: 2026/437 – PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL
Programa de Trabalho: 10.02.12.122.0002.2377 - MANUTENÇÃO DA SECRETARIA MUNICIPAL DE EDUCAÇÃO - ADMINISTRATIVO
Elemento de Despesa: 3.3.90.40.00.00.00.00 – SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – PJ
Fonte de Recurso: 1501 – OUTROS RECURSOS NÃO VINCULADOS
Destinação: 1001020 - MANUTENÇÃO E DESENVOLVIMENTO DO ENSINO - MDE
Rubrica Item: 3.3.90.40.13.00.00.00 – COMUNICAÇÃO DE DADOS E REDES EM GERAL

Secretaria de EDUCAÇÃO - Ensino Fundamental

Dotação: 2026/371 – PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL
Programa de Trabalho: 10.01.12.361.0016.2036 - APLICAÇÃO DOS RECURSOS DO SALÁRIO EDUCAÇÃO-ENS. FUNDAMENTAL
Elemento de Despesa: 3.3.90.40.00.00.00.00 – SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – PJ
Fonte de Recurso: 1550 – TRANSFERÊNCIA DO SALÁRIO - EDUCAÇÃO
Destinação: 0000103 - SALÁRIO EDUCAÇÃO - UNIÃO
Rubrica Item: 3.3.90.40.13.00.00.00 – COMUNICAÇÃO DE DADOS E REDES EM GERAL

Dotação: 2026/465 – PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL
Programa de Trabalho: 10.02.12.361.0016.2037 - MANUTENÇÃO DO ENSINO FUNDAMENTAL - MDE
Elemento de Despesa: 3.3.90.40.00.00.00.00 – SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – PJ

Fonte de Recurso: 1501 – OUTROS RECURSOS NÃO VINCULADOS
Destinação: 1001020 - MANUTENÇÃO E DESENVOLVIMENTO DO ENSINO - MDE
Rubrica Item: 3.3.90.40.13.00.00.00 – COMUNICAÇÃO DE DADOS E REDES EM GERAL

Dotação: 2026/533 – PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL
Programa de Trabalho: 10.03.12.361.0016.2039 - MANUTENÇÃO ENSINO FUNDAMENTAL - FUNDEB 30%
Elemento de Despesa: 3.3.90.40.00.00.00.00 – SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – PJ
Fonte de Recurso: 1540 - TRANSFERÊNCIAS DO FUNDEB
Destinação: 0000031 - FUNDEB (SOMENTE 30%)
Rubrica Item: 3.3.90.40.13.00.00.00 – COMUNICAÇÃO DE DADOS E REDES EM GERAL

Secretaria de EDUCAÇÃO - Educação Infantil

Dotação: 2026/403 – PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL
Programa de Trabalho: 10.01.12.365.0018.2049 - APLICAÇÃO RECURSOS DO SALÁRIO-EDUCAÇÃO-EDUCAÇÃO INFANTIL
Elemento de Despesa: 3.3.90.40.00.00.00.00 – SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – PJ
Fonte de Recurso: 1550 – TRANSFERÊNCIA DO SALÁRIO - EDUCAÇÃO
Destinação: 0000103 - SALÁRIO EDUCAÇÃO - UNIÃO
Rubrica Item: 3.3.90.40.13.00.00.00 – COMUNICAÇÃO DE DADOS E REDES EM GERAL

Dotação: 2026/493 – PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL
Programa de Trabalho: 10.02.12.365.0018.2242 - MANUTENÇÃO CRECHE - MDE
Elemento de Despesa: 3.3.90.40.00.00.00.00 – SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – PJ
Fonte de Recurso: 1501 – OUTROS RECURSOS NÃO VINCULADOS
Destinação: 1001020 - MANUTENÇÃO E DESENVOLVIMENTO DO ENSINO - MDE
Rubrica Item: 3.3.90.40.13.00.00.00 – COMUNICAÇÃO DE DADOS E REDES EM GERAL

Dotação: 2026/640 – PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL
Programa de Trabalho: 10.03.12.365.0018.2454 - MANUTENÇÃO DA EDUC. INFANTIL – CRECHE – FUNDEB 30%
Elemento de Despesa: 3.3.90.40.00.00.00.00 – SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – PJ
Fonte de Recurso: 1540 - TRANSFERÊNCIAS DO FUNDEB
Destinação: 0000031 - FUNDEB (SOMENTE 30%)
Rubrica Item: 3.3.90.40.13.00.00.00 – COMUNICAÇÃO DE DADOS E REDES EM GERAL

Secretaria de SAÚDE

Dotação: 2026/725 - PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL
Programa de Trabalho: 12.01.10.122.0026.2450 - MANUTENÇÃO DE AÇÕES DE APOIO ADMINISTRATIVO
Elemento de Despesa: 3.3.90.40.00.00.00.00 - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PJ
Fonte de Recurso: 1500 - RECURSOS NÃO VINCULADOS DE IMPOSTOS
Destinação : 1002040 - 0040-ACOES E SERVICOS PUBLICOS DE SAUDE - ASPS
Rubrica Item : 3.3.90.40.13.00.00.00 - COMUNICAÇÃO DE DADOS E REDES EM GERAL

Dotação: 2026/795 - PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL
Programa de Trabalho: 12.01.10.301.0022.2421 - MANUTENÇÃO DE AÇÕES NA ATENÇÃO PRIMÁRIA EM SAÚDE
Elemento de Despesa: 3.3.90.40.00.00.00.00 - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PJ
Fonte de Recurso: 1621 - TRANSF FUNDO A FUNDO REC SUS PROV GOV ESTADUAL
Destinação : 0000506 - 4011-ATENCAO BASICA
Rubrica Item : 3.3.90.40.13.00.00.00 - COMUNICAÇÃO DE DADOS E REDES EM GERAL

Dotação: 2026/851 - PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL
Programa de Trabalho: 12.01.10.301.0022.2424 - MANUTENÇÃO DAS AÇÕES NA SAÚDE PRISIONAL

Elemento de Despesa: 3.3.90.40.00.00.00.00 - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PJ

Fonte de Recurso: 1621 - TRANSF FUNDO A FUNDO REC SUS PROV GOV ESTADUAL

Destinação : 0000513 - 4090-PSF/NASF/ESF

Rubrica Item : 3.3.90.40.13.00.00.00 - COMUNICAÇÃO DE DADOS E REDES EM GERAL

Dotação: 2026/910 - PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL

Programa de Trabalho: 12.01.10.301.0022.2473 - MANUTENÇÃO DA ESTRATÉGIA DE SAÚDE DA FAMÍLIA

Elemento de Despesa: 3.3.90.40.00.00.00.00 - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PJ

Fonte de Recurso: 1600 - TRANSF FUNDO A FUNDO REC SUS PROV GOV FEDERAL - ASPS

Destinação : 0000534 - 4500-CUSTEIO - Atenção Básica

Rubrica Item : 3.3.90.40.13.00.00.00 - COMUNICAÇÃO DE DADOS E REDES EM GERAL

Dotação: 2026/959 - PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL

Programa de Trabalho: 12.01.10.301.0022.2474 - MANUTENÇÃO DE AÇÕES E SERVIÇOS DE SAÚDE BUCAL

Elemento de Despesa: 3.3.90.40.00.00.00.00 - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PJ

Fonte de Recurso: 1621 - TRANSF FUNDO A FUNDO REC SUS PROV GOV ESTADUAL

Destinação : 0000506 - 4011-ATENCAO BASICA

Rubrica Item : 3.3.90.40.13.00.00.00 - COMUNICAÇÃO DE DADOS E REDES EM GERAL

Dotação: 2026/1021 - PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL

Programa de Trabalho: 12.01.10.301.0036.2613 - MANUTENÇÃO DE AÇÕES EM SAÚDE NA PRIMEIRA INFÂNCIA

Elemento de Despesa: 3.3.90.40.00.00.00.00 - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PJ

Fonte de Recurso: 1621 - TRANSF FUNDO A FUNDO REC SUS PROV GOV ESTADUAL

Destinação : 0000506 - 4011-ATENCAO BASICA

Rubrica Item : 3.3.90.40.13.00.00.00 - COMUNICAÇÃO DE DADOS E REDES EM GERAL

Dotação: 2026/1082 - PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL

Programa de Trabalho: 12.01.10.302.0023.2430 - MANUTENÇÃO DA CENTRAL DE REGULAÇÃO AMBULATORIAL E HOSPITALAR

Elemento de Despesa: 3.3.90.40.00.00.00.00 - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PJ

Fonte de Recurso: 1500 - RECURSOS NÃO VINCULADOS DE IMPOSTOS

Destinação : 1002040 - 0040-ACOES E SERVICOS PUBLICOS DE SAUDE - ASPS

Rubrica Item : 3.3.90.40.13.00.00.00 - COMUNICAÇÃO DE DADOS E REDES EM GERAL

Dotação: 2026/1103 - PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL

Programa de Trabalho: 12.01.10.302.0023.2431 - MANUTENÇÃO DO CENTRO MATERNO INFANTIL – CEMAI

Elemento de Despesa: 3.3.90.40.00.00.00.00 - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PJ

Fonte de Recurso: 1500 - RECURSOS NÃO VINCULADOS DE IMPOSTOS

Destinação : 1002040 - 0040-ACOES E SERVICOS PUBLICOS DE SAUDE - ASPS

Rubrica Item : 3.3.90.40.13.00.00.00 - COMUNICAÇÃO DE DADOS E REDES EM GERAL

Dotação: 2026/1131 - PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL

Programa de Trabalho: 12.01.10.302.0023.2433 - MANUTENÇÃO DO SETOR DE TRANSPORTES DA SAÚDE

Elemento de Despesa: 3.3.90.40.00.00.00.00 - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PJ

Fonte de Recurso: 1500 - RECURSOS NÃO VINCULADOS DE IMPOSTOS

Destinação : 1002040 - 0040-ACOES E SERVICOS PUBLICOS DE SAUDE - ASPS

Rubrica Item : 3.3.90.40.13.00.00.00 - COMUNICAÇÃO DE DADOS E REDES EM GERAL

Dotação: 2026/1165 - PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL

Programa de Trabalho: 12.01.10.302.0023.2434 - MANUTENÇÃO DO PROGRAMA MELHOR EM CASA

Elemento de Despesa: 3.3.90.40.00.00.00.00 - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E

COMUNICAÇÃO - PJ

Fonte de Recurso: 1600 - TRANSF FUNDO A FUNDO REC SUS PROV GOV FEDERAL - ASPS

Destinação : 0000591 - MELHOR EM CASA

Rubrica Item : 3.3.90.40.13.00.00.00 - COMUNICAÇÃO DE DADOS E REDES EM GERAL

Dotação: 2026/1195 - PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL

Programa de Trabalho: 12.01.10.302.0023.2435 - MANUTENÇÃO DO CENTRO DE ATENÇÃO PSICOSSOCIAL – CAPS II

Elemento de Despesa: 3.3.90.40.00.00.00.00 - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PJ

Fonte de Recurso: 1600 - TRANSF FUNDO A FUNDO REC SUS PROV GOV FEDERAL - ASPS

Destinação : 0000590 - REDE DE SAÚDE MENTAL

Rubrica Item : 3.3.90.40.13.00.00.00 - COMUNICAÇÃO DE DADOS E REDES EM GERAL

Dotação: 2026/1226 - PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL

Programa de Trabalho: 12.01.10.302.0023.2436 - MANUTENÇÃO DO CENTRO DE ATENÇÃO PSICOSSOCIAL DA INFÂNCIA E

Elemento de Despesa: 3.3.90.40.00.00.00.00 - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PJ

Fonte de Recurso: 1600 - TRANSF FUNDO A FUNDO REC SUS PROV GOV FEDERAL - ASPS

Destinação : 0000590 - REDE DE SAÚDE MENTAL

Rubrica Item : 3.3.90.40.13.00.00.00 - COMUNICAÇÃO DE DADOS E REDES EM GERAL

Dotação: 2026/1263 - PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL

Programa de Trabalho: 12.01.10.302.0023.2437 - MANUTENÇÃO DO CENTRO DE ATENÇÃO PSICOSSOCIAL ÁLCOOL E DROGAS - CAPS

Elemento de Despesa: 3.3.90.40.00.00.00.00 - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PJ

Fonte de Recurso: 1600 - TRANSF FUNDO A FUNDO REC SUS PROV GOV FEDERAL - ASPS

Destinação : 0000590 - REDE DE SAÚDE MENTAL

Rubrica Item : 3.3.90.40.13.00.00.00 - COMUNICAÇÃO DE DADOS E REDES EM GERAL

Dotação: 2026/1312 - PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL

Programa de Trabalho: 12.01.10.302.0023.2440 - MANUTENÇÃO DO SERVIÇO DE ATENDIMENTO MÓVEL DE URGÊNCIA – SAMU

Elemento de Despesa: 3.3.90.40.00.00.00.00 - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PJ

Fonte de Recurso: 1621 - TRANSF FUNDO A FUNDO REC SUS PROV GOV ESTADUAL

Destinação : 0000521 - 4170-SAMU/UPA até 2024

Rubrica Item : 3.3.90.40.13.00.00.00 - COMUNICAÇÃO DE DADOS E REDES EM GERAL

Dotação: 2026/1365 - PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL

Programa de Trabalho: 12.01.10.303.0025.2447 - MANUTENÇÃO DAS AÇÕES NA ASSISTÊNCIA FARMACÊUTICA

Elemento de Despesa: 3.3.90.40.00.00.00.00 - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PJ

Fonte de Recurso: 1500 - RECURSOS NÃO VINCULADOS DE IMPOSTOS

Destinação : 1002040 - 0040-ACOES E SERVICOS PUBLICOS DE SAUDE - ASPS

Rubrica Item : 3.3.90.40.13.00.00.00 - COMUNICAÇÃO DE DADOS E REDES EM GERAL

Dotação: 2026/1394 - PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL

Programa de Trabalho: 12.01.10.304.0024.2444 - MANUTENÇÃO DAS AÇÕES DE VIGILÂNCIA SANITÁRIA

Elemento de Despesa: 3.3.90.40.00.00.00.00 - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PJ

Fonte de Recurso: 1600 - TRANSF FUNDO A FUNDO REC SUS PROV GOV FEDERAL - ASPS

Destinação : 0000536 - 4502-CUSTEIO - Vigilância em Saúde

Rubrica Item : 3.3.90.40.13.00.00.00 - COMUNICAÇÃO DE DADOS E REDES EM GERAL

Dotação: 2026/1431 - PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL

Programa de Trabalho: 12.01.10.305.0024.2445 - MANUTENÇÃO DAS AÇÕES DE VIGILÂNCIA EPIDEMIOLÓGICA

Elemento de Despesa: 3.3.90.40.00.00.00.00 - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E

COMUNICAÇÃO - PJ

Fonte de Recurso: 1600 - TRANSF FUNDO A FUNDO REC SUS PROV GOV FEDERAL - ASPS

Destinação : 0000536 - 4502-CUSTEIO - Vigilância em Saúde

Rubrica Item : 3.3.90.40.13.00.00.00 - COMUNICAÇÃO DE DADOS E REDES EM GERAL

Dotação: 2026/1469 - PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL

Programa de Trabalho: 12.01.10.305.0024.2446 - MANUTENÇÃO DAS AÇÕES DE ATENÇÃO INTEGRAL AO HIV/AIDS, OUTRAS IST,

Elemento de Despesa: 3.3.90.40.00.00.00.00 - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PJ

Fonte de Recurso: 1600 - TRANSF FUNDO A FUNDO REC SUS PROV GOV FEDERAL - ASPS

Destinação : 0000536 - 4502-CUSTEIO - Vigilância em Saúde

Rubrica Item : 3.3.90.40.13.00.00.00 - COMUNICAÇÃO DE DADOS E REDES EM GERAL

Dotação: 2026/1511 - PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL

Programa de Trabalho: 12.01.10.305.0024.2616 - MANUTENÇÃO DAS AÇÕES DE VIGILÂNCIA EM SAÚDE DO TRABALHADOR

Elemento de Despesa: 3.3.90.40.00.00.00.00 - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PJ

Fonte de Recurso: 1500 - RECURSOS NÃO VINCULADOS DE IMPOSTOS

Destinação : 1002040 - 0040-ACOES E SERVICOS PUBLICOS DE SAUDE - ASPS

Rubrica Item : 3.3.90.40.13.00.00.00 - COMUNICAÇÃO DE DADOS E REDES EM GERAL

Dotação: 2026/1512 - PREFEITURA MUNICIPAL DE SANTA CRUZ DO SUL

Programa de Trabalho: 12.01.10.305.0024.2616 - MANUTENÇÃO DAS AÇÕES DE VIGILÂNCIA EM SAÚDE DO TRABALHADOR

Elemento de Despesa: 3.3.90.40.00.00.00.00 - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PJ

Fonte de Recurso: 1600 - TRANSF FUNDO A FUNDO REC SUS PROV GOV FEDERAL - ASPS

Destinação : 0000595 - CEREST – CENTRO DE REFERÊNCIA EM SAÚDE DO TRABALHADOR

Rubrica Item : 3.3.90.40.13.00.00.00 - COMUNICAÇÃO DE DADOS E REDES EM GERAL

Santa Cruz do Sul, 22 de Janeiro de 2026.

Álvaro dos Santos Neuwald - 13931

Agente Administrativo

Ricardo Voigt - 11953

Programador

Matheus Luis Ferreira

Secretário Municipal de

Administração e Gestão