Câmara Municipal de Campina Verde - Estado de Minas Gerais

Rua 26 nº 114 – Centro – Campina Verde/MG CNPJ: 23.370.075/0001-60
Fone: (34) 3412-1053 e-mail: camaramunicipalcv@yahoo.com.br

ANEXO I

TERMO DE REFERÊNCIA – LEI 14.133/21

PROCESSO ADMINISTRATIVO Nº 019/2025
PREGÃO ELETRÔNICO Nº 002/2025

1. DAS CONDIÇÕES GERAIS DA CONTRATAÇÃO (art. 6º, XXIII, "a" e "i" da Lei n. 14.133/2021).

1.1. DO OBJETO

Contratação de empresa especializada, que possua outorga da Agência Nacional de Telecomunicações, Prestação de serviços de Internet meio de Link de Internet via óptica com oferta mínima de 1 IPv4 Fixo (público e válido) com Gerenciamento, por meio de link de dedicado de com velocidade de 200 mbps, com fornecimento de equipamento SD-WAN, incluindo o Serviço de Firewall, com suporte técnico 24 horas por dia e 7 (sete) dias por semana, inclusive feriados, mediante contato telefônico com contato direto ao suporte, além da prestação de serviços de implantação das soluções, configuração, manutenção preventiva e corretiva. Link de Internet Dedicado com velocidade de 200 Mbps, com fornecimento equipamento SD-WAN.

2. DA JUSTIFICATIVA DA CONTRATAÇÃO

2.1. A necessidade da contratação encontra-se pormenorizada no ETP (Estudo Técnico Preliminar). Anexa a esse Termo de Referência.

2.2. O objeto desta contratação **não** se enquadra como sendo de bem de **luxo**, conforme Decreto nº 10.818, de 2021.

2.3. O **prazo de vigência** da contratação é **60 (sessenta) meses** (5 anos), contados a partir da Autorização de Fornecimento na forma do artigo 105 da Lei n° 14.133/2021, podendo ser prorrogado na forma do art. 106 e 107 da referida norma legal. A prorrogação poderá, inclusive, contemplar a renovação proporcional do quantitativo contratado, observado o interesse da Administração, a vantajosidade da contratação e a manutenção das condições inicialmente pactuadas.

2.4. O **valor máximo total estimado** R$ 21.795,96 (vinte e um mil setecentos e noventa e cinco reais e noventa e seis centavos). Para um período de 12 (doze meses).

2.5. Da modalidade: **Pregão Eletrônico.**

2.6. Critério de julgamento **menor preço GLOBAL**

3. DOS ITENS, QUANTIDADES E VALORES / VIGÊNCIA CONTRATUAL / FUNDAMENTAÇÃO

LOTE ÚNICO				
Item	**Descrição**	**QTD**	**Preço Unitário Mensal Máximo Estimado R$**	**Valor Total Anual Máximo Estimado R$**
1	Prestação de serviços de Internet meio de Link de Internet via óptica com oferta mínima de 1 IPv4 Fixo (público e válido) com Gerenciamento, por meio de link de dedicado de com velocidade de 200 mbps, com fornecimento de equipamento SD-WAN, incluindo o Serviço de Firewall, com suporte técnico 24 horas por dia e 7 (sete) dias por semana, inclusive feriados, mediante contato telefônico com contato direto ao suporte, além da prestação de serviços de implantação das soluções, configuração, manutenção preventiva e corretiva. Link de Internet Dedicado com velocidade de 200 Mbps, com fornecimento equipamento SD-WAN.	1	1.816,33	21.795,96

3.1. Todos os requisitos e especificações técnicas dos itens da Tabela estão descritos neste Termo de Referência;

3.2. Os serviços serão prestados sob a forma de execução indireta, no regime de empreitada por preço unitário vinculado à cada modalidade, sendo que sua utilização será realizada à medida das necessidades da CONTRATANTE, portanto, sob demanda;

3.3. A quantidade Total de cada item é mera previsão futura que poderá ser concretizada total ou parcialmente, conforme demanda da CONTRATANTE;

3.4. O critério de julgamento da licitação é MENOR PREÇO GLOBAL por lote para a seleção da proposta mais vantajosa;

3.5. A LICITANTE deverá consignar, na forma expressa do sistema eletrônico, o valor global da proposta, já considerados e inclusos todos os tributos, fretes, tarifas e demais despesas decorrentes da execução do objeto, evitando assim prejuízo para o conjunto da solução e perda de economia de escala.

3.6. O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto nº 10.818, de 2021.

3.7. Por se tratar de serviço contínuo, o prazo de vigência da contratação será de 5 (cinco) anos, podendo ser prorrogado, observado o disposto no artigo 107 da Lei

14.133/21. A justificativa desta vigência contratual, se encontra anexa ao ETP – Estudo Técnico Preliminar.

3.8. Alterações do contrato e dos preços, deverão observar o disposto no art. 124 e art. 125 da lei 14.133/21, com as devidas justificativas.

3.9. Será permitida a subcontratação parcial do objeto, o que está definido em tópico específico desse Termo de Referência.

3.10. Critério de julgamento é menor preço global na modalidade pregão eletrônico.

3.11. O prazo máximo de execução do objeto, deverá ocorrer no prazo de máximo de 30 dias corridos, contados da assinatura do contrato.

3.12. O Pregão é definido pela Lei nº 14.133/2021, no seu inciso XLI do artigo 6º, como a "modalidade de licitação obrigatória para aquisição de bens e serviços comuns, cujo critério de julgamento poderá ser o de menor preço ou o de maior desconto".

3.13. A definição de bens e serviços comuns está prevista no inciso XIII do artigo 6º da Lei nº 14.133/2021: "aqueles cujos padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado"

4. LOCAL DE ENTREGA DOS BENS E SERVIÇOS

4.1. A entrega deverá ser realizada na Sede da Câmara Municipal de Campina Verde, situada na rua 26, nº. 114, Centro, Campina Verde, Minas Gerais – CEP – 38 270 000.

5. ESPECIFICAÇÕES TÉCNICAS

5.1. **LINK DEDICADO REQUISITOS GERAIS**

5.1.1. Toda a infraestrutura de rede, acesso a CPE da CONTRATADA deverão ser dimensionados e preparadas para suportar a totalidade do serviço;

5.1.2. A CONTRATADA deverá reservar os canais de comunicação e as portas de acesso à sua infraestrutura para uso exclusivo da CONTRATANTE, não sedo admitido o compartilhamento desses recursos com outro de seus clientes ou usuários;

5.1.3. O acesso referido do item anterior deverá ser provido por meio de backbone próprio da prestadora de serviço;

5.1.4. Os equipamentos da CONTRATADA utilizados em toda a solução deverão ser novos e compatíveis com ambientes corporativos;

5.1.5. A CONTRATADA obriga-se a se responsabilizar e prestar o serviço objeto da licitação, por meio de mão de obra especializada, em conformidade com as especificações do Termo de Referência.

5.1.6. Novos Links deverão ser instalados mediante viabilidade técnica. Neste caso será devido o pagamento de nova contratação, de acordo com o valor da instalação apurado no presente processo;

5.1.7. Será de responsabilidade da CONTRATANTE o fornecimento de energia elétrica para alimentação dos equipamentos nas dependências das unidades, o aterramento da rede elétrica e a climatização das dependências.

5.2. **CARACTERÍSTICAS DO LINK DE INTERNET DEDICADO**

5.2.1. Fornecer e instalar link de internet na taxa de XXX Mbps;

5.2.2. A CONTRATADA deverá disponibilizar 01 endereço IPv4 fixo e válido para o provimento da solução de internet.

5.2.3. Contratação de empresa especializada para o fornecimento de acesso à Rede Mundial de Internet com 100% de garantia de banda downstream e upstream, full duplex, com conectividade em protocolos IPv4 e IPv6;

5.2.4. A CONTRATADA deverá atender as seguintes exigências de Backbone IP para estar apta a prestar os serviços de Internet especificados neste Termo de Referência:

5.2.4.1. O provedor deve ter o seu backbone IP com saída internacional através de conexão direta para os Estados Unidos da América (EUA), com, no mínimo, 100 Gbps. Essa saída deve ser composta por uma ou mais conexões “ponto a ponto” entre o backbone IP do provedor do AS remoto, sem backbone intermediários;

5.2.4.2. O backbone IP do provedor deve ter saída com destino direto para pelo menos outros 03 (três) provedores de backbone IP Nacionais, com banda não inferior a 200 Gbps;

5.2.5. A conexão entre o CPE da CONTRATADA e o equipamento da CONTRATANTE deverá ser realizada através de interface Gigabit Ethernet 1000BASE-T;

5.2.6. A CONTRATADA poderá utilizar acesso de terceiro como última milha, sedo de inteira responsabilidade da CONTRATADA o cumprimento dos SLA especificados no edital.

5.2.7. O acesso físico (conexão entre o ponto de presença da CONTRATADA e os equipamentos de comunicação de dados da CONTRATADA instalados nas dependências da CONTRATANTE) deverá ser realizado exclusivamente por meio de fibra óptica, sendo vedada a utilização de qualquer outra tecnologia de acesso;

5.2.8. O serviço de Internet deverá ser entregue em rede roteada, utilizando protocolos de camada 3, com SLA 99,5% de disponibilidade e MTTR de 4 horas;

5.2.9. Disponibilizar serviço de Domain Name Resolution (DNS) da CONTRATADA, capaz de resolver direta e reversamente endereços de Internet, para registro de servidor DNS primário;

5.2.10. Ser monitorado em regime 24x7 por centro de monitoração da CONTRATADA, sendo responsável pela administração e gerência de

equipamentos e links de comunicação de dados, manutenção dos níveis mínimos de serviços exigidos e prevenção e recuperação de falhas de serviço;

5.2.11. Disponibilizar informações sobre os serviços de acesso à Internet por meio de um portal de Monitoramento, com acesso restrito, utilizando protocolo seguro (HTTPS), contendo estatísticas de desempenho e de disponibilidade do acesso;

5.2.12. Possibilitar que a equipe técnica da CONTRATANTE realize consultas no portal de monitoramento, bem como visualizar relatórios das informações de desempenho dos serviços contratados;

5.2.13. A CONTRATADA não poderá:

5.2.13.1. Implementar nenhum tipo de filtro de pacotes que possa incidir sobre o tráfego originado ou destinado à CONTRATANTE, a menos que tenha expressa concordância com esta;

5.2.13.2. Implementar nenhum tipo de cache transparente a menos que tenha expressa concordância da CONTRATANTE;

5.3. **CARACTERÍSTICAS DO ROTEADOR**

5.3.1. O roteador a ser instalado no ambiente da CONTRATANTE deverá ter, no mínimo, as seguintes características técnicas:

5.3.1.1. O equipamento e seus módulos e softwares não deverão constar em nenhuma lista do fabricante com as situações de “End-of-Sale”, “End-of-Order”, “End-of-Life” ou “End-of-Support”;

5.3.1.2. Deve possuir, no mínimo, 4 interfaces Gigabit Ethernet padrão 1000BASE-T;

5.3.1.3. Possuir protocolo SNMP habilitado com acesso de leitura;

5.3.1.4. Deve implementar os protocolos de roteamento RIP, OSPFv2, OSPFv3 e BGP-4;

5.3.1.5. Deve possuir suporte nativo ao protocolo IPv6;

5.3.1.6. Deve possuir suporte ao protocolo Netflow v9 ou superior;

5.3.1.7. Deve possuir suporte ao protocolo 802.1q;

5.3.1.8. Deve possuir suporte ao protocolo Telnet e SSHv2;

5.3.1.9. Deve possuir gerenciamento local através de uma porta console, sendo que todos os cabos e adaptadores necessários para o gerenciamento através da porta console deverão ser fornecidos pela CONTRATADA de forma a propiciar o gerenciamento do roteador a partir de uma porta USB;

5.3.1.10. Deve ser disponibilizado para a CONTRATANTE com o último release de software estável disponibilizado pelo fabricante do referido software durante o período de vigência do contrato;

5.3.1.11. Deve ser montável em rack padrão EIA-310 com largura padrão 19” ocupando no máximo 1U de altura.

5.4. **PORTAL DE GERENCIAMENTO E ACOMPANHAMENTO DOS SERVIÇOS PARA O LINK DEDICADO**

5.4.1. A CONTRATADA deverá disponibilizar um Portal WEB de gerência, possibilitando a visualização online dos serviços prestados, como também realizar o registro e acompanhamento dos chamados;

5.4.2. Consulta e visualização online: O Portal deverá apresentar informações relativas aos ativos de rede utilizados com as seguintes funcionalidades:

5.4.2.1. Alerta em caso de falhas e anormalidade dos circuitos;

5.4.2.2. Topologia da rede, incluindo roteadores e circuitos, com a visualização do status de todos os elementos;

5.4.2.3. Visualização da utilização de banda dos circuitos, com a visualização do status de todos os elementos;

5.4.2.4. Visualização do consumo de CPU e memória dos roteadores;

5.4.2.5. Indicação dos roteadores contendo a configuração física de cada equipamento (interface, memória, CPU etc.), modelo, fabricante, endereços IP e máscaras.

5.4.3. Registro e acompanhamento de chamados:

5.4.3.1. Permitir o acompanhamento dos registros de problemas e das ações executadas para a recuperação dos serviços relativos à pelo menos aos últimos 90 (noventa) dias, incluindo as seguintes informações:

5.4.3.1.1. Identificação do registro (Número do chamado);

5.4.3.1.2. Data e Hora de abertura do chamado (registro);

5.4.3.1.3. Descrição do problema;

5.4.3.1.4. Identificação do reclamante (Nome e telefone);

5.4.3.1.5. Data e hora de conclusão do atendimento (fechamento do chamado);

5.4.3.1.6. Ações realizadas para a solução do problema.

6. SD-WAN

6.1. Entende-se como tecnologia SD-WAN (Software-Defined WAN):

6.1.1. A rede de área ampla definida por software que centraliza a gerência da rede WAN em uma console única, eliminando a necessidade de intervenções manuais em roteadores em localidades remotas, proporcionando visibilidade do tráfego, seleção de caminho dinâmico baseado em políticas de QoS, aplicação ou performance e utilização de túneis VPN para comunicação entre os sites remotos;

6.1.2. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma ampliação;

6.1.3. A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por ping, http, tcp/udp echo;

6.1.4. Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo;

6.1.5. A solução deve permitir a definição do roteamento para cada aplicação;

6.1.6. Diversas formas de escolha de link devem estar presentes, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação;

6.1.7. Deve possibilitar a definição do link de saída para uma aplicação específica;

6.1.8. Deve implementar balanceamento de link por hash do IP de origem;

6.1.9. Deve implementar balanceamento de link por hash por IP de origem e destino;

6.1.10. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado para cada um dos links. Deve suportar o balanceamento de, no mínimo, 2 (dois) links;

6.1.11. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;

6.1.12. A solução de SD-WAN deve possuir suporte a Policy based routing ou Policy based forwarding;

6.1.13. Deve suportar roteamento estático e dinâmico (OSPF, BGP);

6.1.14. Deve possibilitar a agregação de túneis IPSec;

6.1.15. Deve possuir recursos para correção de erro (FEC), possibilitando a redução de perdas de pacotes nas transmissões;

6.1.16. Deve permitir a customização dos timers para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecidos;

6.1.17. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como YouTube, Facebook etc.), impactando no bom uso das aplicações de negócio, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de shaping. Dentre as tratativas possíveis, a solução deve contemplar:

6.1.17.1. Suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:

6.1.17.1.1. Por endereço de origem;

6.1.17.1.2. Por endereço de destino;

6.1.17.1.3. Por usuário e grupo;

6.1.17.1.4. Por aplicações;

6.1.17.1.5. Por porta;

6.1.18. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex.: banda mínima disponível para aplicações de negócio;

6.1.19. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex.: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como YouTube, Facebook etc.;

6.1.20. Deve ainda possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda;

6.1.21. O QoS deve possibilitar a definição de fila de prioridade;

6.1.22. Além de possibilitar e definição de banda máxima e garantida por aplicação, deve também suportar o match em categorias de URL, IPs de origem e destino, logins e portas;

6.1.23. Deve ter a capacidade de agendar intervalos de tempo onde as políticas de shaping/QoS serão válidas é mandatória. Ex.: regra de controle de banda mais permissivas durante o horário de almoço;

6.1.24. Uma vez que o tráfego é identificado, as políticas de shaping/QoS podem ser compartilhadas a todos os acessos que fizeram match na regra ou por IP. Ex.: 10 Mbps de banda garantida por IP ou para todos os IPs que fizeram match na regra;

6.1.25. Deve possibilitar a definição de bandas distintas para download e upload;

6.1.26. A solução de SD-WAN deve prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do health check (packet loss, jitter e latência);

6.1.27. A solução de SD-WAN deve suportar IPv6;

6.1.28. Deve possibilitar roteamento distinto a depender do grupo de usuário selecionado na regra de SD-WAN;

6.1.29. Deve ser capaz de bloquear acesso à aplicações;

6.1.30. Deve suportar NAT dinâmico bem como NAT de saída;

6.1.31. Deve suportar balanceamento de tráfego por sessão e pacote;

6.1.32. As funcionalidades de SD-WAN devem ser fornecidas no NGFW;

6.1.33. Deve implementar balanceamento de link por custo configurado do link;

6.1.34. Deve suportar o balanceamento de, no mínimo, 5 links;

6.1.35. Deve suportar o balanceamento de links e interfaces físicas, sub interfaces lógicas de VLAN e túneis IPSec;

6.1.36. Deve suportar o balanceamento de links LTE (4G) sem restrições de uso, podendo ser usado em conjunto com outros links e não ser somente o backup para toso os outros links;

6.1.37. Deve gerar log de eventos que registrem alterações no estado dos links do SD-WA, monitorados pela checagem de saúde;

6.1.38. Deve suportar Zero-Touch Provisioning;

6.1.39. Possuir checagem do estado de saúde do link baseando-se em critérios mínimo de: Latência, Jitter e Perda de Pacotes;

6.1.40. Deve ser possível configurar a porcentagem de perda de pacotes e o tempo de latência e jitter, na medição de estado de link. Estes valores serão utilizados pela solução para decidir qual link será utilizado;

6.1.41. A solução deve permitir modificar o intervalo de tempo de checagem, em segundos, para cada um dos links;

6.1.42. A checagem de estado de saúde deve suportar teste com Ping, HTTP e DNS;

6.1.43. As regras de escolha do link SD-WAN devem suportar o reconhecimento de aplicações, grupos de usuários, endereços IP e de destino e Protocolo;

6.1.44. Deve suportar a configuração de nível mínimo, de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SD-WAN;

6.1.45. Deve suportar envio de BGP Route-Map para BGP Neighbors, caso a qualidade mínima de um link não seja detectada pela checagem de saúde do link;

6.1.46. Deve ser possível utilizar o balanceamento round Robin na agregação de duas ou mais IPSec VPN determinando o peso para cada VPN;

6.1.47. Deve ser possível especificar o número mínimo de interfaces ativas em uma regra de SD-WAN para que esta regra seja válida;

6.1.48. A solução deve permitir a duplicação de pacotes entre dois ou mais links, que atendam os parâmetros de qualidade estabelecidos, objetivando uma melhor experiência de uso de aplicações;

6.1.49. Deve dispor de opções que maximize o uso de largura de banda utilizando os links WANS que estejam dentro do nível de saúde estipulado;

6.1.50. Deve possuir capacidade de classificação de tráfego com pobres de SLA, garantindo dessa forma a priorização do tráfego em momentos de congestionamento, evitando oscilações do link SD-WAN.

6.2. **EQUIPAMENTO FIREWALL**

6.2.1. Throughput de, no mínimo, 7.5 Mpps de Firewall (pacote por segundo);

6.2.2. Suporte a, no mínimo, 650 mil de conexões simultâneas (TPC);

6.2.3. Suporte a, no mínimo, 30 mil novas conexões por segundo (TPC);

6.2.4. Throughput de, no mínimo, 2.5 Gbps de VPN IPSec, com pacote de, no mínimo, 512 bytes;

6.2.5. Estar licenciado para, ou suportar o uso de licença, 200 túneis de clientes VPN IPSec simultâneos;

6.2.6. Estar licenciado para, ou suportar sem o uso de licença, 200 túneis de clientes VPN IPSec simultâneos;

6.2.7. Suportar, no mínimo, 900 Mbps de Throughput de IPS;

6.2.8. Suportar, no mínimo, 700 Mbps de Throughput de controle de aplicação;

6.2.9. Suportar, no mínimo, 300 Mbps de Throughput de inspeção SSL;

6.2.10. Throughput de, no mínimo, 490 Mbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e AntiSpyware;

6.2.11. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma para destas funcionalidades, somente o de menor valor será aceito;

6.2.12. Possuir ao menos 4 interfaces RJ45;

6.2.13. Deve incluir porta USB compatível com modem 3G/4G, permitindo ainda que este link WAN seja utilizado nas regras de SD-WAN;

6.2.14. Possuir fonte de alimentação com fonte DC de 100-240V AC, 50-60Hz;

6.2.15. Em caso de uma atualização do sistema que acrescentem novas funcionalidades eles devem funcionar sem a necessidade de aquisição de nova licença;

6.2.16. Caso o fabricante remova o produto de linha, a CONTRATADA deve substituir o produto entregue pela nova geração com capacidade e funcionalidade igual ou superior ao removido da linha de produção;

6.2.17. Deve possuir garantia de hardware e software durante a vigência do contrato;

6.2.18. Deve possuir licenciamento perpetuado para as funcionalidades;

6.2.19. As funcionalidades a seguir devem seguir funcionando, mesmo após vencimento do contrato de suporte e licenciamento: SD-WAN, controle de aplicações e stateful firewall;

6.2.20. Deve possuir licenciamento durante a vigência do contrato para as subscrições de filtro de conteúdo, antivírus, controle de aplicações, IPS e outras que façam parte do produto e da oferta.

6.3. **ESPECIFICAÇÕES TÉCNICAS**

6.3.1. Todos os equipamentos necessários para a conexão entre os pontos serão fornecidos pela empresa CONTRATADA;

6.3.2. Todos os equipamentos e seus componentes deverão ser novos, sem uso, e entregues em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais e acompanhados de todos os acessórios necessários às suas instalações;

6.3.3. Nenhum dos modelos ofertados poderá estar listado no site do fabricante em listas de EOL (End-of-Life) e EOS (End-of-Sale) na data da proposta;

6.3.4. Não serão aceitas soluções baseadas em PCs de uso geral e sim soluções baseadas em appliances desenvolvidos especificamente para a função de Firewall. O Fabricante deve garantir a interoperabilidade do software com o

hardware assegurando a padronização e compatibilidade funcional de todos os recursos;

6.3.5. Os roteadores, de propriedade da CONTRATADA deverão ser fornecidos, instalados, configurados, mantidos, gerenciados e operados pelo mesmo e deverá ser garantido o desempenho e os níveis de serviços;

6.3.5.1. A Gestão do Firewall para aplicação de regras, bloqueio, políticas, entre outras funcionalidades, deverão ser de forma hibrida entre a CONTRATADA e a CONTRATANTE;

6.3.5.2. A CONTRATADA deverá fornecer acesso aos equipamentos (senhas de acesso), para a CONTRATANTE para fazer a gestão híbrida do equipamento.

6.3.6. Todas as atualizações e correções (patches) de software, necessárias para o cumprimento dos requisitos exigidos, deverão ser realizadas sem ônus adicionais para a CONTRATADA;

6.3.7. Todos os firewalls a serem disponibilizados pelo FORNECEDOR no sítio deverão atender as características desse Termo de Referência.

6.4. **CARACTERÍSTICAS EXIGIDAS PARA OS FIREWALLS**

6.4.1. A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de Next Generation Firewall (NGFW) e SD-WAN não sendo permitido appliances virtuais ou solução open source (produto montado);

6.4.1.1. Apenas appliances concentradores deverão possuir funcionalidades de Next Generation (NGFW);

6.4.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

6.4.3. Por funcionalidades de SD-WAN entende-se: roteamento inteligente, uso do melhor link por aplicação, abstração do tráfego em relação aos circuitos físicos e controle do tráfego por aplicação;

6.4.4. As funcionalidades de segurança e SD-WAN que compõem a solução podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação, acompanham os mesmos termos de garantia, atualizações e manutenção, suporte e gerenciamento centralizado;

6.4.5. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

6.4.6. Todos os equipamentos fornecidos não devem ultrapassar a medida máxima de 2U cada;

6.4.7. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

6.4.8. Os dispositivos de proteção de rede devem possuir suporte a VLANs;

6.4.9. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM);

6.4.10. Deve suportar BGPv4/BGP4+, OSPFv2/v3, RIP e roteamento estático;

6.4.11. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;

6.4.12. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;

6.4.13. Os dispositivos de proteção de rede devem suportar sub interfaces ethernet lógicas;

6.4.14. Deve suportar NAT dinâmico (Many-to-Many);

6.4.15. Deve suportar NAT estático (1-to-1);

6.4.16. Deve suportar NAT estático bidirecional 1-to-1;

6.4.17. Deve suportar Tradução de porta (PAT);

6.4.18. Deve suportar NAT de Origem;

6.4.19. Deve suportar NAT de Destino;

6.4.20. Deve suportar NAT de Origem e NAR de Destino simultaneamente;

6.4.21. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

6.4.22. Deve suportar NAT46, NAT64;

6.4.23. Deve implementar o protocolo ECMP;

6.4.24. Deve permitir monitorar via SNMP ou uso de CPU, memória, espaço em disco, VPN, situação do cluster e violação de segurança;

6.4.25. Enviar log para sistemas de monitoração externos;

6.4.26. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;

6.4.27. Proteção anti-spoofing;

6.4.28. Deve suportar modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

6.4.29. Deve suportar Modo Camada - 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;

6.4.30. Deve suportar Modo Camada - 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

6.4.31. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

6.4.32. A configuração em alta disponibilidade deve sincronizar;

- **6.4.32.1.** Sessões;
- **6.4.32.2.** Configurações, incluindo, mas não limitado às políticas de Firewall, NAT, QoS e objetos de rede;
- **6.4.32.3.** Associações de Segurança das VPNs;
- **6.4.32.4.** Tabelas FIB;

6.4.33. O HA (modo de alta-disponibilidade) deve possibilitar monitoração de falha de link;

6.4.34. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;

6.4.35. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;

6.4.36. O equipamento deve possuir suporte a 256 VLAN Tags 802.1Q;

6.4.37. O equipamento deve possuir suporte a agregação de links 802.3ad LACP;

6.5. **POLÍTICAS**

6.5.1. Deverá suportar controles por zonas de segurança;

6.5.2. Deverá suportar controle de políticas por porta e protocolo;

6.5.3. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

6.5.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

6.5.5. Controle de políticas por código de País (Ex.: BR, US, UK, RU);

6.5.6. Deve descriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;

6.5.7. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

6.5.8. Suporte a objetos a regras IPv6;

6.5.9. Suporte a objetos e regras multicast;

6.5.10. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

6.5.11. Deverá ter a capacidade de permitir a criação de regras de segurança específicos para tipos de dispositivos identificados automaticamente (funcionalidade esta conhecida como BYOD – Bring Your Own Device), como, por exemplo: tablets, celulares e PCs, sistemas operacionais Android, Apple, Blackberry, Linux e Windows podendo tomar ações como: colocar o dispositivo em VLAN de quarentena, aplicar bloqueios e filtros na interface do firewall.

6.6. **PREVENÇÃO E AMEAÇAS**

6.6.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulos de IPS, antivírus e AntiSpyware integrados no próprio appliance firewall;

6.6.2. Deve incluir assinaturas de prevenção de instrução (IPS) e bloqueio de arquivos maliciosos (Antivírus e AntiSpyware);

6.6.3. Deve sincronizar as assinaturas de IPS, Antivírus, AntiSpyware quando implementado em alta disponibilidade;

6.6.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;

6.6.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

6.6.6. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

6.6.7. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura;

6.6.8. Deve suportar granularidade nas políticas de IPS, Antivírus e AntiSpyware, possibilitando a criação de diferentes políticas por zona de segurança de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

6.6.9. Deve permitir o bloqueio de vulnerabilidades;

6.6.10. Deve permitir o bloqueio de exploits conhecidos;

6.6.11. Deve incluir proteção contra ataques de negação de serviços;

6.6.12. Ser imune e capaz de impedir ataques básicos como: Syn Flood, ICMP Flood, UDP Flood etc.;

6.6.13. Detectar e bloquear a origem de portscans;

6.6.14. Bloquear ataques efetuados por Worms conhecidos;

6.6.15. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

6.6.16. Possuir assinaturas para bloqueio de ataques de buffer overflow;

6.6.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

6.6.18. Deve permitir usar operadoras de negação na criação de assinaturas customizadas de IPS ou AntiSpyware, permitindo a criação de exceções com granularidade nas configurações;

6.6.19. Permitir o bloqueio de vírus e spyware em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB/CIFS, SMTP, IMPA e POP3;

6.6.20. Identificar e bloquear comunicação com botnets;

6.6.21. Registrar no console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

6.6.22. Os eventos devem identificar o país de onde partiu a ameaça;

6.6.23. Deve incluir proteção contra vírus em conteúdo HTML e Javascript, software espião (Spyware) e Worms;

6.6.24. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

6.6.25. Deve ser possível configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança etc., ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sedo essas

políticas por usuários, grupos de usuários, origem, destino, zonas de segurança;

6.6.26. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;

6.6.27. A solução de sandbox deve ser capaz de criar assinaturas e ainda incluí-las a base de antivírus do firewall, prevenindo e reincidência do ataque;

6.6.28. A solução de sandbox deve ser capaz de incluir no firewall as URLs identificadas como origens de tais ameaças desconhecidas (block list), impedindo que esses endereços sejam acessados pelos usuários de rede novamente;

6.6.29. Dentre as análises efetuadas, a solução deve suportar antivírus, query na nuvem, emulação de código, sandboxing e verificação de call-back;

6.6.30. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado.

6.7. **FILTRO DE URL**

6.7.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia de semana e hora);

6.7.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

6.7.3. Deve possuir capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através de integração com serviços de diretório, Active Directory e base de dados local;

6.7.4. A identificação pela base do Active Directory deve permitir SSO, de forma que o usuário não precise logar novamente na rede para navegar pelo firewall;

6.7.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

6.7.6. Possuir pelo menos 60 categorias de URLs;

6.7.7. Deve possuir a função de exclusão de URLs do bloqueio;

6.7.8. Permitir a customização de página de bloqueio.

6.8. **IDENTIFICAÇÃO DO USUÁRIO**

6.8.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de usuários;

6.8.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários grupos de usuários;

6.8.3. Deve possuir integração e suporte a Microsoft Active Directory para no mínimo o sistema operacional Windows Server 2012 R2;

6.8.4. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sing-on. Essa funcionalidade não deve possuir limites licenciados de usuários;

6.8.5. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

6.8.6. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de Usuários;

6.8.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

6.8.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambiente Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuários sobre o uso das aplicações que estão nestes serviços;

6.8.9. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

6.9. **FILTRO DE DADOS E GEOLOCALIZAÇÃO**

6.9.1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF etc.), identificados sobre aplicações (HTTP, FTP);

6.9.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

6.9.3. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

6.9.4. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

6.10. **VPN**

6.10.1. Suportar VPN Site-to-Site e Client-to-Site;

6.10.2. Suportar IPSec VPN;

6.10.3. A VPN IPSec deve suportar criptografia 3DES, AES128, AES192 e AES256 (Advanced Encryption Standard);

6.10.4. A VPN IPSec deve suportar autenticação MD5, SHA1, SHA256, SHA384 e SHA512;

6.10.5. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Group 15 até 21;

6.10.6. A VPN IPSec deve suportar algoritmo Internet Key Exchange (IKEv1 e v2);

6.10.7. A VPN IPSec deve suportar Autenticação via certificado IKE PKI;

6.10.8. Deve possuir interoperabilidade com no mínimo os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, Sonicwall;

6.10.9. Deve permitir que todo o tráfego dos usuários remots de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

6.10.10. Atribuição de DNS nos clientes remotos de VPN;

6.10.11. Suportar autenticação via AD/LDAP, certificado e base de usuários local;

6.10.12. Suportar leitura e verificação de CRL (Certificate Revocation List);

6.10.13. Deverá manter uma conexão segura com o portal durante a sessão;

6.10.14. O agente IPSec Client-to-Site deve ser compatível com pelo menos: Windows 10 (32 e 64 Bits) ou superior.

7. PROVA DE CONCEITO – POC

7.1. A CONTRATANTE poderá solicitar uma Prova de Conceito que tem por objetivo aferir via demonstração que a PROPONENTE, classificada provisoriamente em primeiro lugar, dispõe de solução corporativa de telefonia fixa, com todos os requisitos mínimos previstos neste documento, bem como se detém o conhecimento sobre sua operacionalização;

7.2. A POC será realizada no prazo de até 07 (sete) dias úteis, contados a partir da data da convocação, em data, local, horário e com duração a serem informados oportunamente pelo CONTRATANTE;

7.3. A condução da POC será realizada minimamente, pelos integrantes requisitantes e técnicos;

7.4. A POC Será realizada conforme condições e requisitos previstos no ANEXO I – Prova de Conceito (POC);

7.5. A POC possui caráter eliminatório, logo, caso o PROPONENTE seja desclassificado nessa prova, será desclassificada deste lote, sendo convocado o PROPONENTE classificado imediatamente a seguir;

7.6. A POC será direcionada apenas para o item de Voz em Nuvem do Lote 2 desse certame.

8. SUBCONTRATAÇÃO

8.1. Será permitida a subcontratação parcial do objeto referente ao serviço de plataforma em nuvem, porém em qualquer hipótese de subcontratação, permanece a responsabilidade integral da CONTRATADA pela perfeita execução contratual, cabendo-lhe realizar a supervisão e coordenação das atividades da subcontratada, bem como responder perante o CONTRATANTE pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da subcontratação;

8.2. Não será permitido a subcontratação do tráfego STFC, sendo obrigatório que os números DDR disponibilizados sejam da própria LICITANTE junto à ABR

Telecom, bem como deverá ser apresentado pelo menos 01 (uma) declaração que possui interconexão com outras operadoras que compreenda a área local a ser atendida;

8.3. A LICITANTE deve ser detentora do plano de numeração registrado junto a ABR Telecom da região solicitada, não podendo ser subcontratado a parte inerente ao objeto STFC;

8.4. Para os demais itens não será permitida a subcontratação, permanecendo a responsabilidade integral da CONTRATADA pela perfeita execução contratual, cabendo-lhe realizar a supervisão e coordenação das atividades;

8.5. Não será permitido a subcontratação do Serviço Móvel Pessoal, sendo obrigatório que os números disponibilizados sejam da própria LICITANTE.

9. QUALIFICAÇÃO TÉCNICA

9.1.1. Apresentar certificado de autorização para exploração de SCM (Serviço de Comunicação Multimídia) emitido pela ANATEL;

9.1.2. Os atestados de capacidade técnica devem ter o serviço de Link Dedicado, SD-WAN/Firewall e Banda Larga comprovando os serviços necessários para compor a solução sendo permitida a somatório de atestados para a comprovação, fornecidos por pessoa jurídica de direito público ou privado, com, no mínimo, 1 ano de prestação dos serviços;

9.1.3. O(s) atestado(s) deverá(ão) ser apresentado(s) em papel timbrado, original ou cópia reprográfica, conter a identificação da pessoa jurídica emitente e a identificação do signatário. Deverá ser apresentado obrigatoriamente junto com a documentação de habilitação da PROPONENTE, sendo motivo de inabilitação da PROPONENTE do certame a ausência da sua apresentação;

9.1.4. Comprovação de aptidão de, no mínimo, 50% para desempenho de atividade pertinente e compatível com o objeto da licitação através de apresentação de Atestado de Capacidade Técnica;

9.1.5. Apresentar certificado de homologação da ANATEL referente ao equipamento SD-WAN contemplado na solução;

9.1.6. Deverá comprovar que possui certificação junto ao fabricante da solução ofertada, comprovando a capacitação técnica dos profissionais que serão responsáveis pelas tarefas de instalação, configuração e suporte dos produtos, mediante a entrega de cópia do certificado técnico destes profissionais junto ao fabricante;

9.1.7. Para comprovação, deverá ser apresentada CTPS do profissional, para apresentar vínculo com a PROPONENTE;

9.1.8. Deverá apresentar carta de parceria com o fabricante que comprove que está apto a comercializar e a operar seus produtos;

9.1.9. Deverá apresentar folheto de dados, manuais e outros meios necessários para comprovar o atendimento ao edital;

9.1.10. Para garantir a robustez e a confiabilidade de infraestrutura de rede do Sistema Autônomo, poderá ser da empresa CONTRATADA ou poderá considerar empresas incorporadas ou do mesmo grupo econômico que estejam conectadas ao Sistema Autônomo (ASN) da licitante;

9.1.11. A LICITANTE deverá comprovar que possui pelo menos um Ponto de Presença (PoP) na localidade da Contratante ou na Capital do estado.

10. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

10.1. Apresentação do Balanço Patrimonial acompanhado do termo de abertura e encerramento do Livro Diário e demonstração de Resultado Econômico contábil do último exercício social, já exigíveis e apresentados na forma da Lei, comprovando a boa situação da empresa, vedada a substituição por balancetes ou balanços provisórios, dispensando-se da apresentação as constituídas há menos de um ano, que não encerraram seu primeiro exercício;

10.2. As empresas obrigadas por lei a apresentar ECD – Escrituração Contábil Digital, deverão juntar o respectivo comprovante de transmissão ao SPED (Sistema Público de Escrituração Digital), bem como o Balanço Patrimonial (Instrução Normativa RFB nº 2.003, de 18 de janeiro de 2021);

10.3. Comprovação, firmada por contador da licitante, da boa situação da empresa, que será avaliada por meio dos seguintes índices financeiros a serem extraídos do balanço do último exercício social da empresa

a) Índice de Liquidez Corrente:

$$ILC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}} \geq 1{,}00 \text{ (um)}$$

b) Índice de Liquidez Geral:

$$ILG = \frac{\text{Ativo Circulante + Realizável a Longo Prazo}}{\text{Passivo Circulante + Exigível a Longo Prazo}} \geq 1{,}00 \text{ (um)}$$

c) Grau de Endividamento Geral:

$$GEG = \frac{\text{Passivo Circulante + Exigível a Longo Prazo}}{\text{Ativo Total}} \leq 0{,}50 \text{ (zero vírgula cinquenta)}$$

10.4. As empresas que apresentarem resultado inferior a 1(um) em qualquer dos índices de Liquidez Geral (LG), e Liquidez Corrente (LC), ou resultado inferior a 0,5 no Grau de Endividamento Geral (GEG), deverão comprovar patrimônio

líquido de 10% (dez por cento) do valor total estimado da contratação ou do item pertinente;

10.5. Certidão Negativa de existência de processo falimentar ou de recuperações previstas na Lei Federal nº 11.101 de 09/02/2005 ou, mesmo, de concordata em nome da licitante ajuizada em data anterior ao advento do diploma legal citado, expedida pelo distribuidor da sede da pessoa jurídica. A certidão requerida deve apresentar data inferior a 90 (noventa) dias da entrega das propostas;

10.6. A apresentação da contestação do pedido de falência, enquanto não proferida a sentença, deverá ser levada em conta pela Comissão de Licitação para efeito de qualificação econômico-financeira

11. PRAZO DE EXECUÇÃO/INSTALAÇÃO

11.1. O prazo máximo de execução do objeto, deverá ocorrer no prazo de máximo de 30 dias corridos, contados da assinatura do termo de contrato.

12. NÍVEIS MÍNIMOS DE SERVIÇO

12.1. A CONTRATADA deverá fornecer o serviço com os seguintes níveis mínimos de qualidade de prestação do serviço:

12.1.1. Internet Link

Métrica Serviços	**Nível Mínimo de Serviço**
Disponibilidade do serviço	>= 99,5%
Tempo de Reparo	4 horas

12.1.2. Banda Larga

Métrica Serviços	**Nível Mínimo de Serviço**
Disponibilidade do serviço	>= 95%
Tempo de Reparo	24 horas

17 **ADEQUAÇÃO** ORÇAMENTÁRIA

17.1 As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento da Câmara Municipal de Campina Verde/MG.

17.1.1 A contratação será atendida pela seguinte dotação:

Função: 01 – LEGISLATIVA
Sub- função: 01.031 – AÇÃO LEGISLATIVA
Programa: 01.031.0001 - AÇÃO LEGISLATIVA

Proj/Atividade: 2.006- CORPO LEGISLATIVO
Elem. da Despesa: 3.3.90.39.00 – OUTROS SERVIÇOS DE TERCEIROS – PESSOA JURÍDICA
Sub Elemento: 43 – SERVIÇOS DE TELECOMUNICAÇÕES
01.01.00-01.031.0001.2.006-3.3.90.39.43

18 OBRIGAÇÕES DA CONTRATANTE

18.1. São obrigações da Contratante:

18.1.1. receber o objeto no prazo e condições estabelecidas no Termo de Referência deste edital;

18.1.2. verificar minuciosamente, no prazo fixado, a conformidade dos itens com as especificações constantes do edital e da proposta, para fins de aceitação e recebimento definitivo;

18.1.3. comunicar à Contratada, por escrito, sobre imperfeições, falhas ou

irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

18.1.4. acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de comissão/servidor especialmente designado;

18.1.5. efetuar o pagamento à contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Termo de Referência;

18.2. A Administração não responderá por quaisquer compromissos assumidos pela Contratada com terceiros, ainda que vinculados à execução do presente Termo de Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da Contratada, de seus empregados, prepostos ou subordinados.

18.3. Verificar, durante toda a execução do Contrato, a manutenção, pela Contratada, de todas as condições de habilitação e qualificação exigidas na Licitação, em compatibilidade com as obrigações assumidas;

18.4. Permitir o acesso dos empregados da Contratada ao local de fornecimento do material;

19. OBRIGAÇÕES DA CONTRATADA

19.1. A Contratada deve cumprir todas as obrigações constantes deste termo de referência e em seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

19.1.1. efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no edital e seus anexos, acompanhado da respectiva nota fiscal,

na qual constarão as indicações referentes a marca, fabricante, modelo, procedência e prazo de garantia ou validade;

19.1.2. responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

19.1.3. substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste edital, o objeto com avarias ou defeitos;

19.1.4. comunicar à Contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

19.1.5. manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

19.1.6. indicar preposto para representá-la durante a execução do contrato.

19.1.7. Garantir a substituição imediata dos produtos em casos de imprestabilidade ou não conformidade detectada no momento da entrega, mesmo que não haja prazo contratual de garantia, dado o caráter perecível dos alimentos.

19.1.8. Responder por quaisquer danos causados à Administração Pública ou a terceiros em decorrência de culpa ou dolo na execução do objeto contratado, inclusive por problemas sanitários, contaminações ou intoxicações alimentares.

19.1.9. Cumprir rigorosamente as normas técnicas e sanitárias vigentes, especialmente aquelas relativas à vigilância sanitária, segurança alimentar, transporte e armazenamento de alimentos.

19.1.10. Manter, durante toda a vigência contratual, ao menos um canal de comunicação eletrônico ativo e acessível com a contratante, por meio de telefone, e-mail institucional e/ou aplicativo de mensagens instantâneas (como WhatsApp), com prazo máximo de resposta de até 1 (uma hora) horas após o envio da solicitação pela contratante, nos dias úteis entre 12h e 18h. A ausência de retorno no prazo estabelecido poderá ser considerada infração contratual, sujeita às sanções previstas.

19.1.11. Encaminhar, obrigatoriamente, juntamente com a nota fiscal para pagamento, as certidões comprobatórias de regularidade fiscal e trabalhista exigidas na fase de habilitação, para verificação da manutenção das condições pela fiscalização contratual, nos termos do art. 147, §1º da Lei nº 14.133/2021.

20. DAS SANÇÕES

20.1. Comete infração administrativa o fornecedor que cometer quaisquer das infrações previstas no art. 155 da Lei Federal nº 14.133, de 2021.

20.1.1.dar causa à inexecução parcial do contrato;

20.1.2. dar causa à inexecução parcial do contrato que cause grave dano à Câmara, ao funcionamento dos serviços públicos ou ao interesse coletivo;

20.1.3. dar causa à inexecução total do contrato;

20.1.4. deixar de entregar a documentação exigida para o certame;

20.1.5. não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

20.1.6. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

20.1.7. ensejar o retardamento da execução ou da entrega do objeto sem motivo justificado;

20.1.8. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a sessão do pregão ou a execução do contrato;

20.1.9. fraudar a sessão do pregão ou praticar ato fraudulento na execução do contrato;

20.1.10. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

20.1.11. praticar atos ilícitos com vistas a frustrar os objetivos deste certame.

20.1.12. praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

20.2. O fornecedor que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

a) Advertência pela falta do subitem 20.2.1 deste termo de referência, quando não se justificar a imposição de penalidade mais grave;

b) Multa de 10% (dez por cento) sobre o valor estimado dos itens prejudicados pela conduta do fornecedor, por qualquer das infrações dos subitens 20.2.1 a 20.2.12;

c) Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, nos casos dos subitens 20.2.2 a 20.2.7 deste termo de referência, quando não se justificar a imposição de penalidade mais grave;

d) Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 20.2.8 a 20.2.12, bem como nos demais casos que justifiquem a imposição da penalidade mais grave;

20.3. Na aplicação das sanções serão considerados:

20.3.1. a natureza e a gravidade da infração cometida;

20.3.2. as peculiaridades do caso concreto;

20.3.3. as circunstâncias agravantes ou atenuantes;

20.3.4. os danos que dela provierem para a Administração Pública;

20.3.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

20.4. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pela Administração ao contratado, além da perda desse valor, a diferença será cobrada judicialmente.

20.5. A aplicação das sanções previstas neste termo de referência não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Câmara Municipal.

20.6. A penalidade de multa pode ser aplicada cumulativamente com as demais sanções.

21. DO PAGAMENTO

21.1. FORMA DE PAGAMENTO

21.1.1.O pagamento será realizado mensalmente, mediante emissão de boleto ou através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

21.2**. PRAZO DE PAGAMENTO**

21.2.1. O pagamento será efetuado após a emissão do boleto correspondente, mediante apresentação da Nota Fiscal, devidamente atestada pelo responsável no acompanhamento e recebimento dos produtos/serviços.

21.2.2. Nenhum pagamento será efetuado à contratada enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência, sem que isso gere direito ao pleito de reajustamento dos preços ou correção monetária.

21.2.3. Deverá ser emitida Nota Fiscal em nome da Câmara Municipal conforme descrição da Autorização de Fornecimento.

21.2.4. A Nota Fiscal que for apresentada com erro será devolvida ao detentor, para retificação ou substituição.

21.2.5. Para realização dos pagamentos, o licitante vencedor deverá manter a regularidade fiscal apresentada durante processo de habilitação;

21.2.6. A retenção do imposto de renda deverá ser destacada no corpo do documento fiscal, conforme disposto no decreto Municipal do Município de Campina Verde/MG N° 055/2023 de 02 de agosto de 2023. Que pode ser visualizado no endereço eletrônico - https://www.campinaverde.mg.leg.br/leis/decretos/decreto-055-2023/view

22. DAS DISPOSIÇÕES GERAIS

22.1. A Câmara Municipal poderá revogar a licitação ou rescindir o contrato, por motivo de interesse público e deverá realizar a anulação da licitação quando houver ilegalidade, sendo de ofício ou mediante provocação de terceiro;

22.2. Os casos omissos no Termo de Referência, deverão ser supridos pela Lei nº. 14.133/2021 e suas alterações.

22.3. Fica estabelecido o Foro da Comarca do Município de Campina Verde/MG para dirimir quaisquer dúvidas oriundas das avenças.

22.4. Faz parte desse Termo de Referência o ANEXO I.

Campina Verde, 30 de outubro de 2025

Leonardo Freitas Caetano Tostes
Presidente da Câmara Municipal

ANEXO I – PROVA DE CONCEITO (POC)

12.2. A POC será realizada nas dependências da CONTRATANTE ou poderá ser realizada de forma remota de acordo com o indicado no documento de convocação;

12.3. O ato de convocação, será expedido preferencialmente por meio eletrônico, com confirmação de resposta, e informará a data, local e horário da realização da POC;

12.4. Para realizar a POC, a CONTRATANTE se limitará a disponibilização do circuito de Internet, deste modo caberá a PROPONENTE dispor de todos os equipamentos, acompanhada de software, manuais, guias de instalação e outros documentos necessários para dirimir as dúvidas, a fim de que possa ser realizado procedimento de verificação com os requisitos técnicos requeridos nesta contratação;

12.5. Após iniciada a POC, não será permitida a alteração de códigos, compilação, correção, update e outros. Caso esse fato seja constatado pela equipe avaliadora, a PROPONENTE terá sua proposta sumariamente desclassificada;

12.6. Realizada a POC, a CONTRATANTE emitirá parecer conclusivo sobre a realização da prova, do qual conste manifestação sobre o atendimento de todas as funcionalidades requeridas para as ferramentas;

12.7. O parecer conclusivo será encaminhado à Comissão de Licitação, para prosseguimento do certame;

12.8. Se a PROPONENTE não demonstrar o atendimento à totalidade das funcionalidades requeridas, nos casos de teste, a proposta será desclassificada, devendo ser chamada a próxima colocada na etapa de lances para apresentar sua proposta de preços e documentação de habilitação e consequentemente realizar os procedimentos relativos a prova de conceito nas mesmas condições discriminadas nessa contratação;

12.9. Para a presente POC, foi estabelecido o conjunto mínimo que a PROPONENTE deverá demostrar, conforme casos de testes a seguir:

Tabela 01 - POC 01.

Das funcionalidades do Sistema de Gestão

Id.	Funcionalidades Gerais	Atende	Não atende
1.	Todo o gerenciamento e operação do sistema deverá ser disponibilizado através de interface Web, sem a necessidade de instalação de aplicativos ou clientes locais.		
2.	A ferramenta de gerenciamento deverá permitir a configuração de perfis de usuários, no mínimo 03 (três), definindo níveis de acesso a cada perfil.		

3.	Deverá possuir painéis para acompanhamento em tempo real (dashboard), que apresentem pelo menos as seguintes informações:		
4.	Disponibilidade da solução, apresentando para um período pré-determinado, o tempo de indisponibilidade da plataforma.		
5.	Disponibilidade de cada ramal telefônico, com indicação de status/cor: disponível/verde, ocupado/vermelho, indisponível/cinza.		
6.	Deverá permitir a visualização de todos os ramais telefônicos da solução, com identificação do seu número, setor, local e data de instalação.		
7.	Visualização de todas as chamadas em curso, por perfil de tráfego (ramal-ramal, local, móvel, LDN).		
8.	Visualização do consumo de minutagem, por perfil de tráfego (ramal-ramal, local, móvel, LDN)		
9.	Visualização da lista telefônica pública e privada.		
10.	Deverá permitir a emissão de relatórios que apresentem as seguintes informações:		
11.	Disponibilidade da solução.		
12.	Disponibilidade de cada ramal.		
13.	Ramais telefônicos da solução, com identificação do seu número, setor, local e data de instalação		
14.	Quantidade de chamadas realizadas e recebidas, atendidas, não atendidas, ocupadas, com falhas, congestionadas, por ramal e global e por data		
15.	Quantidade de chamadas realizada, por ramal, por perfil de tráfego (ramal-ramal, local, móvel, LDN), por consumo de minutagem e por data		
16.	Tráfego de dados, identificando a hora de cada dia com maior número de chamadas.		
17.	Evolução do consumo de minutagem, por perfil de tráfego, mês a mês, no mínimo dos últimos 06 (seis) meses.		