TERMO DE REFERÊNCIA

1. DIRETORIA REQUERENTE:

Departamento de Informática - Alcides Neto Feliciano Fernandes/Diretor.

2. DAS CONDIÇÕES GERAIS DA CONTRATAÇÃO

A licitação destina-se aquisição de solução de segurança para ambiente corporativo software antivírus e antimalware.

2.1 ESPECIFICAÇÕES DO OBJETO

2.2 Quantidade/Especificação dos Itens

Item	Qtde.	Unid.	Descrição do Objeto
01	**237**	Unid	Aquisição de Solução de Segurança para ambiente corporativo, baseado nas soluções de mercado com foco na monitoração e proteção da segurança tecnológica, conforme condições, quantidades, exigências e estimativas, estabelecidas na descrição detalhada, com console de administração, incluindo instalação. A Solução de Segurança ofertada deverá constar no Gartner na categoria Endpoint Protection Platforms ano 2025. Licenças de software antivírus e antimalware, conforme descrição detalhada. Período de licenciamento do software e suporte: 36 (trinta e seis) meses.
02	**100**	Unid	Aquisição de Solução de Segurança para ambiente corporativo, baseado nas soluções de mercado com foco na monitoração e proteção da segurança tecnológica, conforme condições, quantidades, exigências e estimativas, estabelecidas na descrição detalhada, com console de administração, incluindo instalação. A Solução de Segurança ofertada deverá constar no Gartner na categoria Endpoint Protection Platforms ano 2025. Licenças de software antivírus e antimalware, conforme descrição detalhada. Período de licenciamento do software e suporte: 36 (trinta e seis) meses. Quantidade estimada, utilização sob demanda.
03	**20**	Horas	Horas extras para suporte técnico adicional, on-site ou remoto, por hora/anual, visando à resolução de problemas com a solução, não cobertos pela garantia. Sob demanda.

2.3 O objeto desta contratação não se enquadra como sendo bem de luxo e possui natureza comum, sendo possível a utilização da modalidade pregão.

2.4 Licitação com a participação exclusiva de Microempresa e Empresa de Pequeno Porte (ME e EPP), conforme artigo 48, inciso I, da Lei Complementar nº 123, de 14 de dezembro de 2006, e artigo 6º do Decreto nº 8.538, de 06 de outubro de 2015.

2.5 Em caso de divergência entre as descrições e especificações constantes no CATMAT e no presente Termo de Referência, prevalece o descrito no Termo de Referência. Portanto, os licitantes deverão elaborar suas propostas com base na descrição constante no quadro acima.

3. ESTIMATIVA DO VALOR DA CONTRATAÇÃO:

3.1 O custo estimado da contratação possui caráter sigiloso e será tornado público apenas e imediatamente após o julgamento das propostas, uma vez que este procedimento tem sido positivo para a Câmara Municipal, com a redução dos preços das contratações, já que incentiva a competitividade entre os licitantes, evitando assim que os concorrentes limitem suas ofertas aos valores previamente cotados pelo Departamento de Licitações e Compras.

4 JUSTIFICATIVA

4.1 A aquisição das licenças de antivírus tem como objetivo prevenir a infecção ou invasão por vírus, malwares e suas variantes, ataques Cibernéticos de ransomware e ameaças avançadas nos computadores da Câmara Municipal de Uberlândia, o que pode colocar em risco a integridade e disponibilidade de informações necessárias aos trabalhos desenvolvidos nesta Casa de Leis.

4.2 O grande volume de utilização de e-mails e acesso a páginas de internet exige a disponibilidade de um software de antivírus, visando fornecer um mínimo de segurança à infraestrutura de rede de computadores da Câmara Municipal de Uberlândia.

4.3 Não obstante, a presente requisição se dá em função da proximidade da extinção do atual contrato n.º 030/2022, que se dará em 20 de outubro de 2025, que já atingiu o limite previsto no artigo 57, inciso II da Lei nº 8.666/1993, cujo ajuste será prorrogado por até 60 (sessenta) meses, nesse sentido a presente requisição visa manter a proteção dos computadores, resguardando problemas que podem prejudicar os trabalhos e a disponibilização de informações inerentes ao funcionamento da Câmara Municipal de Uberlândia.

4.4 Assim, a aquisição é considerada imprescindível para garantir a disponibilidade, integridade e confiabilidade dos dados e continuidade das atividades de todos os departamentos, seções e Gabinetes da Câmara.

4.5 O período da licença é de 3 anos a partir da instalação.

4.6 A instalação deverá correr de forma presencial ou remota sem requerer outro software ou agente adicional previamente instalado, sendo que um representante técnico da Contratada deverá estar presente na Câmara no momento da preparação do serviço de instalação e configuração do servidor que irá gerenciar a solução, que poderá ser local ou em nuvem (desde que a nuvem seja do fornecedor da solução).

4.7 A solução deverá ser entregue instalada, atualizada e configurada nos computadores da Câmara, cuja instalação será demandada de acordo com a necessidade.

4.8 A Contratada deverá realizar repasse de conhecimento da solução de segurança no ambiente da contratante, incluindo o momento da instalação.

4.9 Ainda deverá disponibilizar portal de serviços e atendimento telefônico 24x7x365, para registro e acompanhamento dos chamados de suporte técnico.

4.10 O suporte posterior a primeira instalação poderá ser na modalidade remota ou presencial, desde que, devidamente fundamentado, conforme a necessidade, seja autorizado pela Contratante

4.11 Em atendimento ao artigo 18, inciso II da Lei Federal 14.133/21, e, de acordo com o artigo n.º 45 da Portaria nº 205/2023, este Termo de Referência trata da aquisição de licenciamento do software antivírus corporativo para satisfazer a seguinte necessidade:

4.11.1 Manter a proteção adequada e atualizada do ambiente computacional (computadores e servidores da rede), de modo a preservar os ativos corporativos (hardware, software e dados), garantindo a integridade, confidencialidade e segurança das informações institucionais contra as ações de software mal intencionados que ponham em risco a segurança dos dados computacionais desta Casa de Leis.

5 DESCRIÇÃO DETALHADA

5.1 O preço é fixo e irreajustável para os itens 01 e 02.

5.2 MÓDULO DE PROTEÇÃO ANTI-MALWARE

5.2.1 Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

5.2.1.1 Windows Server 2016 e posteriores (32/64-bit);

5.2.1.2 Windows 7 e posteriores (x86/x64);

5.2.2 Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso. Para garantir que os casos de insucesso sejam monitorados para tomada de ações pontuais;

5.2.3 Deve ser integrada ao Windows Security Center, quando utilizado plataforma Microsoft;

5.2.4 Deve detectar, analisar e eliminar programas maliciosos, tais como Vírus, Malware, Worms, Cavalos de Troia (Trojans), Ransomware, Spyware,Adware, Rootkits, Phishing (com detecção de sites e e-mails maliciosos), Exploits e Ataques Zero-Day e Programas Potencialmente Indesejados (PUPs)

5.2.5 Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos;

5.2.6 Processos em execução em memória principal (RAM);

5.2.7 Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);

5.2.8 Arquivos compactados automaticamente, pelo menos, nos seguintes formatos: zip, exe, arj, mime/uu, Microsoft cab;

5.2.9 Arquivos recebidos por meio de programas de comunicação instantânea (telegram, whatsapp, skype, entre outros)

5.2.10 Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como Javascript, Vbscript/Activex;

5.2.11 Deve possuir detecção heurística de vírus desconhecidos;

5.2.12 Deve permitir diferentes configurações de detecção (varredura ou rastreamento):

5.2.12.1 Em tempo real de arquivos acessados pelo usuário;

5.2.12.2 Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;

5.2.12.3 Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;

5.2.12.4 Automáticos do sistema com as seguintes opções:

5.2.12.5 Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;

5.2.13 Ação: se uma correspondência for encontrada, o antivírus deve identificar o arquivo como malware e tomar a ação pré-definida, como quarentena, exclusão ou limpeza;

5.2.14 Frequência: horária, diária, semanal e mensal;

5.2.15 Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados;

5.2.16 Deve possuir mecanismo de cache de informações dos arquivos já escaneados;

5.2.17 Deve possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;

5.2.18 Deve possuir ferramenta de alterações de parâmetros de comunicação entre o cliente antivírus e o servidor de gerenciamento da solução de antivírus;

5.2.19 Deve permitir a utilização de servidores locais de reputação para análise de arquivos e URL's maliciosas, de modo a prover rápida detecção de novas ameaças;

5.2.20 Deve ser capaz de aferir a reputação das URL's acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-in ao navegador web, de forma a proteger o usuário independente da maneira de como a URL está sendo acessada;

5.2.21 Deve ser capaz de detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de quarentena a ameaça;

5.2.22 Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante;

5.2.23 Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança;

5.2.24 Deve permitir em conjunto com a restauração dos arquivos quarentenados a adição automática as listas de exclusão de modo a evitar novas detecções dos arquivos;

5.2.25 Deve fazer análise de processos com capacidade para detectar malware por comportamento.

5.2.26 Suporte ao Windows Server 2016.

5.2.27 A licença deve permitir a transferência, ou seja, deve ser possível desinstalá-la e desativá-la de um equipamento para posterior reatribuição a outro, desde que respeitados os procedimentos adequados;

5.3 FUNCIONALIDADE DE ATUALIZAÇÃO

5.3.1 O sistema deve permitir que o administrador agende atualizações automáticas das definições de vírus. Essas atualizações, com frequência mínima diária, podem ser baixadas de um local predefinido na rede ou de um site seguro na internet. O agendamento deve ser configurável através de Políticas de Grupo do Windows, diretivas PowerShell, WMI, ou ferramentas de gerenciamento centralizado, garantindo horários de atualização padronizados em todos os computadores da rede.

5.3.2 Deve permitir a atualização incremental da lista de definições de vírus;

5.3.3 Deve permitir a atualização automática da "engine" do programa de proteção a partir de localização da rede local ou da internet, a partir de fonte autenticável;

5.3.4 Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utiliza-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas;

5.3.5 Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento;

5.3.6 O servidor da solução de anti-malware, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os agentes replicadores de atualizações e configurações, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização;

5.3.7 O agente replicador de atualizações e configurações deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização.

5.4 FUNCIONALIDADE DE ADMISNITRAÇÃO

5.4.1 Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pelo console de administração da solução completa;

5.4.2 Deve possibilitar instalação "silenciosa";

5.4.3 Deve permitir o bloqueio por nome de arquivo;

5.4.4 Deve permitir o travamento de pastas e diretórios;

5.4.5 Deve permitir o rastreamento e bloqueio de infecções;

5.4.6 Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;

5.4.7 Deve efetuar a instalação remota nas estações de trabalho, sem requerer outro software ou agente adicional, previamente instalado e sem necessidade de reiniciar a estação de trabalho;

5.4.8 Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente;

5.4.9 Deve permitir a desinstalação através da console de gerenciamento da solução;

5.4.10 Identificar através da integração com o Active Directory, quais máquinas estão sem a solução de anti-malware instalada;

5.4.11 Deve permitir criação de diversos perfis e usuários para acesso a console de administração;

5.4.12 Deve permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

5.4.13 Deve possuir solução de consulta do hash dos arquivos integrada e gerenciada através da solução de antivírus, cancelando o download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante;

5.4.14 Deve permitir agrupamento automático de estações de trabalho e notebooks da console de gerenciamento baseando-se no escopo do Active Directory ou IP;

5.4.15 Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento;

5.4.16 Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos, integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

5.4.17 Deve registrar no sistema de monitoração de eventos da console de anti-malware informações relativas ao usuário logado no sistema operacional

5.4.18 Deve prover ao administrador relatório de conformidade do status dos componentes, serviços, configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento da console de antivírus;

5.4.19 Deve prover ao administrador informações sobre quais estações de trabalho e notebooks fazem parte do escopo de gerenciamento da console de anti-malware não realizaram o escaneamento agendado ou o escaneamento demandado pelo administrador no período determinado de dias;

5.4.20 Deve prover segurança através de SSL para as comunicações entre o servidor e a console de gerenciamento web;

5.4.21 Deve prover segurança através de SSL para as comunicações entre o servidor e os agentes de proteção;

5.4.22 Deve suportar múltiplas florestas e domínios confiáveis do Active Directory;

5.4.23 Deve utilizar de chave de criptografia que seja/esteja em conformidade com o Active Directory para realizar uma conexão segura entre servidor de antivírus e o controlador de domínio;

5.4.24 Deve permitir a criação de usuários locais de administração da console de anti-malware;

5.4.25 Deve possuir a integração com o Active Directory para utilização de seus usuários para administração da console de anti-malware;

5.4.26 Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes da console de gerenciamento;

5.4.27 Deve bloquear acessos indevidos a área de administração do agente que não estejam na tabela de políticas definidas pelo administrador;

5.4.28 Deve se utilizar de mecanismo de autenticação da comunicação entre o servidor de administração e os agentes de proteção distribuídos nas estações de trabalho e notebooks;

5.4.29 Deve permitir a gerência de domínios separados para usuários previamente definidos;

5.4.30 Deve ser capaz de enviar notificações específicas aos respectivos administradores de cada domínio definido no console de administração;

5.4.31 Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto.

5.5 FUNCIONALIDADE DE CONTROLE DE DISPOSITIVOS

5.5.1 Deve possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total;

5.5.2 Deve possuir o controle de acesso a drives de mídias de armazenamento como CDROM, DVD, com as opções de acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

5.5.3 Deve possuir o controle a drives mapeados com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

5.5.4 Deve permitir escaneamento dos dispositivos removíveis e periféricos (USB, disquete, CDROM) mesmo com a política de bloqueio total ativa.

5.6 MÓDULO DE PROTEÇAO ROTEAÇÃO (anti-malware para estações Linux caso a solução ofereça módulo separado por S.O.)

5.6.1 Varredura manual com interface gráfica, personalizável, com opção de limpeza dos malwares encontrados;

5.6.2 Varredura manual por linha de comando, parametrizável e com opção de limpeza automática em todos os sistemas operacionais;

5.6.3 Capacidade de detecção e remoção de todos os tipos de malware, incluindo spyware, adware, grayware, cavalos de tróia, rootkits, e outros;

5.6.4 Detecção e remoção de códigos maliciosos de macro do pacote Microsoft office, em tempo real;

5.6.5 O cliente da solução deve armazenar localmente, e enviar para o servidor (para fins de armazenamento) logs de ocorrência de ameaças, contendo no mínimo os seguintes dados: nome da ameaça, caminho do arquivo comprometido (quando disponível), data e hora da detecção, endereço ip do cliente e ação realizada;

5.6.6 A desinstalação do cliente nas estações de trabalho deverá ser completa, removendo arquivos, entradas de registro e configurações, logs diversos, serviços do sistema operacional e quaisquer outros mecanismos instalados;

5.6.7 Possibilidade de rastrear ameaças em arquivos compactados em, no mínimo, 15 níveis recursivos de compactação;

5.6.8 As mensagens exibidas aos usuários devem ser traduzidas para o português do Brasil;

5.7 FUNCIONALIDADE DE HIPS – Host IPS e Host Firewall

5.7.1 Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

5.7.2 Windows Server 2016 e posteriores (32/64-bit);

5.7.3 Windows 7 e posteriores (x86/x64);

5.7.4 Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host ips e host firewall;

5.7.5 Todas as regras das funcionalidades de firewall e ips de host devem permitir apenas detecção (log) ou prevenção (bloqueio);

5.7.6 Deve permitir ativar e desativar o produto sem a necessidade de remoção;

5.7.7 Deve permitir a varredura de portas lógicas do sistema operacional para identificar quais estejam abertas e possibilitando trafego de entrada ou saída;

5.7.8 A funcionalidade de host ips deve possuir regras para controle do tráfego de pacotes de determinadas aplicações;

5.7.9 Deve efetuar varredura de segurança automática ou sob demanda que aponte vulnerabilidades de sistemas operacionais e aplicações e atribua automaticamente as regras de host ips para proteger a estação de trabalho ou notebook contra a possível exploração da vulnerabilidade;

5.7.10 A varredura de segurança deve ser capaz de identificar as regras de host ips que não são mais necessárias e desativá-las automaticamente;

5.7.11 Deve prover proteção contra as vulnerabilidades de aplicações terceiras, por meio de regras de host ips, tais como Oracle Java, Abobe PDF Reader, Microsoft Office, Apple Itunes, Apple Quick Time, Apple Safari, Google Chrome, Mozilla Firefox, Opera Browser, MS Internet Explorer, entre outras;

5.7.12 Deve permitir a criação de políticas diferenciadas em múltiplas placas de rede no mesmo sistema operacional;

5.7.13 Deve permitir a criação de políticas de segurança personalizadas;

5.7.14 Deve permitir a emissão de alertas via smtp e snmp;

5.7.15 Deve permitir configuração e manipulação de políticas de firewall através de prioridades;

5.7.16 Deve permitir criação de regras de firewall utilizando os seguintes protocolos:

5.7.17 Icmp, icmpv6, igmp, ggp, tcp, pup, udp, idp, nd, raw, tcp+udp.

5.7.18 Deve permitir criação de regras de firewall por origem de ip ou Mac ou porta e destino de ip ou mac ou porta;

5.7.19 Deve permitir a criação de regras de firewall pelos seguintes frametypes:Ip, ipv4, ipv6, arp, revarp.

5.7.20 Deve permitir a criação de grupos lógicos através de lista de ip, Mac ou portas;

5.7.21 Deve permitir a criação de contextos para a aplicação para criação de regras de firewall;

5.7.22 Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar a visualização e gerenciamentos.

5.8 INSTALAÇÃO E CONFIGURAÇÃO

5.8.1 A solução deverá ser entregue instalada, atualizada e configurada nos computadores da Câmara Municipal de Uberlândia, sendo 250 instalações imediatas e outras 100 sob demanda para computadores que forem adquiridos posteriormente.

5.8.2 A instalação deverá ocorrer, preferencialmente, de forma remota, podendo ser utilizado console de gerenciamento centralizada (local ou em nuvem) que permita implantar o agente remotamente em múltiplos dispositivos, ou ainda:

5.8.3 Utilizando políticas de grupo do Windows para distribuir o instalador para máquinas da rede GPO (Group Policy Objects);

5.8.4 Instalação automatizada via scripts - scripts de linha de comando.

5.8.5 Caso não seja possível a instalação de forma remota, a CONTRATADA deverá proceder com as instalações nos locais físicos. Nesses casos, será responsabilidade da CONTRATADA fornecer transporte e mão de obra para instalação do software, sem ônus para a CONTRATANTE;

5.8.6 A caso a solução vencedora não seja a atualmente utilizada pela Câmara Municipal de Uberlândia, a Contratada deverá viabilizar a sua remoção, o que poderá se dar por meio de recurso disponível na nova solução ou ainda por meio do serviço de instalação contratado;

5.8.7 A CONTRATADA deverá ter capacidade de realizar no mínimo 60 (sessenta) instalações por dia;

5.8.8 A CONTRATANTE irá fornecer o hardware e software (Sistema Operacional) para instalação do servidor que irá gerenciar a solução, será responsabilidade da CONTRATADA fornecer, instalar e configurar o software de gerência;

5.8.9 A CONTRATADA deverá instalar e configurar o software de gerência em até 5 (cinco) dias.

5.9 PÓS-INSTALAÇÃO E GERENCIAMENTO

5.9.1 A CONTRATADA deverá configurar as políticas de segurança, de verificação, de detecção de ameaças, de firewall e de controle de aplicativos, a serem definidas e aplicadas centralmente na console de gerenciamento;

5.9.2 A CONTRATADA deverá avaliar o status dos end-points na console para verificar a saúde do agente, detectar ameaças e gerenciar incidentes, estabelecendo as políticas de tratamento em cada caso.

5.9.3 A CONTRATADA deverá otimizar a solução para que a varredura em tempo real e outras atividades de varredura, não impactem no desempenho dos sistemas e nem comprometam a segurança;

5.9.4 A CONTRATADA deverá configurar as atualizações automáticas das definições de vírus, módulos de software e patches de segurança;

5.9.5 A CONTRATADA deverá avaliar a necessidade de integração da solução end-point com outras ferramentas de segurança (SIEM, EDR), visando uma solução completa da postura de segurança;

5.10 REPASSE DE CONHECIMENTO

5.10.1 A CONTRATADA deverá realizar repasse de conhecimento da solução de segurança no ambiente da CONTRATANTE;

5.10.2 A transferência de tecnologia deverá capacitar até 4 (quatro) técnicos da CONTRATANTE, os quais deverão obter conhecimentos para operar, configurar, administrar e resolver problemas usuais na solução ofertada.

5.11 SUPORTE TÉCNICO ADICIONAL SOB DEMANDA

5.11.1 A CONTRATADA deverá disponibilizar Portal de Serviços e Atendimento Telefônico 24x7x365, para registro e acompanhamento dos chamados de suporte técnico.

5.11.2 A CONTRATADA deverá disponibilizar suporte na modalidade 24x7x365, com atendimento presencial;

5.11.3 O prazo de início de atendimento para os chamados de suporte técnico não poderá exceder 120 (cento e vinte) minutos, a contar da abertura do chamado, incluindo deslocamento de técnicos e/ou mão de obra para atendimento no site da CONTRATANTE;

5.11.4 A CONTRATADA deverá considerar 60 (sessenta) horas (20 h/a) para prestação de serviço de suporte na sede da CONTRATANTE durante o período de 36 (trinta e seis) meses, sempre que for acionada. Quantidade: Sob Demanda.

5.11.5 A substituição de servidores antigos por novos, não implicar no pagamento de novos serviços.

6 DOS REQUISITOS DA CONTRATAÇÃO

6.1 Para a adequada solução das necessidades administrativas pontuadas preliminarmente, a contratação/aquisição pretendida deverá atender os seguintes requisitos mínimos:

6.1.1 Padrões mínimos de qualidade: proteger o ambiente computacional da Câmara Municipal de Uberlândia (computadores e servidores da rede), de modo a preservar os ativos corporativos (hardware, software e dados), garantindo a integridade, confidencialidade e segurança das informações institucionais contra as ações de software mal intencionados que ponham em risco à segurança dos dados.

6.1.2 A versão da solução deverá ser a mais atual disponível no mercado brasileiro para a aplicação;

6.1.3 Prazo e Local da entrega (plano de logística): 10 dias;

6.1.4 Expectativa de funcionamento: garantir a integridade, confidencialidade e segurança das informações institucionais contra as ações de software mal intencionados que ponham em risco a segurança dos dados;

6.1.5 Não é admitida a subcontratação do objeto contratual;

6.1.6 Não haverá exigência da garantia da contratação dos artigos 96 e seguintes da Lei nº 14.133, de 2021;

6.1.7 Não há necessidade de realização de avaliação prévia do local de execução dos serviços.

7 DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

7.1 O presente Termo de Referência, como já informado, refere-se à aquisição dos objetos relacionados, descritos tecnicamente, destinados a proteger o ambiente computacional da Câmara Municipal de Uberlândia (computadores e servidores da rede), de modo a preservar os ativos corporativos (hardware, software e dados), garantindo a integridade, confidencialidade e segurança das informações institucionais contra as ações de software mal intencionados que ponham em risco a segurança dos dados, contemplando a solução como um todo.

8 JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

8.1 Não há possibilidade de parcelamento, ante a interdependência dos objetos, que formam o conjunto de produto/serviços a serem contratados. A licitação é composta de grupo único segundo as informações constantes neste Termo de Referência, devendo o licitante oferecer proposta para todos os itens que compõe o Grupo.

8.2 O grupo único abarcou todos os elementos necessários, aos objetos, destinados a prover a solução de segurança do ambiente computacional do Órgão Contratante.

8.3 Considerando a dependência entre os itens que compõem o objeto desta contratação, comprovou-se técnico e economicamente inviável o seu parcelamento, visto que, a divisão do objeto pode comprometer o cumprimento dos requisitos técnicos apresentados neste artefato. A contratação do objeto da licitação em menor preço global do grupo único, garante a unicidade técnica da solução e da prestação do serviço, permitindo que a empresa contratada, esteja capacitada tecnicamente para entregar de forma integrada com os componentes desta solução. Tal necessidade é melhor compreendida quando descrevemos, de forma exemplificativa, as etapas dos serviços que a licitante vencedora deverá executar.

8.4 Conforme Acórdão nº 861/2013 - Plenário - É lícito o agrupamento em grupos de itens a serem adquiridos por meio de pregão, desde que possuam a mesma natureza e guardem relação entre si; segundo o Acórdão nº 5260/2011 - TCU - 1ª Câmara, de 06/07/2011: "Inexiste ilegalidade na realização do pregão com previsão de adjudicação por grupos, e não por itens, desde que os grupos sejam integrados por itens de uma mesma natureza e guardem correlação entre si".

9 DOS RESULTADOS PRETENDIDOS

9.1 Sem prejuízo dos elementos e requisitos indispensáveis da aquisição dos itens já expostos, pretende-se a continuidade dos serviços públicos, exigindo-se do(s) fornecedor(es) contratado(s) o atendimento dos requisitos básicos de economicidade, eficácia, eficiência e melhor aproveitamento dos recursos financeiros e materiais da administração Pública.

10 PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO

10.1 A presente contratação requer por parte da administração pública o acompanhamento de profissional qualificado para analisar, julgar, receber a solução e os serviços solicitados, de forma a verificar que todas as especificações técnicas e exigências solicitadas foram cumpridas.

10.2 CONTRATAÇÕES CORRELATAS OU INTERDEPENDENTES

10.3 Diante do levantamento das necessidades da contratação, acompanhada dos demais elementos que consolidam o presente Termo de Referência, analisando a solução como um todo e o ciclo de vida do objeto, não se faz necessária demais contratações correlata/interdependentes para a viabilidade da contratação pretendida.

11 POSSÍVEIS IMPACTOS AMBIENTAIS

11.1 Com o objetivo de atender a preceitos legais e constitucionais que exige do Poder Público, a partir de competência concorrente entre a União, Estados, Municípios e Distrito Federal a proteção, manutenção e preservação do meio ambiente, com o combate à poluição

em qualquer de suas formas, a presente contratação deve manter critérios de sustentabilidade nas aquisições e contratações, sendo dever do contratado a atuação na execução e prestação de serviços públicos de acordo com boas práticas de sustentabilidade.

11.2 No entanto, apesar do dever intrínseco imposto aos fornecedores de serviços, bens e produtos à Administração Pública, a presente contratação não vislumbra possíveis impactos ambientais.

12 VISTORIA

12.1 Não se aplica a vistoria, uma vez que se trata de prestação de serviço não suscetível à vistoria.

12.2 Não será admitida a subcontratação total ou parcial do objeto.

13 EXECUÇÃO DO OBJETO

13.1 Início da execução dos objetos se dará em REMESSA ÚNICA, com prazo não superior a 10 (dez) dias úteis após recebimento da Nota de Empenho pelo fornecedor.

13.2 A entrega das licenças será feita em etapa única, ficando a Contratada posteriormente à disposição apenas para eventuais suportes técnicos relacionados ao uso e configurações da solução disponibilizada durante todo o período de vigência da licença contratada.

13.3 A solução/serviço deverá ser entregue e instalada no Departamento TI na Câmara Municipal de Uberlândia – Av. João Naves de Ávila n° 1617, CEP: 38408-144, B: Santa Mônica, no horário das 08:00h ao 12:00h, e das 14:00h às 17:00h no Seção de Almoxarifado, telefone: (34) 3239-1134.

13.4 A instalação e configuração nos servidores de rede deverá ser feita no Departamento de Informática e nos demais equipamentos, deverá ser feita pela empresa vencedora de forma remota. Deverá ser disponibilizado arquivo e/ou link de instalação para utilização posterior.

13.5 O gestor, Departamento de TI, rejeitará, no todo ou em parte, o fornecimento executado em desacordo com os termos do Termo de Referência.

13.6 Caso não seja possível a entrega no prazo máximo, a empresa deverá apresentar justificativa plausível com pelo menos 2 (dois) dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

13.7 O não cumprimento do disposto no objeto do presente termo, acarretará a aplicação de penalidades previstas no edital e a convocação do fornecedor subsequente, considerando a ordem de classificação do certame.

14 GARANTIA

14.1 O prazo de garantia contratual dos serviços, complementar à garantia legal, será de, no mínimo, 36 (trinta e seis) meses, contados a partir do primeiro dia útil subsequente à data da ativação definitiva das licenças.

14.2 GESTÃO DO CONTRATO

14.3 O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

14.4 Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

14.5 A Contratante e a Contratada devem realizar registro por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

14.6 A Câmara poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

14.7 Após a assinatura do contrato ou instrumento equivalente, o Departamento de Informática poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da Contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

14.8 A execução do contrato deverá ser acompanhada e fiscalizada pelo fiscal do contrato. (art. 117, caput da Lei 14.133, de 2021)

14.9 Cabe ao fiscal do contrato:

14.9.1 Acompanhar a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Câmara Municipal.

14.9.2 Anotar no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133 de 2021, art. 117, §1º)

14.9.3 Identificar qualquer inexatidão ou irregularidade e emitir notificação para a correção da execução do contrato, determinando prazo para a correção.

14.9.4 Informar ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.

14.9.5 Comunicar ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade.

14.9.6 Acompanhar a manutenção das condições de habilitação da Contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário.

14.9.7 Caso ocorra descumprimento das obrigações contratuais, o fiscal do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência.

14.10 Cabe ao gestor do contrato:

14.10.1 Coordenar e atualizar o processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações

contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.

14.10.2 Acompanhar a manutenção das condições de habilitação da Contratada, para fins de empenho de despesa e pagamento, e anotar os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.

14.10.3 Acompanhar os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.

14.10.4 Tomar providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela Comissão de que trata o art. 158 da Lei nº 14.133 de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso.

15 CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

15.1 Do recebimento:

15.1.1 Os bens serão recebidos provisoriamente, de forma sumária, no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável ao acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

15.1.2 Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 05 (cinco) dias úteis, a contar da notificação da Contratada, às suas custas, sem prejuízo da aplicação das penalidades.

15.1.3 O recebimento definitivo ocorrerá no prazo de 05 (dias) dias úteis, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do objeto e consequente aceitação mediante termo detalhado.

15.1.4 O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

15.1.5 O prazo para a solução pelo Contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Câmara durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

15.1.6 O não cumprimento do disposto nos subitens 7.3, 7.5, 9.1.2, 9.2.3, 9.2.9, acarretará a aplicação de penalidades previstas no edital e a convocação do fornecedor subsequente considerando a ordem de classificação do certame.

15.2 Da forma de pagamento:

15.2.1 O pagamento será efetuado ao Contratado em até 5 dias após a liquidação da Nota Fiscal.

15.2.2 Para fins do devido pagamento a Contratada deverá fazer juntada à Nota Fiscal, prova de cumprimento da regularidade fiscal e trabalhista, com a apresentação das certidões negativas exigidas no Edital na fase da Habilitação, devidamente atualizadas.

15.2.3 Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à Contratação, ou ainda, circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a Contratada providencie a regularização. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

15.2.4 O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

15.2.5 Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

15.2.6 Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

15.2.7 Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

15.2.8 O Contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

15.2.9 Constatando-se, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do contratante.

15.2.10 Persistindo a irregularidade, o Contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao Contratado a ampla defesa.

16 FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

16.1 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 POR GRUPO.**

16.2 HABILITAÇÃO

16.2.1 Para fins de habilitação, deverá o licitante comprovar os requisitos descritos nos itens abaixo.

Declarações: Declarar em campo próprio do sistema compras.gov:

16.2.2 Declaração de idoneidade e ausência de fato impeditivo para licitar com o poder público.

16.2.3 Declaração atestando que não utiliza mão de obra direta ou indireta de menores (conforme Art. 7º, inciso XXXIII, da Constituição Federal).

16.2.4 Declaração de estar ciente que se enquadra em um dos dois regimes, na forma do disposto da Lei Complementar n° 123, de 14/12/2006.

16.3 Habilitação Jurídica:

16.3.1 Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

16.3.2 Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br;

16.3.3 Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

16.3.4 Sociedade empresária estrangeira com atuação permanente no País: decreto de autorização para funcionamento no Brasil;

16.3.5 Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores.

16.3.6 Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

16.4 Habilitações fiscal, social e trabalhista:

16.4.1 Prova de inscrição no Cadastro Nacional da Pessoa Jurídica (CNPJ);

16.4.2 Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de Certidão Negativa de Débitos relativos a Créditos Tributários Federais e à Dívida Ativa da União (CND);

16.4.3 Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

16.4.4 Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de Certidão Negativa de Débitos Trabalhistas (CNDT);

16.4.5 Prova de regularidade com as Fazendas Estadual, Distrital e Municipal do domicílio ou sede do contratado;

16.4.6 Prova de regularidade fiscal para com a Fazenda Municipal de Uberlândia para todos licitantes - domiciliados em Uberlândia ou não, fornecido pelo site da Prefeitura de Uberlândia, em que conste o CNPJ da licitante com a devida informação de que não está cadastrada (cadastro inexistente) ou não possui débitos. Os licitantes com cadastro inexistente no município de Uberlândia, deverá ser apresentada a impressão da tela do sítio da Prefeitura com a devida informação.

16.5 Qualificação técnico-profissional e técnico-operacional:

16.5.1 Apresentação do atestado de capacidade técnica fornecido por pessoa jurídica de direito público ou privado, o qual comprove que a licitante forneceu ou está fornecendo, de forma satisfatória e sem restrições, produto pertinente e compatível com o objeto do Termo de Referência.

16.6 Habilitação econômico-financeira:

16.6.1 Apresentar a Cópia da Certidão Negativa de Falência ou Concordata expedida pelo distribuidor da sede da pessoa jurídica, com validade na data de abertura da licitação.

16.7 PARA ACETAÇÃO DA PROPOSTA será consultado especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

16.7.1 Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/ceis);

16.7.2 Cadastro de fornecedores Impedidos de Licitar e Contratar com o município de Uberlândia - CADUDI.

16.7.3 Sistema de Cadastro Unificado de Fornecedores- SICAF - Relatório de Ocorrências Impeditivas de Licitar.

17 ADEQUAÇÃO ORÇAMENTÁRIA: As despesas decorrentes da presente contratação, correrão à conta da dotação: 01.122.7005.2258 - Manutenção dos Serviços Administrativos - Ficha 27604 – 3.3.90.40.00 - Serviços de T.I. e Comunicação - Pessoa Jurídica - 04 - Manutenção de Software.

Uberlândia, 23 de julho de 2025.

ALCIDES NETO FELICIANO FERNANDES

DIRETOR DO DEPARTAMENTO DE INFORMÁTICA