



INSTITUTO DE PREVIDÊNCIA SOCIAL DOS SERVIDORES DE CAJAMAR  
ESTADO DE SÃO PAULO

|          |                     |
|----------|---------------------|
| Matr. nº | 217                 |
| PROG. nº | 35/25               |
| Rubrica  | <i>[assinatura]</i> |

**AVISO DE DISPENSA DE LICITAÇÃO**  
(art. 75, II da Lei 14.133/2021)

INSTITUTO DE PREVIDÊNCIA SOCIAL DOS SERVIDORES DE CAJAMAR ESTADO DE SÃO PAULO - CNPJ: 02.675.642/0001-16; torna público que pretende adquirir ou contratar o objeto abaixo discriminado e tem interesse em obter propostas adicionais de eventuais interessados.

Os interessados deverão apresentar proposta até o horário indicado abaixo através de formulário de proposta (Anexo II) a ser endereçado para o e-mail: [fernando@ipssc.sp.gov.br](mailto:fernando@ipssc.sp.gov.br).

**1. OBJETO:**

1.1. Contratação de empresa especializada para prestação de serviços de locação de firewall com gerenciamento unificado de ameaças de última geração para proteção de perímetro de rede, contemplando o hardware, software de gerenciamento, licenciamento, instalação, configuração, treinamento e atualizações, nas dependências do Instituto de Previdência Social dos Servidores de Cajamar - IPSSC, conforme condições, quantidades estimadas e exigências estabelecidas neste instrumento.

**2. DATA PARA APRESENTAÇÃO DA PROPOSTA:**

2.1. Data início para apresentação de novas propostas: 19/08/2025 às 09:00

2.1. Data limite para apresentação de novas propostas: 22/08/2025 às 09:00

**3. PROPOSTA**

3.1. O fornecedor interessado deverá encaminhar sua proposta devidamente em papel timbrado da empresa e assinada pelo representante legal, mediante documento que comprove a representação.

**4. DOCUMENTOS DE HABILITAÇÃO:**

4.1. Para fins de contratação, o fornecedor que apresentar o menor preço será convocado por e-mail para que no prazo de 24 (vinte e quatro) horas, apresente os seguintes documentos, sob pena de decair do direito de contratar:

I - Contrato social, requerimento de empresário individual, Estatuto Social, ou outro documento apto a comprovar a existência jurídica da proponente;

II - Inscrição no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Nacional da Pessoa Jurídica (CNPJ);

III - Prova de regularidade perante a Fazenda Municipal (mobiliários);

IV - Prova de regularidade relativa à Seguridade Social e ao FGTS, que demonstre cumprimento dos encargos sociais instituídos por lei;

V - Certidão Negativa do Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e o Cadastro Nacional de Empresas Punidas (Cnep); (link: <https://certidoes.cgu.gov.br/>);

VI - Prova de regularidade perante a Justiça do Trabalho;

VII – Prova de regularidade com as Fazendas Federal e Estadual (inscritos em dívida ativa);

VIII – Falência e recuperação judicial (vide Súmula 50 do TCESP) e

IX - Prova de registro ou inscrição na entidade profissional competente, quando for caso.



|          |                     |
|----------|---------------------|
| Folha nº | 218                 |
| Proc nº  | 3525                |
| Rubrica  | <i>[assinatura]</i> |

## 5. CONTRATAÇÃO

5.1. Caso se conclua pela contratação e após a autorização da autoridade competente, será firmado Termo de Contrato ou emitido instrumento equivalente. O fornecedor vencedor da melhor proposta terá o prazo de 24 (vinte e quatro) horas para assinar o Termo de Contrato ou aceitar instrumento equivalente (nota de empenho ou autorização de fornecimento), sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste aviso.

5.2. O aceite da nota de empenho ou autorização de fornecimento, emitida ao fornecedor, implica no reconhecimento de que referido documento está substituindo o contrato, o contratado se vincula à sua proposta às previsões contidas no Aviso de Contratação e anexos e o contratado reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 137 a 138 da Lei 14.133/21 e reconhece os direitos da Administração previstos nos artigos 137 e 139 da mesma lei.

5.3. As condições de habilitação deverão ser mantidas pelo fornecedor durante a vigência do contrato, inclusive para fins de pagamento.

5.4. As penalidades administrativas são aquelas previstas na Lei Federal nº 14.133, de 2021, concomitantemente com as disposições do Decreto Municipal nº 7.144, de 2024.

## 6. DISPOSIÇÕES GERAIS:

6.1. A apresentação da proposta implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, Anexo I.

6.2. Uma vez enviada a proposta por e-mail, o fornecedor NÃO poderá substituí-la, podendo, contudo, solicitar o seu cancelamento através de mensagem para o mesmo e-mail da proposta desde que devidamente justificado.

6.3. A apresentação de propostas adicionais não implica na necessidade de a Administração adquirir ou contratar do fornecedor proponente podendo, se for o caso, contratar fornecedor que eventualmente tenha apresentado proposta de melhor preço por ocasião da realização da pesquisa de preços.

6.4. Caberá ao fornecedor acompanhar as operações, ficando responsável pelo ônus decorrente da perda do negócio diante da inobservância de quaisquer mensagens emitidas pela Administração ou de sua desconexão.

Cajamar, 18 de agosto de 2025

*[assinatura]*  
**Diretor Executivo**



TERMO DE REFERÊNCIA

**PROCESSO ADMINISTRATIVO Nº 35/2025**  
**DOCUMENTO DE FORMALIZAÇÃO DE DEMANDA (DFD) Nº 11/2025**

Sigilo: ( ) SIM ( X ) NÃO

Previsão no Plano de Contratação Anual: ( X )SIM ( ) NAO

**1. OBJETO**

- 1.1. Contratação de empresa especializada para prestação de serviços de locação de firewall com gerenciamento unificado de ameaças de última geração para proteção de perímetro de rede, contemplando o hardware, software de gerenciamento, licenciamento, instalação, configuração, treinamento e atualizações, nas dependências do Instituto de Previdência Social dos Servidores de Cajamar - IPSSC, conforme condições, quantidades estimadas e exigências estabelecidas neste instrumento.

| Item         | Descrição   | Unidade de Medida | Quantidade/Mês | Valor Mensal Estimado | Valor Total Estimado | Porcentagem |
|--------------|---|-------------------|----------------|-----------------------|----------------------|-------------|
| 1            | Locação de Firewall UTM NGFW  | SV                | 12 meses       | R\$ 4.368,53          | R\$ 52.422,36        | 87,55%      |
| 2            | Locação de switch gerenciável Layer 3 com múltiplas interfaces de alta velocidade | SV                | 12 meses       | R\$ 269,06            | R\$ 3.228,66         | 5,39%       |
| 3            | Instalação e configuração de Firewall UTM NGFW                                    | SV                | 01 serviço     | R\$ 1.909,42          | R\$ 1.909,42         | 3,19%       |
| 4            | Visita Técnica  | SV                | 12 visitas     | R\$ 192,42            | R\$ 2.314,45         | 3,87%       |
| <b>TOTAL</b> |   |                   |                |                       | <b>R\$ 59.874,90</b> | <b>100%</b> |

**2. Da Vedação da Aquisição de Bens de Consumo de Luxo**

- 2.1. Em consonância com o artigo 20 da Lei 14.133/2021 e artigo 25 do Decreto Municipal 7.139/2021 trata-se de contratação de serviço comum, sendo indispensável para a segurança da informação e vazamento de dados deste IPSSC.

**3. Descrição do Objeto:**

**3.1. Solução Firewall Next Generation**

- 3.1.1. A solução de segurança de redes, também chamado de Firewall UTM ou Firewall NG, deverá permitir acesso as informações do produto, em idioma Português (Brasil), não somente através de um acesso direto ao equipamento e ao seu painel, como também acesso à um servidor em Cloud (nuvem). Permitindo assim ser acessado de qualquer lugar, sem restrições de origem, através de login e senha com possibilidade de possuir dupla autenticação a fim de aumentar o nível de segurança de acesso.
- 3.1.2. O painel em Cloud (nuvem), deve permitir visualizar informações essenciais dos produtos em tempo real, a fim de monitoramento, tais como informações do hardware, processamento, memória, disco, informações de qualidade do link, disponibilidade, latência e perda de pacotes.
- 3.1.3. O servidor em nuvem, deverá efetuar backup das configurações dos produtos, no mínimo diariamente, a fim de aumentar a segurança em caso de algum incidente que afete as configurações ou o hardware.



- 3.1.4. O servidor em nuvem, deverá avaliar o nível de risco do produto, no que se refere as melhores práticas de configuração de segurança de redes, sendo analisado pelo menos as regras de firewall, regras de NAT, qualidade da senha de acesso, configurações de VPN, entre outros. Tal análise tem que ser no mínimo diária.
- 3.1.5. Deverá possuir aprendizado de máquina (Machine Learning) trabalhando na prevenção de ataques em todas as camadas segundo o modelo OSI, referenciando arquivos.
- 3.1.6. Estabelecer comunicação contínua com mecanismos em nuvem para receber atualizações de informações de maneira contínua, visando aperfeiçoamento e reciclagem de conteúdo.
- 3.1.7. Possuir recurso para recomendação de boas práticas relacionadas a controle, gestão e segurança através de alertas, gráficos e análise de risco. Existir ainda a possibilidade de configurar as recomendações para reduzir as chances de falhas humanas, automatizando alertas.
- 3.1.8. Em caso de impossibilidade de configuração via interface gráfica, devido à algum incidente, a solução deverá permitir também o acesso via console de linha de comando, podendo ser acessível através de protocolo de acesso remoto. Tal como: SSH ou conexão direta via cabo console. As configurações mínimas permitidas por meio de linha de comando deverá ser:
  - 3.1.9. Configuração de interface de rede, configuração de senha de acesso à WEB, "resetar" equipamento para a configuração "padrão de fábrica", reiniciar o sistema, parar o sistema, acesso ao sistema operacional, lista das atividades do firewall, visualizar filtro do firewall, reiniciar o serviço de acesso à WEB, acessar o sistema operacional como "desenvolver", à fim de reparação de algum bug. Atualização do sistema, habilitar acesso via SSH, efetuar download de módulos, pacotes ou atualizações, logout e ping.
  - 3.1.10. Com objetivo de ter uma instalação fácil, prática e rápida. A solução deverá permitir a utilização de um auxiliador de configuração (wizard) nos casos de primeira instalação do sistema.
  - 3.1.11. A solução deverá suportar uso de VLANs 802.1Q.
  - 3.1.12. A solução deverá suportar regras de Firewall tradicionais, permitindo filtrar por: origem e IP de destino, porta de origem do protocolo, e destino IP para o tráfego TCP e UDP, com limite de conexões simultâneas por regra, com possibilidade de alteração do gateway para cada regra, podendo fazer balanceamento de carga ou failover por regra. As regras de Firewall devem permitir também gestão da tabela de estado das conexões.
  - 3.1.13. A solução deverá permitir efetuar regras de Firewall por Objetos. Por objetos considerasse um IP, Porta, URL, sub-redes, entre outros.
  - 3.1.14. A solução deverá fazer bloqueios na camada de aplicação (considerando camada 7 no modelo de camadas OSI de comunicação), também chamado de Firewall por aplicação permitindo assim:
    - 3.1.15. Reconhecer aplicações independente de porta e protocolo, tendo a capacidade de bloquear e liberar aplicações diretamente através de configuração por meio da interface gráfica com poucos cliques, podendo configurar regras por grupo e usuário.
    - 3.1.16. Efetuar regras por usuário ou grupo através de integração com Microsoft Active Directory ou base local.
    - 3.1.17. A solução deverá reconhecer pelo menos aplicações nas seguintes categorias: redes sociais, ameaças, pornografia, antivírus, portais.
    - 3.1.18. A solução deve mostrar por meio de um painel o percentual do tráfego de cada rede social, tais como: facebook, twitter, instagram, whatsapp, linkedin, youtube e as aplicações que estão sendo utilizadas no momento, com informações sobre a aplicação, data e hora, nome de usuário que está originando o tráfego e se o tráfego está liberado ou bloqueado.
    - 3.1.19. A solução deverá prover relatório de acesso do uso das aplicações.



- 3.1.20. A solução deverá possuir proteção contra tráfego malicioso, ataques, independente de porta e protocolo, ou seja, proteção na camada 7 (camada de aplicação segundo modelo OSI), permitindo visualizar em um dashboard de maneira gráfica e georreferenciada de acordo com a origem dos ataques.
- 3.1.21. A proteção na camada 7 contra tráfego malicioso, deverá garantir bloqueio de no mínimo worms, trojans, malwares, além de protocolos de uso não recomendados como: UltraSurf, UltraVPN, CyberGhost, Express VPN etc.
- 3.1.22. Deverá ainda ter proteção em tempo real de forma distinta da proteção na camada de aplicação.
- 3.1.23. Uma vez que seja uma ferramenta de proteção de borda nativamente na interface WAN, deverá englobar todas as ferramentas de proteção como antivírus, antiphishing, antispymware, antiransomware e IDS/IPS.
- 3.1.24. Deve possuir dashboard exclusivo com gráficos de informações dos principais países de origem das tentativas de invasões.
- 3.1.25. Ter recurso para exibir um resumo das tentativas de invasão, infecções identificadas e nível de risco de cada uma delas.
- 3.1.26. Deverá possuir proteção integrada de IPs com assinaturas mantidas também pelo fabricante.
- 3.1.27. Deverá ter disponível uma ferramenta responsável por identificar e bloquear aplicações ou serviços independente de uso de um Proxy nos dispositivos. Com capacidade de bloquear até mesmo tráfego de dispositivos móveis.
- 3.1.28. Oferecer opção de separação de gráficos e as porcentagens de acesso por rede/interface.
- 3.1.29. Exibir consumo por aplicações e detalhes de pelo menos as 5 principais aplicações que mais consomem banda da internet.
- 3.1.30. As informações de navegação devem ser em tempo real, com a possibilidade de separar interface/rede.
- 3.1.31. Deverá ter gráfico com porcentagem de navegação separado por categoria.
- 3.1.32. Deverá possuir a seleção total ou parcial de bloqueios ou liberações de aplicativos ou websites.
- 3.1.33. A solução deve possuir a possibilidade de uso de regras separadas por redes (book de regras), e ainda ser possível configurar políticas de navegação distintas entre as redes.
- 3.1.34. Deve ainda possuir um modo simplificado de uso do recurso agindo na camada de aplicação, para uso em equipamentos com hardware com carga alta de consumo.
- 3.1.35. Deve possuir recurso de limpeza de log e data base de log de navegação, com recurso de limpeza automática, com possibilidade de personalização e alterações de configurações.
- 3.1.36. A solução deverá permitir efetuar bloqueio de conexões recebidas por determinado país ou continente, tendo como uma das funcionalidades, permitir visualizar países ou continentes líderes no ranking de tráfego malicioso e assim fazer bloqueios de entrada e saída.
- 3.1.37. A solução deverá permitir regras de redirecionamento de portas, atuando como um recurso para informar ao equipamento qual o destino a ser dado aos pacotes.
- 3.1.38. A solução deverá permitir regras de NAT (Network Address Translator), entre os hosts da rede interna e a internet, traduzindo os IPs com as seguintes características: Encaminhamento de portas, incluindo faixas de rede e o uso de múltiplos IPs públicos, NAT para IPs individuais ou sub-redes inteiras, NAT de saída, NAT de saída avançado, permitindo que seu comportamento padrão seja desativado e permitindo a criação de múltiplas flexões de regras de NAT, NAT Reflection, possibilitando que os serviços possam ser acessados por IP público a partir de redes internas.



|          |       |
|----------|-------|
| Folha nº | 222   |
| Proc. nº | 35/25 |
| Rubrica  | Fls   |

- 3.1.39. A solução deverá fazer proxy do protocolo IGMP entre segmentos de rede, bem como interface de upstream e downstream.
- 3.1.40. A solução deverá, através de funcionalidade, permitir suporte ao protocolo Universal Plug and Play (UPnP) e NAT Port Mapping Protocol (NAT-PMP), podendo configurar download e upload máximo caso necessário.
- 3.1.41. A solução deverá possuir suporte para ser configurado o serviço de Wake on LAN, através de suporte no hardware, com objetivo de ligar o computador através de um pacote específico de rede.
- 3.1.42. A solução deverá possuir suporte para atualização automática da base de seu sistema, sempre que existir alguma disponível.
- 3.1.43. A solução deverá permitir criação de tabela de horários para agendamento de regras, bem como vincular uma regra a uma agenda definida para que elas vigorem a partir de ou durante datas e horários previamente especificados.
- 3.1.44. A solução deverá fornecer recursos de gerência de tráfego de rede, sendo possível a criação de regras dos seguintes tipos: Priorização de tráfego, definindo quais protocolos possui prioridade, Limite de tráfego por protocolo, definindo qual limite máximo de um protocolo, reserva de tráfego com empréstimo em caso de não estar sendo utilizado em seu limite.
- 3.1.45. Permitir que o DHCP Relay encaminhe requisições para um servidor definido em outro segmento de rede.
- 3.1.46. A solução deverá dispor de servidor DHCP, que permita atribuir endereços IPs e configurações relacionadas aos dispositivos da rede, por meio de MACAddress.
- 3.1.47. A solução deverá permitir uso de DNS dinâmico para que seja registrado o endereço IP público com um número de prestadores de serviços de DNS dinâmico comumente usados para conectar-se à VPNs, Web Servers e também Mail Servers. Podendo ser usado conta em serviço de terceiros no mínimo as seguintes opções: DynDNS, No-IP, OpenDNS, ZoneEdit e DyNS.
- 3.1.48. A solução deverá permitir gravar logs separando por pelo menos as seguintes categorias: Firewall, DHCP, Autenticação, IPSec, PPP, VPN, Load Balance, OpenVPN, NTP.
- 3.1.49. A solução deverá permitir gravar logs em servidor externo podendo configurar até 3 servidores.
- 3.1.50. O sistema deverá permitir envio de informações pré-programadas referente ao status do link, permitindo selecionar o gráfico a ser enviado, bem como enviar e-mail informando quando houver queda de link.
- 3.1.51. O sistema deverá permitir gerenciar certificados através de modo gráfico, e criar e/ou revogar novos certificados através do painel web.
- 3.1.52. O sistema deverá permitir efetuar controle de permissão para acesso às funcionalidades da solução.
- 3.1.53. A solução deverá permitir load balancing e/ou failover no tráfego de saída para Internet, permitindo configurar de acordo com a qualidade do link ou queda do mesmo.
- 3.1.54. Possibilidade de sincronização de horário do equipamento utilizando protocolo NTP.
- 3.1.55. A solução deverá possuir suporte, através de um serviço do sistema operacional para OLSR (Optimized Link State Routing Protocol).
- 3.1.56. A solução deverá permitir utilização do protocolo Netflow versão 1, 5 ou 9 para envio de informações referente à tráfego/link, permitindo configurar no mínimo: IP de destino, porta, IP de origem e restrição de direção.
- 3.1.57. A solução deverá permitir configurar roteamento dinâmico, tal como: RIP versão 1 e 2, OSPF padrão RFC 1583 ou BGP.
- 3.1.58. A solução deverá suportar utilizar protocolo SNMP.



- 3.1.59. A solução deverá possuir no mínimo os seguintes gráficos: memória, throughput, links, VPN, qualidade dos links, processamento.
- 3.1.60. A solução deverá permitir configurar um servidor PPPoE Server no equipamento, podendo ter autenticação por: base local, RADIUS, ou acessar um servidor PPPoE para ativar algum link.
- 3.1.61. A solução deverá permitir no mínimo as seguintes opções de VPN (Site-to-Site ou Client-to-Site): IPSec, OpenVPN e o L2TP, podendo a solução ser o server ou o client e permitindo uso de VPN com outros equipamentos de outros fornecedores, sem limite de licenças.
- 3.1.62. A solução deverá permitir uso de um cliente OpenVPN do fabricante, com opção de autenticação em base AD (Active Directory) ou LDAP, podendo ser instalado em estações de trabalho Windows, MAC OS X, ou dispositivos móveis como IOS (iPhone/iPad), Android.
- 3.1.63. Deverá possuir a funcionalidade de enviar e-mail sempre que: algum usuário se conectar ou desconectar no túnel VPN. A solução deverá ainda gravar logs das conexões de VPN, permitindo visualizar relatórios.
- 3.1.64. Todos os equipamentos deverão suportar funcionamento em modo Cluster e todas licenças para seu uso deverão estar inclusas no fornecimento, permitindo a configuração de dois firewalls como um grupo de "failover", se uma interface falhar no primário ou ficar "off-line" completamente, o secundário se torna ativo, sem qualquer prejuízo de parada, lentidão ou interrupções de atividade de operação, tendo o secundário mesma capacidade que o primário (quantidade de usuários, conexões simultâneas, throughput, etc.) especificadas no dimensionamento.
- 3.1.65. A solução deverá disponibilizar funcionalidade para fazer cópias seguras de seus dados, tais como configuração e relatórios, podendo ou não ser agendados.
- 3.1.66. A solução deverá permitir também efetuar backup em servidor em nuvem (cloud) de maneira automática e deverá estar incluso no contrato o serviço em nuvem para manter ao menos 5 cópias das configurações do equipamento.
- 3.1.67. A solução deverá possuir módulo de liberação e bloqueio de maneira fácil e rápida e atualizados diariamente comuns para liberação ou bloqueio em uma rede considerada comum, tais como: Windows Update, Java, Caixa/Conectividade Social, Bancos, Microsoft, Governo, Acesso remoto, Redes sociais.
- 3.1.68. A solução deverá permitir gerenciamento de visitantes para acesso à redes para visitantes, com possibilidade de autenticação para usuários, por meio de cadastro, facebook, AD / LDAP, RADIUS.
- 3.1.69. A solução deverá permitir bloqueio de acesso à sites, por meio de categoria (atualizado diariamente com no mínimo 48 categorias), com regras que permita a escolha de trabalhar com proxy transparente ou autenticado. No caso de autenticação, os usuários poderão se autenticar através de: base local, LDAP, Active Directory (AD), RADIUS, NTdomain e Single-Sign-on.
- 3.1.70. A solução deverá permitir a criação de categorias personalizadas sem limite de quantidades, bem como permitir criação de lista brancas/negras como exceções. A solução deverá também scanear arquivos que forem efetuados download para verificar de vírus/malwares (todas licenças inclusas).
- 3.1.71. A solução deverá ter módulo de diagnóstico de bloqueio ou liberação de URL por usuário, mostrando qual regra está permitindo ou bloqueando o acesso a fim de diagnóstico rápido de ajuste da regra. A solução deverá também permitir o usuário justificar o acesso à uma URL bloqueado, podendo assim acessar mediante somente a justificativa ou mediante aprovação após a justificativa por parte de usuário com acesso administrativo.
- 3.1.72. A solução deverá compor suite de relatórios no mesmo equipamento ou em caso de necessidade de uso de outro equipamento ou software o fornecedor deverá incluir todas os valores e licenças bem como equipamentos para atender ao quesito "relatórios de



gerenciamento"; A suíte de relatórios deverá possuir capacidade de ser acessada por meio de smartphones IOS/Ipnone e Android e poder gerenciar os usuários que possuem acesso à ferramenta.

- 3.1.73. A suíte de relatório deverá permitir a personalização da marca estampada no cabeçalho do relatório, e possuir ao menos as seguintes informações de acesso: usuários, consumo de link, acessos por IP, acessos por usuário, acesso por categoria, acesso por meio de VPN.
- 3.1.74. A solução deverá permitir visualizar estrutura de rede conectada entre unidades por meio do painel em Cloud, permitindo visualizar problemas de rotas de conexão entre unidades, e permitir fazer failover sobre conexões de VPN de maneira automática sem intervenção manual.
- 3.1.75. A solução deverá fornecer sistema de detecção e prevenção de intrusão com capacidade de inspecionar o "payload" do pacote, fazendo o registro dos pacotes, além de detectar as invasões. Capaz de detectar quando um ataque está sendo realizado e, baseado nas características do ataque, alterar ou remodelar sua configuração de acordo com as necessidades, além de permitir a configuração de avisos ao administrador do ambiente sobre o ataque.
- 3.1.76. A solução deverá ser fornecida em appliance, ou seja, integração do hardware com software do mesmo integrador. Não serão aceitos equipamentos de uso genérico.
- 3.1.77. Caso o fabricante tenha um novo modelo durante o período do contrato, a CONTRATADA deverá efetuar a substituição pelo modelo mais novo sem ônus adicional à CONTRATANTE.
- 3.1.78. Não serão aceitos modelos do tipo SOHO (Small Office/Home Office) ou quaisquer appliances preparados para modelos do tipo "Home office".
- 3.1.79. No caso de módulos opcionais, caso o equipamento não permita a substituição, deverá ser contemplado o equipamento considerando o opcional como permanente.
- 3.1.80. A solução deverá ser entregue em formato de equipamentos físicos, sendo vedado o fornecimento de solução virtualizada.
- 3.1.81. O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.
- 3.1.82. Somente serão aceitos equipamentos novos e sem uso anterior. Não serão aceitos equipamentos do tipo end-of-life ou descontinuados.
- 3.1.83. **Hardware**
  - 3.1.83.1. O dispositivo de hardware deverá possuir as especificações técnicas mínimas abaixo relacionadas:
  - 3.1.83.2. Possuir memória mínima de: 4GB
  - 3.1.83.3. Possuir no mínimo 4 interfaces Gigabit Ethernet
  - 3.1.83.4. Possuir no mínimo 2 interfaces Bypass
  - 3.1.83.5. Processador com 2 núcleos e 2 threads
  - 3.1.83.6. Frequência mínima de 2.40 GHz para o processador
  - 3.1.83.7. Possuir porta Console com conexão RJ45
  - 3.1.83.8. Saída de vídeo HDMI ou VGA
  - 3.1.83.9. Possuir 2 portas USB
  - 3.1.83.10. Possuir fonte de alimentação Full Range.
  - 3.1.83.11. Armazenamento interno de 240GB tipo SSD
  - 3.1.83.12. Permitir simultaneamente no mínimo a quantidade simultânea de 50 dispositivos
  - 3.1.83.13. Possuir throughput mínimo de Firewall de 3.9 Gb/s
- 3.1.84. **ATUALIZAÇÕES DE SOFTWARE**



3.1.84.1. Durante a vigência contratual, deverá ser possível realizar a atualização do software dos equipamentos para obter novas funcionalidades e correção de bugs, sem custos adicionais para a CONTRATANTE.

### 3.2. LOCAÇÃO DE SWITCH GERENCIÁVEL LAYER 3

- 3.2.1. O equipamento deve possuir no mínimo os seguintes requisitos:
- 3.2.2. Múltiplas portas Gigabit Ethernet e interfaces SFP+;
- 3.2.3. Agregação de links (LACP) e suporte à redundância;
- 3.2.4. VLANs 802.1Q e roteamento Layer 3;
- 3.2.5. QoS avançado para priorização de tráfego crítico;
- 3.2.6. ACLs, autenticação 802.1X e protocolos contra loops (STP/RSTP/MSTP);
- 3.2.7. Integração com SNMP, análise de tráfego por sFlow/NetFlow;
- 3.2.8. Interface de gerenciamento local e remoto.

### 3.3. INSTALAÇÃO E CONFIGURAÇÃO

- 3.3.1. Todos os equipamentos devem ser instalados e configurados nas dependências da CONTRATANTE no prazo de 10 dias.
- 3.3.2. A CONTRATADA deverá prestar serviços de instalação e configuração da solução, que compreendem, entre outros, os seguintes procedimentos:
- 3.3.3. Reunião de alinhamento para criação do escopo do projeto previamente a instalação.
- 3.3.4. Instalação física dos equipamentos e configuração da solução no local determinado pela equipe responsável pelo projeto por parte da CONTRATANTE.
- 3.3.5. Efetuar previamente a instalação uma análise da topologia e arquitetura da rede, considerando o funcionamento de todos equipamentos já existentes e instalados.
- 3.3.6. Análise do acesso à internet, sites remotos, serviços de rede oferecidos aos colaboradores e aos usuários externos.
- 3.3.7. Configuração do sistema de firewall, VPN, IPS, filtro URL, NAT, de acordo com as exigências levantadas.
- 3.3.8. Toda configuração do sistema deverá ser realizada de acordo com as melhores práticas recomendadas.
- 3.3.9. A instalação física dos equipamentos deverá ocorrer na sede da contratante, em horário acordado previamente com o representante local para que não haja prejuízos junto aos trabalhos executados pela OCNTRATANTE.

### 3.4. VISITA TÉCNICA/SUPORTE TÉCNICO

- 3.4.1. O suporte técnico tem por finalidade garantir a sustentação e a plena utilização da tecnologia durante a vigência do contrato. Inclui o atendimento para sanar dúvidas relacionadas com instalação, configuração e uso da tecnologia ou para correção de problemas, com ênfase na configuração de parâmetros, falhas, erros, defeitos, manutenção corretiva em geral ou vícios identificados no funcionamento da tecnologia. O suporte será prestado conforme o "SLA" descrito neste Termo de Referência.
- 3.4.2. Com o objetivo de maior assertividade na atuação, ao ocorrerem, os alertas deverão ser classificados em: Crítico (necessária atuação imediata devido a indisponibilidade ou risco iminente de indisponibilidade), Atenção (necessária atuação rápida para evitar indisponibilidade de serviços) e Informação (informação e conhecimento).
- 3.4.3. A CONTRATADA deverá fornecer serviço de monitoramento proativo, consistindo na verificação dos alertas durante o horário comercial (8h às 17h). Em caso de alertas críticos e/ou alertas repetidos de atenção, a CONTRATADA deverá contatar a equipe técnica da CONTRATANTE para solicitar aprovação de uma ação com o objetivo de evitar a indisponibilidade de algum serviço.
- 3.4.4. A CONTRATADA deverá realizar, no mínimo, visita técnica mensal totalizando 04 (quatro) horas mês para manutenção preventiva do firewall, validando as condições físicas de instalação, a fim de prevenir problemas de conexão elétricas, oxidação e demais problemas físicos que possam vir a ocorrer. Garantindo assim o pleno funcionamento da solução.



- 3.4.5. A CONTRATADA deverá mensalmente de forma presencial efetuar uma avaliação individual de cada computador da contratada, com o propósito de identificar possíveis infecções presentes no sistema operacional, realizando sua remoção imediatamente, garantindo uma rede interna protegida contra vulnerabilidades.
- 3.4.6. **Nível de severidade dos chamados técnicos**
- 3.4.7. A CONTRATADA deverá possuir sistema de chamado web para registro das solicitações, com geração de protocolo para o acompanhamento e aferição do cumprimento dos índices indicados na Meta de Disponibilidade e de Atendimento.
- 3.4.8. Para a prestação do serviço de manutenção e suporte técnico, a CONTRATADA deverá garantir os níveis mínimos de serviço definidos no "SLA - ACORDO DE NÍVEL DE SERVIÇO".
- 3.4.9. **SlA - acordo de nível de serviço**
- 3.4.10. As falhas de responsabilidade da CONTRATADA deverão ser recuperadas conforme prazos especificados abaixo, de acordo com a severidade do incidente,
- 3.4.11. Critérios de impacto para falhas na solução da CONTRATADA:
- 3.4.12. Alto: o produto ficou inoperante ou ocorreu falha de grande impacto e o sistema está parado. Para este nível de severidade o atendimento deve ser imediato e com tempo de resposta de até 1 (uma) hora para resolução total ou encontro de solução temporária de contorno.
- 3.4.13. Médio: travamento ou parada de ambiente parcial. Para este nível de severidade o tempo de resposta deve ser de até 2 (duas) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno.
- 3.4.14. Baixo: redução de performance do equipamento ou aplicação de solução temporária de contorno bem-sucedida. Para este nível de severidade o tempo de resposta deve ser de até 6 (seis) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno.
- 3.4.15. Muito Baixo: dúvidas de configuração ou anomalia de baixo impacto. Para este nível de severidade o tempo de resposta deve ser de até 8 (oito) horas, em horário comercial.
- 3.4.16. O tempo de recuperação será contado a partir do aceite do ticket, através da ferramenta, até a solução da falha.
- 3.4.17. Os tempos máximos esperados para tratamento de cada ticket também são mostrados na tabela - Tempo de Resposta e Recuperação.

**Tabela - Tempo de Resposta e Recuperação**

| Nível de Prioridade | SLA                               |                             |
|---------------------|-----------------------------------|-----------------------------|
|                     | Tempo Máximo de Primeira Resposta | Tempo Máximo de Recuperação |
| <b>Crítico</b>      | 1 hora                            | 4 horas                     |
| <b>Alto</b>         | 1 hora                            | 6 horas                     |
| <b>Médio</b>        | 2 horas                           | 12 horas                    |
| <b>Baixo</b>        | 6 horas                           | 48 horas                    |
| <b>Acordado</b>     | 8 horas                           | 72 horas                    |

- 3.4.18. Equipamento de backup



|         |       |
|---------|-------|
| Ítem nº | 227   |
| Proc nº | 35/25 |
| Subitem | 10    |

- 3.4.19. A CONTRATADA compromete-se a disponibilizar, em até 72 (setenta e duas) horas, um equipamento de backup com as mesmas especificações técnicas em caso de indisponibilidade da solução por causa de falhas de componentes ou outros problemas em que impeçam seu funcionamento.
- 3.4.20. Em caso de recorrência da indisponibilidade no mesmo chamado, a CONTRATADA deverá disponibilizar visita técnica in loco dentro do SLA previsto para a solução do problema.
- 4. SUSTENTABILIDADE**
- 4.1. A implementação do firewall de última geração (NGFW) em regime de locação contribui para a sustentabilidade, reduzindo custos iniciais com aquisição e oferecendo flexibilidade financeira. A locação do equipamento elimina a necessidade de investimentos em hardware, enquanto o suporte técnico fornecido pela empresa contratada assegura a manutenção contínua e a atualização do sistema, garantindo alta disponibilidade e segurança. Essa abordagem reduz custos operacionais e de pessoal, além de otimizar recursos, uma vez que a empresa contratada gerencia a solução de forma eficiente, alinhada às regulamentações e melhores práticas de segurança.
- 5. JUSTIFICATIVA DE NECESSIDADE DE CONTRATAÇÃO E RESULTADO PRETENDIDO**
- 5.1. Os crescentes ataques cibernéticos colocam em riscos a segurança dos dados/informações do IPSSC, servindo como prova ao fato apresentado boletim de ocorrência DD2155-1/2025 – 1ª Edição de 27/02/2025, e Resolução que Institui a Política de Segurança da Informação do IPSSC, nº 03 de 31 de março de 2025, anexo aos autos do Processo Administrativo.
- 5.2. Necessidade da Contratação: A crescente sofisticação dos ataques cibernéticos representa uma ameaça constante à integridade, confidencialidade e disponibilidade das informações que circulam no IPSSC. Diante da importância dos documentos e dados que transitam pela rede, torna-se essencial a adoção de uma solução tecnológica que garanta a proteção dos ativos institucionais e a mitigação de riscos associados a acessos não autorizados e vulnerabilidades exploráveis por agentes mal-intencionados.
- 5.3. Além disso, a implementação garantirá maior conformidade com normativas e regulamentações vigentes, como a Lei Geral de Proteção de Dados (LGPD), reforçando o compromisso da instituição com a privacidade e a segurança da informação. Diante da criticidade das informações que transitam a adoção dessa solução representa um avanço essencial na proteção dos dados e na garantia da continuidade das operações com maior segurança e eficiência.
- 5.4. Resultado pretendido: Com um sistema estruturado para oferecer alta disponibilidade e resiliência, a solução possibilita um ambiente mais seguro e estável, minimizando impactos operacionais decorrentes de incidentes cibernéticos. A simplificação operacional também contribui para a redução de custos e para a otimização dos recursos humanos.
- 6. SUBCONTRATAÇÃO**
- 6.1. Não será permitida subcontratação.
- 7. LOCAL DE ENTREGA DOS SERVIÇOS**
- 7.1. Os serviços deverão ser disponibilizados na sede do Instituto de Previdência Social de Cajamar - IPSSC.
- 8. PRAZO DO CONTRATO**
- 8.1. O Prazo contratual terá a duração de 12 (doze) meses a contar da sua assinatura, podendo ser prorrogado nos termos do art. 107 da Lei nº 14.133/2021.
- 8.2. O início da prestação de serviços será na data da assinatura contratual, devendo sua entrega ocorrer no prazo de 30 (trinta) dias a contar da emissão da ordem de serviço.
- 9. ATENDIMENTO A LGPD**
- 9.1. As partes deverão cumprir a Lei no 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.
- 9.2. É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.



- 9.3. A CONTRATADA deverá assegurar total conformidade com a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018) em todas as atividades relacionadas ao desenvolvimento, manutenção e hospedagem do site e aplicativo. Para tanto, a contratada deverá:
- 9.4. Utilizar medidas técnicas e organizacionais adequadas para proteger os dados pessoais tratados contra acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
- 9.5. Garantir a transparência no tratamento dos dados pessoais e facilitar o exercício dos direitos dos titulares, como acesso, correção, exclusão, portabilidade, e revogação de consentimento, conforme previsto pela LGPD.
- 9.6. Coletar apenas os dados pessoais estritamente necessários para o desenvolvimento e funcionamento adequado do site e aplicativo, evitando a coleta e o processamento de dados excessivos ou desnecessários.
- 9.7. Assegurar que os dados pessoais sejam tratados somente mediante o consentimento dos titulares ou em conformidade com as bases legais previstas na LGPD, e que o tratamento seja realizado exclusivamente para as finalidades informadas aos titulares.
- 9.8. Estar preparada para demonstrar, a qualquer momento, no prazo fixado pelo Contratante (prorrogável justificadamente) que todas as práticas de tratamento de dados pessoais estão em conformidade com a LGPD, através de documentação apropriada, auditorias internas e externas, e relatórios de impacto à proteção de dados.
- 9.9. Orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.
- 9.10. O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.
- 9.11. Os contratos e convênios de que trata o § 1º do art. 26 da LGPD deverão ser comunicados à autoridade nacional.
- 10. EXECUÇÃO DO OBJETO**
- 10.1. A contratada deverá prestar todo o serviço, bem como esclarecimentos relativos ao objeto contratado sempre que for acionada;
- 10.2. Atender somente consultas formuladas pelos agentes expressamente credenciados pelo IPSSC, sempre que relacionadas aos itens 1.0 ao 3.4.20 e subitens deste Termo de Referência;
- 11. MODELO DE GESTÃO DE CONTRATO**
- 11.1. 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.
- 11.2. 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.
- 11.3. As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.
- 11.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.
- 11.5. Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade 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.
- 12. DAS OBRIGAÇÕES DA CONTRATADA**
- 12.1. Executar fielmente o ajustado, prestando os serviços descritos neste Termo de Referência, em perfeitas condições para o fim a que se destinam;
- 12.2. Prestar assistência e atendimento sempre que houver solicitação da CONTRATANTE;
- 12.3. Assumir as despesas decorrentes da presente avença;



|          |                     |
|----------|---------------------|
| Folha nº | 229                 |
| Proc. nº | 35/25               |
| Rubrica  | <i>[assinatura]</i> |

- 12.4. Manter o contrato observando sempre a legislação vigente aplicável à espécie;
- 12.5. Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões de serviços que se fizerem necessários, até os limites previstos na Lei 14.133/2021, inclusive quanto aos valores, tendo como base o valor inicial do contrato, mediante celebração de termo aditivo, sempre precedido de justificativa técnica por parte da CONTRATANTE.
- 12.6. Manter durante toda a execução do objeto deste termo a compatibilidade com as obrigações assumidas, condições de habilitação e qualificação exigidas;
- 12.7. Responsabilizar-se pela emissão da Nota Fiscal e seus impostos.
- 13. DAS OBRIGAÇÕES DA CONTRATANTE:**
- 13.1. Proporcionar todas as condições necessárias à boa execução do contrato;
- 13.2. Responsabilizar-se pela comunicação, em tempo hábil, das informações de acesso aos servidores que realizarão o treinamento e gerenciamento;
- 13.3. Efetuar o pagamento convencionado em Cláusula do presente instrumento, dentro do prazo previsto, desde que atendidas às formalidades previstas.
- 14. DAS SANÇÕES**
- 14.1. As penalidades administrativas são aquelas previstas na Lei Federal nº 14.133, de 2021, concomitantemente com as disposições do Decreto Municipal nº 7.144, de 2024.
- 15. FISCALIZAÇÃO DO CONTRATO**
- 15.1. O contrato será fiscalizado pelos servidores do quadro efetivo do IPSSC - Instituto de Previdência Social dos Servidores de Cajamar, a serem indicados em momento oportuno.
- 16. ESTIMATIVA DO VALOR DA CONTRATAÇÃO**
- 16.1. O valor global estimado para 12 (doze) meses de contrato corresponde a R\$ 59.874,90 (cinquenta e nove mil, oitocentos e setenta e quatro reais e noventa centavos).
- 17. DO PAGAMENTO**
- 17.1. O pagamento será realizado de forma parcelada, a ser realizado todo o dia 10 ou dia 24 de cada mês durante a vigência contratual, mediante Nota Fiscal, a qual deverá ser emitida no prazo de 10 (dez) dias anterior a data de pagamento
- 17.2. A contratada deverá enviar juntamente com a Nota Fiscal relatório detalhado de todo o serviço prestado, o qual será verificado e analisado pelos Fiscais do contrato.
- 18. FUNDAMENTO LEGAL**
- 18.1. A prestação de serviço a que se refere o objeto será por meio de Dispensa de Licitação, nos termos da Lei 14.133/2021, Artigo 75, Inciso II.
- 19. SELEÇÃO DO FORNECEDOR**
- 19.1. A empresa vencedora será aquela que oferecer o menor preço global dentro das especificações técnicas deste Termo de Referência.
- 20. CONDIÇÕES PARA ASSINATURA DO CONTRATO**
- 20.1. Deverão ser apresentadas pela empresa selecionada as certidões de Regularidade Fiscal, FGTS, CNPJ e demais documentos necessários;
- 20.2. Para fins de contratação, o fornecedor que apresentar o menor preço global será convocado por e-mail para que no prazo de 24 (vinte e quatro) horas, apresente os seguintes documentos, sob pena de decair do direito de contratar:
- Contrato social, requerimento de empresário individual, Estatuto Social, ou outro documento apto a comprovar a existência jurídica da proponente;
  - Inscrição no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Nacional da Pessoa Jurídica (CNPJ);
  - Prova de regularidade perante a Fazenda Municipal (mobiliários);
  - Prova de regularidade relativa à Seguridade Social e ao FGTS, que demonstre cumprimento dos encargos sociais instituídos por lei;
  - Prova de regularidade perante a Justiça do Trabalho;
  - Prova de regularidade com as Fazendas Federal e Estadual (inscritos em dívida ativa);
  - Certidão Negativa do Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e o Cadastro Nacional de Empresas Punidas (Cnep); (link: <https://certidoes.cgu.gov.br/>)
  - Falência e recuperação judicial (vide Súmula 50 do TCE/SP);



|          |       |
|----------|-------|
| Folha nº | 130   |
| Proc nº  | 39125 |
| Rubrica  | Pea   |

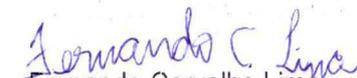
i) Prova de registro ou inscrição na entidade profissional competente, quando for caso.  
**Parágrafo único. Para os fins do disposto nos incisos anteriores deste artigo, poderão ser consultados os seguintes cadastros:**

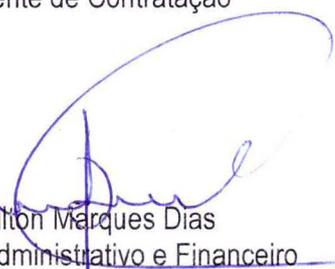
- I. Sistema de Cadastramento Unificado de Fornecedores — SICAF;
- II. Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS);
- III. Relação de apenados publicada pelo Tribunal de Contas do Estado de São Paulo;
- IV. Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa e Inelegibilidade (CNIA — CNJ).

**21. ADEQUAÇÃO ORÇAMENTÁRIA / FONTE DO RECURSO**

21.1. O recurso será proveniente da Dotação Orçamentária nº 03.01.01.09.122.0080.2174.3.3.90.39.00, Ficha nº 09, Destinação de Recurso nº 04.690.0000-RPPS TAXA ADMINISTRATIVA.

Cajamar, 10 de junho de 2.025.

  
Fernando Carvalho Lima  
Agente de Contratação

  
Milton Marques Dias  
Diretor Administrativo e Financeiro



|          |                     |
|----------|---------------------|
| Folha nº | 231                 |
| Proc nº  | 35/25               |
| Rubrica  | <i>[assinatura]</i> |

**ANEXO II – FORMULÁRIO DE PROPOSTA**

**DADOS PARA PREENCHIMENTO:**

**FORMULÁRIO DE PROPOSTA**

**DADOS CADASTRAIS DO FORNECEDOR**

**Razão Social:**

---

---

**CNPJ:**

---

---

**Endereço:**

---

---

**Município:**

---

---

**Telefone:**

---

---

**E-mail:**

---

---



|          |              |
|----------|--------------|
| Folha nº | 232          |
| Proc nº  | 75/25        |
| Rubrica  | [assinatura] |

**DADOS CADASTRAIS DO REPRESENTANTE LEGAL**

**Nome:**

\_\_\_\_\_

\_\_\_\_\_

**CPF:** \_\_\_\_\_ **RG:** \_\_\_\_\_

\_\_\_\_\_

**Endereço:**

\_\_\_\_\_

\_\_\_\_\_

**Município:**

\_\_\_\_\_

\_\_\_\_\_

**Telefone:**

\_\_\_\_\_

\_\_\_\_\_

**E-mail:**

\_\_\_\_\_

\_\_\_\_\_

**Cargo na empresa:**

\_\_\_\_\_

\_\_\_\_\_

**PROPOSTA**



| Item  | Descrição   | Unidade de Medida | Quantidade/Mês | Valor Mensal | Valor Total | Porcentagem |
|-------|---|-------------------|----------------|--------------|-------------|-------------|
| 1     | Locação de Firewall UTM NGFW  | SV                | 12 meses       | R\$          | R\$         | 87,55%      |
| 2     | Locação de switch gerenciável Layer 3 com múltiplas interfaces de alta velocidade | SV                | 12 meses       | R\$          | R\$         | 5,39%       |
| 3     | Instalação e configuração de Firewall UTM NGFW                                    | SV                | 01 serviço     | R\$          | R\$         | 3,19%       |
| 4     | Visita Técnica  | SV                | 12 visitas     | R\$          | R\$         | 3,87%       |
| TOTAL |   |                   |                |              | R\$         | 100%        |

### DECLARAÇÃO

DECLARO, sob as penas da lei que:

1. Sou o representante legal da empresa proponente;
2. A empresa proponente está atualmente enquadrada como microempresa ou empresa de pequeno porte não havendo qualquer impedimento a aplicação dos benefícios da Lei Complementar nº 123/2006 e Lei nº 14.133/2021;
3. O prazo de validade da proposta é de 60 (sessenta) dias a contar da data da apresentação desta proposta;
4. Li o Termo de Referência e o Aviso da Dispensa de Licitação e estou ciente das condições e prazo para entrega ou prestação dos serviços e, também, das implicações no caso de não assinatura do contrato ou aceitação da nota de empenho ou inadimplência;
5. Caso seja a classificada como melhor oferta, tenho condições de apresentar no prazo consignado os documentos exigidos para habilitação;
6. O(s) preço(s) indicado(s) contempla(m) todos os custos diretos e indiretos incorridos na data da apresentação desta proposta incluindo, entre outros: tributos, encargos sociais, material, despesas administrativas, lucro etc.

\_\_\_\_\_, \_\_\_\_ de \_\_\_\_\_ de 202\_\_.

representante legal

assinatura