CONTRATO ADMINISTRATIVO Nº 03/2025

PROCESSO ADMINISTRATIVO Nº: 35/2025
DISPENSA DE LICITAÇÃO Nº: 04/2025
CONTRATANTE: INSTITUTO DE PREVIDENCIA SOCIAL DOS SERVIDORES DE CAJAMAR
CONTRATADO: A2W TECNOLOGIA LTDA.

Pelo presente termo de contrato de prestação de serviços, de um lado o IPSSC – INSTITUTO DE PREVIDENCIA SOCIAL DOS SERVIDORES DE CAJAMAR, com sede na Rua Vereador Mário Marcolongo, Nº 462, Bairro: Jordanésia, CEP: 07.776-430, na cidade de Cajamar, Estado de São Paulo, inscrito no CNPJ sob o nº 02.675.642/0001-16, neste ato representado por seu Diretor Executivo **LUIZ HENRIQUE MIRANDA TEIXEIRA**, brasileiro, casado, economista, portador da cédula de identidade RG nº 28.391.407- 5 SSP/SP, devidamente inscrito no CPF sob o nº 278.478.908-01 doravante denominado CONTRATANTE, e do outro lado simplesmente denominada como doravante CONTRATADA a empresa **A2W TECNOLOGIA LTDA.**, com sede na Rua Hilda Del Nero Bisquolo, nº 102, sala 816, Jardim Flórida, Jundiaí – SP, CEP: 13208-703, devidamente inscrita no CNPJ sob o nº 07.840.931/0001-47, neste ato representada legalmente por **Anderson Franco Penteado,** brasileiro, solteiro, portador da cédula de identidade RG nº 29.418.644-X – SSP- SP e inscrito no CPF sob nº 179.536.598-67, domiciliado na Rua Pedro Domingues, nº 32, Centro, Cajamar – SP, CEP: 07750-830, **CONFORME ATOS CONSTITUTIVOS DA EMPRESA OU PROCURAÇÃO APRESENTADA NOS AUTOS**, tendo em vista o que consta no Processo nº 35/2025 e em observância às disposições da Lei nº 14.133, de 2021, resolvem celebrar o presente Termo de Contrato, decorrente ***DA DISPENSA DE LICITAÇÃO N. 04/2025***, mediante as cláusulas e condições a seguir enunciadas.

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	Valor Total
1	Locação de Firewall UTM NGFW	SV	12 meses	R$ 3.835,00	46.020,00
2	Locação de switch gerenciável Layer 3 com múltiplas interfaces de alta velocidade	SV	12 meses	R$ 260,00	R$ 3.120,00
3	Instalação e configuração de Firewall UTM NGFW	SV	01 serviço		R$ 1.900,00
4	Visita Técnica	SV	12 visitas	R$ 189,00	R$ 2.268,00
TOTAL				R$ 4.284,00	R$ 53.308,00

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, antispyware, 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.

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, troughput, 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 copias 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 suíte 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/Iphone 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
Crítico	1 hora	4 horas
Alto	1 hora	6 horas
Médio	2 horas	12 horas
Baixo	6 horas	48 horas
Acordado	8 horas	72 horas

3.4.18. Equipamento de backup

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. SUBCONTRATAÇÃO

5.1. Não será permitida subcontratação.

6. LOCAL DE ENTREGA DOS SERVIÇOS

6.1. Os serviços deverão ser disponibilizados na sede do Instituto de Previdência Social de Cajamar - IPSSC.

7. PRAZO DO CONTRATO

7.1. 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.

7.2. 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.

8. MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS

8.1 O regime de execução contratual, o modelo de gestão, assim como os prazos e condições de conclusão, constam no Termo de Referência, anexo a este contrato.

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. ANTICORRUPÇÃO

10.1 Para a execução deste contrato, nenhuma das partes poderá oferecer, dar ou se comprometer a dar a quem quer que seja, ou aceitar ou se comprometer a aceitar de quem quer que seja, tanto por conta própria quanto por intermédio de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou não financeiras ou benefícios de qualquer espécie que constituem prática ilegal ou de corrupção, seja de forma direta quanto ao objeto deste contrato, ou de outra forma a ele não relacionada, devendo garantir, ainda que seus prepostos e colaboradores ajam da mesma forma.

11. EXECUÇÃO DO OBJETO

11.1. A contratada deverá prestar todo o serviço, bem como esclarecimentos relativos ao objeto contratado sempre que for acionada;

11.2. 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;

12. MODELO DE GESTÃO DE CONTRATO

12.1. 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.

12.2. 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.

12.3. 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.

12.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

12.5. 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.

13. DAS OBRIGAÇÕES DA CONTRATADA

13.1. Executar fielmente o ajustado, prestando os serviços descritos neste Termo de Referência, em perfeitas condições para o fim a que se destinam;

13.2. Prestar assistência e atendimento sempre que houver solicitação da CONTRATANTE;

13.3. Assumir as despesas decorrentes da presente avença;

13.4. Manter o contrato observando sempre a legislação vigente aplicável à espécie;

13.5. 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.

13.6. Manter durante toda a execução do objeto deste termo a compatibilidade com as obrigações assumidas, condições de habilitação e qualificação exigidas;
13.7. Responsabilizar-se pela emissão da Nota Fiscal e seus impostos.

14. DAS OBRIGAÇÕES DA CONTRATANTE:

14.1. Proporcionar todas as condições necessárias à boa execução do contrato;
14.2. Responsabilizar-se pela comunicação, em tempo hábil, das informações de acesso aos servidores que realizarão o treinamento e gerenciamento;
14.3. Efetuar o pagamento convencionado em Cláusula do presente instrumento, dentro do prazo previsto, desde que atendidas às formalidades previstas.

15. DAS SANÇÕES

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

16. FISCALIZAÇÃO DO CONTRATO

16.1. O contrato será fiscalizado pelos servidores CARLOS EUGÊNIO DE OLIVEIRA JUNIOR, CPF nº 281.494.558-09 - fiscal técnico e JOANNA MARIA FERREIRA GONÇALVES, CPF nº 338.236.468-93 - fiscal administrativo.

17. DO PAGAMENTO

17.1. O valor global para 12 (doze) meses de contrato corresponde a R$ 53.308,00 (cinquenta e três mil e trezentos e oito reais).
17.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

18. PRAZO DE PAGAMENTO

18.1. O pagamento será realizado de forma parcelada, a ser realizado todo o dia 10 ou dia 20 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
18.2. 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.

19. FORMA DE PAGAMENTO

19.1 O pagamento será realizado através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado:

a) **NOME BENEFICIÁRIO:** A2W TECNOLOGIA LTDA.
b) **TIPO DE PESSOA:** JURÍDICA
c) **CPF/CNPJ:** 07.840.931/0001-47
d) **BANCO:** BRADESCO
e) **AGÊNCIA:** 0368-9
f) **CONTA CORRENTE:** 295189-4

20. CONDIÇÕES DE PAGAMENTO

20.1.1. A emissão da Nota Fiscal/Fatura será precedida do recebimento definitivo do objeto da contratação, conforme

disposto neste instrumento e/ou no Termo de Referência. Quando houver glosa parcial do objeto, o contratante deverá comunicar a empresa para que emita a nota fiscal ou fatura com o valor exato dimensionado.

20.1.2. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que o contratado providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o contratante;

20.1.3. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133/2021.

20.1.4. Previamente a cada pagamento, a Administração deverá realizar consulta para verificar a manutenção das condições de habilitação exigidas na contratação;

20.1.5. 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.

20.1.6. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

20.1.7. 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.

20.1.8. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação.

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

20.1.10. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

20.1.11. 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.

21. REAJUSTE

21.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano (doze meses) contado da data da proposta em 21 agosto de 2025.

21.2. Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do índice IPCA/IBGE (ou outro índice que venha a substitui-lo), exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

21.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

21.4. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

21.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

21.6. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

21.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

21.8. O reajuste será realizado por apostilamento.

22. FUNDAMENTO LEGAL

22.1. 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.

23. CONDIÇÕES PARA ASSINATURA DO CONTRATO

23.1. Deverão ser apresentadas pela empresa selecionada as certidões de Regularidade Fiscal, FGTS, CNPJ e demais documentos necessários;

23.2. 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 quaro) horas, apresente os seguintes documentos, sob pena de decair do direito de contratar:

a) Contrato social, requerimento de empresário individual, Estatuto Social, ou outro documento apto a comprovar a existência jurídica da proponente;
b) Inscrição no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Nacional da Pessoa Jurídica (CNPJ);
c) Prova de regularidade perante a Fazenda Municipal (mobiliários);
d) Prova de regularidade relativa à Seguridade Social e ao FGTS, que demonstre cumprimento dos encargos sociais instituídos por lei;
e) Prova de regularidade perante a Justiça do Trabalho;
f) Prova de regularidade com as Fazendas Federal e Estadual (inscritos em dívida ativa);
g) 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/)
h) Falência e recuperação judicial (vide Súmula 50 do TCESP);
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).

24. DA EXTINÇÃO CONTRATUAL

24.1 O contrato se extingue quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes;

24.2 O contrato pode ser extinto antes do prazo nele fixado, sem ônus para o Contratante, quando esta não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

24.3 A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação do contratado pelo contratante nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia.

24.4 Caso a notificação da não-continuidade do contrato de que trata este subitem ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação.

24.5 O contrato pode ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da NLLC, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

24.6 Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

24.7 A alteração social ou modificação da finalidade ou da estrutura da empresa não ensejará rescisão se não restringir sua capacidade de concluir o contrato.

24.8 Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

24.9 O termo de rescisão, sempre que possível, será precedido de balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos; relação dos pagamentos já efetuados e ainda devidos e indenizações e multas.

25. ADEQUAÇÃO ORÇAMENTÁRIA / FONTE DO RECURSO

25.1. 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.

26. DOS CASOS OMISSOS

26.1 Os casos omissos serão decididos pelo CONTRATANTE, segundo as disposições contidas na Lei nº 14.133, de 2021 e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

27. DAS ALTERAÇÕES

27.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

27.2. O CONTRATADO é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do termo de contrato.

27.3. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

28. DA PUBLICAÇÃO

28.1. Incumbirá à CONTRATANTE providenciar a publicação deste instrumento nos termos e condiçõe previstas na Lei nº 14.133/21.

29. DO FORO

29.1. É eleito o Foro da Comarca do município de Cajamar para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não possam ser compostos pela conciliação, conforme art. 92, §1º da Lei nº 14.133/21.

Cajamar, 18 de setembro de 2025.

gov.br Documento assinado digitalmente
LUIZ HENRIQUE MIRANDA TEIXEIRA
Data: 18/09/2025 11:08:12-0300
Verifique em https://validar.iti.gov.br

IPSSC – Instituto de Previdência Social dos Servidores de Cajamar
LUIZ HENRIQUE MIRANDAS TEIXEIRA
Diretor Executivo
Contratante

gov.br Documento assinado digitalmente
ANDERSON FRANCO PENTEADO
Data: 18/09/2025 17:00:39-0300
Verifique em https://validar.iti.gov.br

A2W TECNOLOGIA LTDA.
Anderson Franco Penteado
Sócio
Contratada

TESTEMUNHAS:

1._____
Nome: Joanna Maio T. Gonçalves
RG nº 42.192.899-2

2._____
Nome:
RG nº

ANEXO LC-01 - TERMO DE CIÊNCIA E DE NOTIFICAÇÃO

CONTRATANTE: Instituto de Previdência Social dos Servidores de Cajamar - IPSSC

CONTRATADA: A2W TECNOLOGIA LTDA.

CONTRATO Nº 03/2025

OBJETO: 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

Na qualidade de Contratante e Contratado, respectivamente, do Termo acima identificado, e, cientes do seu encaminhamento ao TRIBUNAL DE CONTAS DO ESTADO, para fins de instrução e julgamento, damo-nos por CIENTES e NOTIFICADOS para acompanhar todos os atos da tramitação processual, até julgamento final e sua publicação e, se for o caso e de nosso interesse, para, nos prazos e nas formas legais e regimentais, exercer o direito da defesa, interpor recursos e o mais que couber.Outrossim, estamos CIENTES, doravante, de que todos os despachos e decisões que vierem a ser tomados, relativamente ao aludido processo, serão publicados no Diário Oficial do Estado, Caderno do Poder Legislativo, parte do Tribunal de Contas do Estado de São Paulo, de conformidade com o art. 90 da Lei Complementar n° 709, de 14 de janeiro de 1993, precedidos de mensagem eletrônica aos interessados.

Cajamar, 18 de setembro de 2025.

CONTRATANTE:

Nome e cargo: Luiz Henrique Miranda Teixeira
Diretor Executivo

E-mail institucional: diretoria_executiva@ipssc.sp.gov.br

E-mail pessoal: luizhmt@yahoo.com.br

Assinatura: gov.br Documento assinado digitalmente
LUIZ HENRIQUE MIRANDA TEIXEIRA
Data: 18/09/2025 11:08:12-0300
Verifique em https://validar.iti.gov.br

CONTRATADA:

Nome e cargo:

E-mail institucional:

E-mail pessoal: gov.br Documento assinado digitalmente
ANDERSON FRANCO PENTEADO
Data: 18/09/2025 17:02:28-0300
Verifique em https://validar.iti.gov.br

Assinatura:

Folha nº 6
Proc. nº 3225
Rubrica

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%
TOTAL					R$ 59.874,90	100%

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.

Folha nº
Proc. nº
Rubrica

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.

Folha nº 26
Proc nº 23135
Rubrica

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, antispyware, 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.

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, troughput, 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 copias 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 suíte 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/Iphone 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.

Folha nº 34
Proc. nº 3345
Rubrica

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
Crítico	1 hora	4 horas
Alto	1 hora	6 horas
Médio	2 horas	12 horas
Baixo	6 horas	48 horas
Acordado	8 horas	72 horas

3.4.18. Equipamento de backup

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.

Folha nº 76
Proc. nº 3/24
Rubrica

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

Folha nº 22
Proc. nº 3572/25
Rubrica

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;
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 n° 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 através de Portaria contendo as devidas informações.

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 quaro) horas, apresente os seguintes documentos, sob pena de decair do direito de contratar:
a) Contrato social, requerimento de empresário individual, Estatuto Social, ou outro documento apto a comprovar a existência jurídica da proponente;
b) Inscrição no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Nacional da Pessoa Jurídica (CNPJ);
c) Prova de regularidade perante a Fazenda Municipal (mobiliários);

Folha nº 11
Proc. nº 35124
Rubrica

d) Prova de regularidade relativa à Seguridade Social e ao FGTS, que demonstre cumprimento dos encargos sociais instituídos por lei;
e) Prova de regularidade perante a Justiça do Trabalho;
f) Prova de regularidade com as Fazendas Federal e Estadual (inscritos em dívida ativa);
g) 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/)
h) Falência e recuperação judicial (vide Súmula 50 do TCESP);
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).

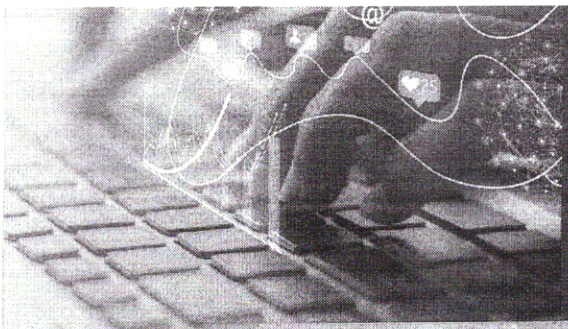
21. ADEQUAÇÃO ORÇAMENTÁRIA / FONTE DO RECURSO

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



A2W

Edifício The One Office Tower
Rua Hilda de Nero Bisquolo, 102 – Sala 816 – Jundiaí – SP
CNPJ 07.840.931/0001-47 – IE 407.963.484.119

Cajamar 21 de Agosto de 2025.

PROPOSTA

INSTITUTO DE PREVIDÊNCIA SOCIAL DOS SERVIDORES DE CAJAMAR

OBJETO: 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 estabelecid.as neste instrumento.

ITEM	DESCRIÇÃO	UNID DE MEDIDA	QTDE MÊS	VAL. MEN. ESTIMADO	VAL. TOT. ESTIMADO
1	Locação de Firewall UTM NGFW	SV	12 Meses	R$ 3.835,00	R$ 46.020,00
2	Locação de switch gerenciável Layer 3 com múltiplas interfaces de alta velocidade	SV	12 Meses	R$260,00	R$ 3.120,00
3	Instalação e configuração de Firewall UTM NGFW	SV	1 Serviço	R$1.900,00	R$1.900,00
4	Visita Técnica	SV	12 Visitas	R$189,00	R$2.268,00

Valor da proposta mensal: R$4.442,33 (Quatro mil, quatrocentos e quarenta e dois reais e trinta e três centavos).

Valor total da proposta anual: R$53.308,00 (Cinquenta e três mil, trezentos e oito reais).

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 apl icação dos benefícios da Lei Complementar n° 123/2006 e Lei n° 14.133/2021;

Folha nº 135
Proc nº 35/25
Rubrica

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(rn) todos os custos diretos e indiretos incorridos na data da apresentação desta proposta incluindo, entre outros: tributos, encargos sociais, materia l, despesas administrativas, lucro etc.

Cajamar 21 de agosto de 2025

Anderson Franco Penteado
A2W Tecnologia LTDA

11 99750-3344

contato@a2wtecnologia.com.br