ANEXO I - TERMO DE REFERÊNCIA

1. UNIDADE REQUISITANTE: COORDENADORIA DE GESTÃO DAS AQUISIÇÕES PÚBLICAS E ADMINISTRAÇÃO PATRIMONIAL - CAPAP/SEGET

2. DO OBJETO: AQUISIÇÃO DE SOLUÇÃO DE SEGURANÇA – APPLIANCE com características de Firewall (Next Generation Firewall - NGFW) stateful, VPN, filtro de URL, filtro de spyware, incluindo hardware, software, serviços de instalação, configuração, operação assistida, suporte técnico, treinamento certificado pelo fabricante do equipamento e garantia dos equipamentos.

2.1. Proteger a infraestrutura computacional da Prefeitura Municipal de Sobral com uma solução de segurança, com alta disponibilidade, capaz de bloquear ameaças externas (Internet) e internas, bem como controlar o fluxo de dados entre essas redes.

2.2. GARANTIA: 36 (trinta e seis) meses.

2.3. Este objeto será realizado através de **Adesão à Ata Registro de Preço**, com fornecimento POR DEMANDA.

2.4. Valor aderido

R$ 243.000,00 (duzentos e quarenta e três mil reais)

3. DA JUSTIFICATIVA:

A contratação se justifica pela necessidade de expansão e modernização do Datacenter da Prefeitura Municipal de Sobral, possibilitando instalação, execução e armazenamento dos bancos de dados e cópias de segurança de vários novos sistemas desenvolvidos e utilizados especificamente pela administração pública, aprimorando a gestão municipal, sempre visando a eficiência e a melhoria dos serviços prestados aos cidadãos.

A presente aquisição visa a estruturação e a qualidade da gestão do serviço público, sendo a adesão instrumento legal e eficiente para adequação das aquisições à economicidade e ao orçamento, resguardando-se dessa forma contratações em quantidades e em qualidades inferiores prevenindo soluções de continuidade nas ações essenciais, uma vez que, durante a realização de um processo licitatório para aquisição de equipamentos de T.I. e até mesmo após a contratação, várias intercorrências prejudiciais à aquisição de todos os itens necessários para a expansão e modernização do Datacenter da Prefeitura Municipal de Sobral podem acontecer, não havendo na legislação solução rápida e eficiente que garanta o sucesso da licitação e o efetivo recebimento de um produto de qualidade, sendo a Adesão mecanismo legal que minimiza as possibilidades de intercorrência na aquisição pública.

O processo de adesão requerido tem por objetivo prover a expansão e modernização tecnológica do sistema de redes da Prefeitura Municipal de Sobral, a qual necessita fornecer aos servidores, convidados e/ou colaboradores eventuais, acesso aos sistemas de gestão pública de maneira segura, pratica e eficiente para que sejam desenvolvidas suas atividades laborais em conformidade com os padrões de eficiência necessários para o bom funcionamento da gestão municipal como um todo, refletindo no aprimoramento da prestação dos serviços públicos, da transparência administrativa e da fiscalização interna e externa. Assim, faz-se necessária à contratação de Empresa que opere no ramo de fornecimento de material de redes e infraestrutura e que disponha de condições para pronto atendimento da demanda municipal.

Pelo exposto, e em função de sua essencialidade, é oportuno e há conveniência da Administração em buscar a referida contratação, uma vez que a infraestrutura de redes da Prefeitura Municipal de Sobral, em decorrência das constantes inovações tecnológicas, necessita ser modernizada e potencializado o sistema de redes desta municipalidade, sobretudo para que não haja infortúnios que acarretem a interrupção da gestão pública de Sobral.

4. DAS ESPECIFICAÇÕES E QUANTITATIVOS

ITEM DA ATA	ESPECIFICAÇÃO	QTD.
1.	XG 310 HW APPLIANCE WITH 8 X GBE COPPER PORTS, 2 X GBE SFP, 2 X 10 GBE SFP+, 1 EXPANSION BAY FLEXI PORT MODULE, 3 USB 3.0 PORTS, HDMI PORT, SSD 180GB, CONNECTOR FOR 2ND EXTERNAL POWER SUPPLY, CONNECTOR FOR POE POWER + BASE LICENSE (FW, VPN & WIRELESS) + CABLE	02
	XG 310 ENTERPRISE GUARD SUBCRIPTIONS COM CONTROLE SOBRE POLÍTICAS, FILTRO DE URL & DOMAIN, ANTIVÍRUS (NÍVEL DE GATEWAY), CONTROLE DE APLICAÇÃO E FILTRO DE CONTEÚDO, CARACTERÍSTICAS DE IPS, IDENTIFICAÇÃO DO USUÁRIO, QOS E TRAFFIC SHAPING, VPN CLIENTE TO SITE, VPN SITE TO SITE, NAT E ROTEAMENTO, AS SOLUÇÕES DE ARMAZENAM. LOGS COM GESTÃO DE RELATÓRIOS E GRÁFICOS E CAPACIDADE DE ARMAZENAM DE ATÉ 13 MESES E GESTÃO CENTRALIZADO DE 5 APPLIANCES POR 3 ANOS	01
	XG 310 – ENHANCED SUPPORT POR 3 ANOS	01
	SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO COM OPERAÇÃO ASSISTIDA DE 30 DIAS PARA 2 (DOIS) XG 310 HW NO FORMATO ATIVO-PASSIVO COM ENTERPRISE GUARD SUBSCRIPTION DOS APPLIANCES POR 3 ANOS	01

	SERVIÇOS COOPTEC DE SUPORTE ON SITE ADVENCED (24X76HS) PARA 2 (DOIS) XG 310 HW COM ENTERPRISE GUARD SUBSCRIPTION DOS APPLIANCES POR 3 ANOS	01
	SERVIÇOS DE TREINAMENTO EAD COM CERTIFICAÇÃO OFICIAL DO FABRICANTE SOPHOS, MINISTRADO NA LÍNGUA PORTUGUESA	02

4.1. Especificação Detalhada:

4.1.1. A solução deve possuir licenças baseadas nos recursos do appliance;

4.1.2. A solução deverá ser com altura de 1U e 19 polegadas para instalação em RACK;

4.1.3. O appliance deve possui, no mínimo, 8 (oito) portas padrão Gigabits Ethernet 1000BaseT com permitindo a conectorização de cabo UTP categoria 6 com conector RJ45 e operando em modo autosense e half/full duplex., 2 (duas) portas GbE SFP e 2 (duas) portas 10GbE SFP.

4.1.4. Deve possuir portas USB 3.0

4.1.5. Deve possuir porta HDMI

4.1.6. Deve possuir painel LCD na parte frontal de appliance com funcionalidades básicas para ajudar na gerência do equipamento.

4.1.7. Possuir no mínimo 01 (uma) interface do tipo console RJ45, para gerência local do equipamento.

4.1.8. Implementar agregação de links conforme padrão IEEE 802.3ad com suporte a LACP.

4.1.9. Deve possuir, no mínimo, 180GB de espaço em SSD interno, para armazenamento local de eventos e relatórios.

4.1.9.1. Deve possuir uma gaveta/slot para expansão de portas, contendo as seguintes opções de extensão:

2.5.10.1.1 8 (oito) ports GE copper;

2.5.10.1.2 8 (oito) ports GE SFP

2.5.10.1.3 2 (duas) ports 10GE SFP+

2.5.10.1.4 4 (quatro) ports 10 GE SFP+

2.5.10.1.5 2 (duas) ports 40GE QSFP+

2.5.10.1.6 4 (quatro) ports GE cooper

2.5.10.1.7 1 (uma) port LAN by-pass

2.5.10.1.8 4 (quatro) ports GE PoE

2.5.10.1.9 8 (oito) ports GE PoE

4.1.10. Deve possuir possibilidade (opcional) de instalar uma fonte redundante;

4.1.11. Suportar, no mínimo:

4.1.11.1. 200.000 novas conexões por segundo

4.1.11.2. 17.000.000 sessões simultâneas

4.1.11.3. 27 Gbps de rendimento de throughput do FireWall para pacotes UDP;

4.1.11.4. 5 Gbps de tráfego analisado por IPS;

4.1.11.5. 2,5 Gbps de throughput de VPN AES;

4.1.12. A solução deverá atender, no mínimo, as seguintes características e critérios de throughput em ambiente/mundo real, baseados em testes realizados com um mix de protocolos do mundo corporativo, utilizando até 50% da capacidade de processamento do appliance.

2.5.13.1 500 Mbits de rendimento de throughput de IPS;

2.5.13.2 330 Mbits de rendimento de throughput de funcionalidades NGFW;

2.5.13.3 600 Mbits de rendimento de throughput VPN AES;

4.1.13. Possuir uma solução de software e hardware com capacidade de armazenar 365 dias para a função de gerenciamento dos logs e relatórios, que ficará hospedado na infraestrutura da CONTRATANTE.

5. REQUERIMENTOS GERAIS

5.1. Ser APPLIANCES, ou seja, hardwares e softwares customizados e dedicados especificamente para a aplicação a que se destinam.

5.2. Ser composto por dispositivos fisicamente independentes, com gabinete e fonte de alimentação própria. Cada equipamento deverá ser uma solução utilizando um único gabinete, montável em rack padrão de 19', não sendo superior a 1U, incluindo kit tipo trilho para a adaptação caso necessário, e cabos de alimentação.

5.3. Cada equipamento deve possuir fonte de alimentação com chaveamento automático 110/220 V – 50-60Hz. A fonte fornecida deve suportar sozinha a operação da unidade com todos os módulos de interface ativos;

5.4. Suportar:

5.4.1. sFlow ou NetFlow ou IPFIX;

5.4.2. Protocolo NTP para sincronismo de relógio do equipamento.

5.4.3. Protocolo SNMP, para checagem de status e TRAP para envio e notificação de alarmes.

5.5. Possuir capacidade de enviar logs e eventos em um servidor remoto via protocolo syslog.

5.6. Possui a função de tolerância a falhas (alta disponibilidade) no modo Ativo/Passivo entre equipamentos do mesmo modelo, de forma a garantir que, se um dos firewalls parar de funcionar, o outro deverá assumir automaticamente, suportando todo o tráfego.

5.7. Permitir o encaminhamento de no mínimo 10.000 (dez mil) endereços IP nas redes internas.

5.8. Permitir backup da configuração remotamente para um host ou servidor de gerenciamento.

5.9. Todos os recursos solicitados na especificação devem funcionar e receber atualizações até a data de expiração do período de garantia.

5.10. Os recursos de VPN, routing e firewall devem continuar funcionando mesmo após o término da garantia.

5.11. A solução deverá permitir contemplar gestão de wireless com APS do próprio fabricante.

5.12. A solução deverá permitir gerenciar os APS em uma zona própria para contemplar a segurança da rede.

5.13. A solução deverá permitir suportar o uso de hotspot e capitive portal gerenciado.

5.14. A solução deverá ´permitir, opcionalmente, o uso de hotspot e captive portal com envio automático de senhas para autenticação, via SMS ou WhatsApp.

5.15. A solução deverá permitir suportar a criação de múltiplos SSID.

5.16. A solução deverá permitir a criação de grupos de APS.

5.17. A solução deverá permitir a criação de hotspot vouchers por períodos, e por volume de dados com a opção de cotas para minutos, horas e dias, MB e GB.

5.18. A solução deverá permitir a customização do hotspot.

5.19. A solução deverá permitir o redirecionamento para um URL especifico após o login no hotspot.

5.20. A solução deverá permitir a aplicação de políticas de segurança como "WEB Policy, Ips Policy, Traffic Shaping", na rede Wireless.

Controle sobre políticas.

5.1.21 Suporte integrado de política controlada por parâmetros de: perímetro, usuário, grupo, ip, aplicação e agendamento.

5.22. Suportar os seguintes controles sobre políticas para todas as características de segurança por:

5.22.1. Porta (socket) e protocolo;

5.22.2. Aplicação e categoria de aplicação;

5.22.3. URL e Domínio;

5.22.4. Usuário e Grupo;

5.22.5. Endereço IP, rede e zonas de segurança;

5.22.6. Política DLP;

5.22.7. Política de IPS;

5.22.8. Por tipo de arquivo (myme type);

5.23. Suportar políticas de objetos e regras IPV6;

5.24. Suportar aplicações multimídia como: H.323, SIP.

5.25. Permitir a criação de objetos do tipo IP, SUBREDE, Protocolo e também objetos que agrupem estes, podendo ser utilizados nas políticas de modo a facilitar a criação de regras.

Filtro de URL & Domain

5.26. Suportar "URL-Filtering" e "Domain Filter".

5.27. Possuir um Banco de Assinaturas que deverá ser atualizado automaticamente.

5.28. Suportar categorização de URL e Domínios, contemplando um mínimo de categorias que possam identificar os seguintes conteúdos: Adulto ou pornográfico, jogos online, vídeo ou áudio em streaming, sites maliciosos, redes sociais, chats, sites de download (filesharing), armazenamento em nuvem, proxy anônimos, acesso remoto, sites de conteúdo de gosto duvidoso, ou apavorante ou que cause choque, entre outras categorias comumente encontradas em soluções proprietárias ou livres.

5.29. Suportar a customização de páginas de bloqueio de conteúdo, permitindo a alteração de título, logótipo e mensagens personalizadas além de mostrar no mínimo a URL/Domínio, categoria, o IP do cliente e o nome do Usuário.

5.30. Enviar para log tráfego permitido ou negado com detalhes como IP/Usuário, Grupo, Categoria, URL, Data e hora, etc.

5.31. Fazer "full inspection ssl trafic", além de inspecionar HTTP comprimido ou zipado

Antivírus (Nível de Gateway)

5.32. Conter solução antivírus integrado com mecanismos de automatização de atualização de assinaturas periódicas.

5.33. Inspecionar tráfegos HTTP, HTTPS e FTP, detectando e bloqueando vírus e malwares.

5.34. Gravar em log tráfego malicioso bloqueado detalhando IP/Usuário/Grupo, Conteúdo Malicioso, Data e Hora.

5.34. Fornecer proteção contra-ataques dia zero por:

5.34.1. Visibilidade de aplicação e seu conteúdo;

5.34.2. SSL-tráfego comprimido;

5.34.3. Tráfego comprimido;

5.34.4. Arquivos tunelados com aplicações e protocolos;

5.35. Este recurso deve possibilitar a atualização das assinaturas automaticamente e carregar as novas sem interrupção.

Controle de Aplicação e Filtro de Conteúdo

5.36. Permitir criação de objetos customizados para identificação de assinaturas de aplicações não conhecidas.

5.37. O reconhecimento das aplicações deve se baseado no reconhecimento de assinatura da aplicação, não somente identificando pela porta de comunicação (Exemplo tcp/80=http).

5.38. Permitir visualização de lista de aplicações conhecidas suportadas.

5.39. Suportar atualização dinâmica de banco de dados de aplicações.

5.40. Reconhece tráfego "peer2peer" como: Bittorrent, emule, neonet, etc.

5.41. Reconhecer tráfego específicos de "instant messaging" (IM) como: AIM, YIM, Facebook Chat, etc.

5.42. Reconhecer tráfego de proxies como: ultrasurf, ghostsurf e Kproxy;

5.43. Suportar protocolos baseados em voz.

5.44. Possuir identificação de usuário integrada permitindo políticas baseadas em usuários e grupos de Active Directory permitindo ou negando acesso de determinadas aplicações.

Caraterísticas de IPS

5.45. Possuir recursos habilitados incluso de IPS interno, capaz de detectar e impedir automaticamente uma gama de ataque compatível aos principais ataques orientados às 7 camadas do modelo OSI.

5.46. Identificar as ameaças baseando-se em assinaturas de sua base de dados.

5.47. Bloquear ataques a aplicações vulneráveis.

5.48. Bloquear ataques de spyware e malware.

5.49. Bloquear ataques de "exploit" de rede e de camada de aplicação.

5.50. Bloquear ataques "buffer overflow".

5.51. Bloquear ataques do tipo DoS, limitando o número de requisições de um cliente por requisições por segundo e por requisições dentro de um período de tempo.

5.52. Bloquear ataques em IPV6 e IPV4.

5.53. Suportar assinaturas de ataques pelo administrador e recursos disponíveis para a plena edição destas.

5.54. O recurso de IPS deve possuir a possibilidade de atualização das assinaturas automaticamente e carregar as novas sem interrupção.

5.55. O funcionamento dos recursos de IPS se dará através de análise de assinaturas ou de comportamento de ataque, permitindo que ações sejam programadas para a prevenção de acesso destes endereços atacantes por tempo determinado.

Identificação do Usuário

5.56. Suportar os seguintes tipos de serviços de autenticação para identificação de usuário e grupo:

5.56.1. Active Directory

5.56.2. LDAP

5.56.3. RADIUS

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

Qos e Traffic Shaping

5.57. Suportar a criação de políticas QoS:

5.57.1. Por endereço de origem.

5.57.2. Por endereço de destino.

5.57.3. Por usuário e grupo do AD.

5.57.4. Por aplicação como: Skype, Bittorrent, Youtube, etc.

5.57.5. Por grupo de aplicação como: IM, P2P.

5.57.6. Por porta (socket).

5.57.7. Por agendamento de política para funcionamento em períodos parametrizados;

5.58. Suportar definição de QoS com:

5.58.1. Banda mínima garantida.

5.58.2. Banda máxima tolerada.

VPN Cliente to Site

5.59. Permitir regras de acesso da VPN baseado em usuários e grupos de Active Directory;

5.60. Suportar IPSec VPN e SSL VPN;

5.61. Deverão ser inclusas licenças para suportar no 500 (quinhentos) usuários simultâneos na VPN Client-to-Site no modo túnel IPSec;

5.62. Caso seja necessário a instalação de um software para os clientes VPN:

5.63. O software cliente VPN deverá ser capaz de realizar autenticação utilizando os protocolos LDAP

(padrão aberto e também do Active Directory) e RADIUS.

5.64. O software cliente deve ser compatível com Windows 7, Windows 8, Windows 10 e Mac OS X ou superior.

5.65. Possuir certificação VPNC Basic Interop, ou ICSA IPSec, ou certificação equivalente que comprove interoperabilidade com as principais soluções de VPN IPSec do mercado?

5.66. Suportar o recurso de NAT Traversal (NAT-T) para VPNs IPSec;

5.67. Suportar a criação e túneis VPN (Virtual Private Network) Cliente-to-Site, sob o produto IPSec e L2TP.

5.68. Gerar logs de informações sobre a conexão de clientes VPN de modo que seja possível através de relatórios, contabilizar o tempo de conexão dos clientes VPN bem como o tráfego passante desta conexão.

VPN Site to site

5.69. Possuir funcionalidade e tunelamento IPSec VPN Site to Site com no mínimo 01 (uma) licença

5.70. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;

5.71. Possuir interoperabilidade com no mínimo os seguintes fabricantes de Appliance de Segurança:

5.72. Cisco;

5.73. Checkpoint;

5.74. Sophos;

5.75. Palo Alto Networks;

5.76. Fortinet;

5.77. Sonic Wall;

5.78. Suportar os padrões de IPSEC VPN abaixo:

5.78.1. 3DES, AES 128, 192 e 256;

5.78.2. MD5 and SHA-1 authentication;

5.78.3. Internet Key Exchange (IKE) algorithm.

NAT e Roteamento

5.79. Implementar recurso de NAT e PAT, permitindo a tradução simultânea de endereços IPs e portas, possibilitando inclusive NAT 1:1, N:1 e N:N.

5.80. Suportar roteamento estático e dinâmico RIP, OSPF e BGPv4;

5.81. Possuir funcionalidades de DHCP Cliente, Servidor e Relay.

5.82. Permitir roteamento baseado em política com parâmetros tais como Endereço de Origem e Destino, porta de Origem e Destino.

6. SISTEMA DE RELATÓRIOS CENTRALIZADOS

6.1. A solução deverá possuir ferramenta que permita que todos os appliances do fabricante possam centralizar seus relatórios em um equipamento para esta função.

6.2. A solução deverá possuir ferramenta que permita que o administrador realize agendamentos destes relatórios para que estes sejam enviados via e-mail para todos os e-mails cadastrados.

6.3. A solução deverá possuir ferramenta que permita ter relatórios customizados e em compliance com pelo menos estes órgãos: HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA.

6.4. A solução deverá possuir ferramenta que permita ter fácil identificação das atividades de rede e ataques em potencial.

6.5. A solução deverá possuir ferramenta que permita armazenar histórico dos relatórios em disco local, já licenciada, no mínimo de 100 GBytes, sem custo adicional.

6.6. A solução deverá possuir ferramenta que permita extrair relatórios únicos para cada um dos módulos ofertados pela solução.

6.7. A solução deverá possuir ferramenta que permita gerar multi formatos de relatórios, pelo menos tabular e gráfico.

6.8. A solução deverá possuir ferramenta que permita exportar relatórios para: PDF, Excel e HTML.

6.9. A solução deverá possuir ferramenta que permita gerar relatórios sobre as pesquisas realizadas pelos usuários nos principais buscadores: Yahoo, Bing, Wikipedia, Rediff,eBay.

6.10. A solução deverá possuir ferramenta que permita gerar relatórios que informem principais atividades em cada módulo.

6.11. A solução deverá possuir ferramenta que permita ter logs em tempo real.

6.12. A solução deverá possuir ferramenta que permita ter logs arquivados para consulta posterior.

6.12.1. A solução deverá possuir ferramenta que permita que o administrador consiga realizar pesquisas dentro dos logs arquivados.

6.13. A solução deverá possuir ferramenta que permita gerar logs de auditoria.

6.14. A solução deverá possuir ferramenta que permita ter sua gerencia totalmente baseada em acesso web.

6.15. A solução deverá possuir ferramenta que permita que o administrador crie regras baseadas em usuários onde cada usuário criado poderá ter acesso a funcionalidades especificas na ferramenta.

6.16. A solução deverá possuir ferramenta que permita múltiplas dashboards onde deve-se haver uma exclusivamente para os relatórios e outro exclusivamente para tratar dos recursos e saúde do appliance.

6.17. A solução deverá possuir ferramenta que permita agrupamento dos equipamentos por tipo do dispositivo e modelo do equipamento.

6.18. A solução deverá possuir ferramenta que permita o administrador poder acessar estes relatórios de qualquer lugar através de apenas um navegador.

6.19. A solução deverá possuir ferramenta que permita o gerenciamento somente de appliances favoritos.

6.20. A solução deverá possuir ferramenta que permita total gerencia sobre a retenção dos dados armazenados neste equipamento.

6.21. A solução deverá possuir ferramenta que permita ter disponibilidade em appliance virtual e software caso necessário instalar o appliance em um hardware baseado em intel.

6.21.1. A solução deverá possuir ferramenta que permita suporte no mínimo aos virtualizadores:

6.21.1.1. Vmware

6.21.1.2. Hyper-V

6.21.1.3. Citrix

6.21.1.4. KVM

6.21.2. A solução deverá possuir ferramenta que permita capacidade de armazenamento ilimitado, tendo apenas o disco como limitador e a necessidade do licenciamento adicional.

7. CENTRALIZADOR DE GERENCIAMENTO DE APPLIANCES

7.1 A solução deverá prover uma ferramenta distribuída pelo mesmo fabricante para gerenciamento centralizado de todos os appliances adquiridos pela contratante, já licenciada para até 5 appliances, sem ônus adicional para a CONTRATANTE.

7.2. A solução de gerenciamento deverá permitir que o administrador da ferramenta possa criar políticas de gerenciamento para um ou mais equipamentos e aplica-los todos de uma única vez.

7.2.1. As políticas de configurações devem ter no mínimo as seguintes opções:

7.2.1.1. Proteção e políticas de acesso web

7.2.1.2. Controle de aplicativos

7.2.1.3. IPS

7.2.1.4. VPN

7.2.1.5. E-mail

7.2.1.6. Firewall

7.3. A solução deverá oferecer funcionalidade que permita o administrador criar tamplates de configuração para que o administrador possa aproveitar as mesmas regras para novos appliances.

7.4. Deverá haver na dashboard da solução, indicadores que permitam o administrador avaliar a saúde do equipamento de uma maneira fácil para visualização.

7.5. Possuir múltiplas formas de customização de warning thresholds.

7.6. Possuir flexibilização na hora da criação de grupos de appliances gerenciados, sendo possível diferencia-los como por exemplo: Região, modelo e ou outros parâmetros.

7.7. Deverá possuir funcionalidade que permita o administrador delegar funções para diferentes técnicos com diferentes funções.

7.8. Possuir logs de todas as alterações para que seja possível realizar o rollback das alterações realizadas caso necessário.

7.9. Deve ser possível integrar tanto com appliances físicos quanto virtuais.

7.10. Possuir funcionalidade que permita o centralizador de gerencia, também gerenciar os updates de firmware de todos os appliances.

7.11. O gerenciador poderá ser oferecido como hardware appliance oferecido pela fabricante, virtual, onde permite a contratante instalar ele em um ambiente virtual e software, permitindo o software ser instalado em um hardware baseado em intel.

7.12. Poder gerenciar até 1000 appliances em uma única console, mediante licenciamento adicional ao licenciamento inicial de 5 appliances, já incluso na solução.

8. DOS SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO

8.1. A solução deverá ser fornecida, instalada, otimizada, testada e documentada de acordo com Projeto de Instalação e Configuração, que deverá ser elaborado pela CONTRATADA.

8.1.1. O projeto deverá ser revisado e aprovado pelo fabricante da solução.

8.1.2. O projeto deverá ser aprovado pelo CONTRATANTE.

8.2. São atividades inerentes a instalação e configuração, as quais devem ser executadas pela CONTRATADA:

8.2.1. Elaboração da documentação, contendo no mínimo os seguintes itens:

8.2.1.1. Cronograma;

8.2.1.2. Levantamento de informações sobre o ambiente atual;

8.2.1.3. Definição dos parâmetros de configuração básicos e avançados a serem implementados;

8.2.1.4. Mapa de rede contendo a topologia a ser implementada ou atualizada;

8.2.1.5. Gerenciamento de mudanças, contemplando análise de riscos de implementação da solução;

8.2.1.6. Procedimentos de implementação e de rollback no caso de problemas não previstos previamente.

8.2.2. Elaboração de procedimento de implementação/atualização e procedimento de recuperação de falhas (backup e restore) da solução.

8.2.3. Definição da arquitetura de rede e segurança de:

8.2.3.1. Firewall;

8.2.3.2. VPNs;

8.2.3.3. Segmentação da rede;

8.2.3.4. Redes de serviço;

8.2.3.5. Perímetro Internet.

8.2.4. Definição dos parâmetros de configuração de:

8.2.4.1. Políticas e regras de segurança;

8.2.4.2. Zonas de segurança;

8.2.4.3. Objetos de firewall;

8.2.4.4. Políticas e regras de VPN;

8.2.4.5. Políticas e regras de prevenção e detecção de intrusos;

8.2.4.6. Usuários privilegiados para operação e administração.

8.2.5. Instalação física dos equipamentos em local a ser definido pelo contratante, incluindo os componentes necessários: cabeamento, braços, conectores SFP+/XFP, etc.

8.2.6. Configuração de NAT/PAT, DNS, endereçamento IP e roteamento estático e dinâmico.

8.2.7. Configuração de regras para SMTP, WEB, FTP, Telnet, conexões de banco de dados e outros serviços solicitados durante a fase de planejamento.

8.2.8. Configuração de endereços IPs virtuais, políticas de alta-disponibilidade, roteamento simétrico/assimétrico e sincronismo das configurações dos firewalls de rede.

8.2.9. Deverá ser realizada configuração de todas as funcionalidades presentes na Solução, mesmo as que não constam explicitamente como requisitos neste documento.

8.2.10. Otimização das regras e objetos de segurança da solução implantada, objetivando a redução do número de políticas de segurança e ganhos de desempenho.

8.2.11. Configuração de alarmes e notificações automatizadas via SNMP e/ou SMTP e/ou SMS.

8.2.12. Integração com a ferramenta de correlação de eventos, caso exista, para coleta, monitoramento e correlação de registros de segurança da informação.

8.2.13. Integração com ferramenta de monitoramento via SNMP, caso exista.

8.2.14. Teste e homologação da solução implantada.

8.2.15. Documentação AS-BUILT, contendo planejamento, relatório de instalação, configuração adotada, testes realizados e seus resultados.

8.2.16. Elaboração dos planos de recuperação de desastres, bem como testes para validação do plano.

8.2.17. Repasse de tecnologia realizado durante a implementação para a equipe técnica do CONTRATANTE, realizado in loco e no ambiente implantado, com o objetivo de prover informações suficientes para supervisão e gestão do ambiente.

8.2.18. As despesas de viagem, hospedagem, alimentação e demais para execução dos serviços correrão por conta da CONTRATADA.

8.2.19. Os serviços de instalação e configuração deverão ser prestados por técnico da CONTRATADA certificado pelo fabricante da solução. Durante todo o período da etapa de instalação e configuração, o fabricante deverá disponibilizar, mesmo que remotamente, equipe técnica para esclarecimento de dúvidas, validação das configurações pretendidas e aplicadas, além de resolução de problemas.

9. DO TREINAMENTO

9.1. A CONTRATADA deverá fornecer 2 (dois) vouchers para realização de treinamento na solução adquirida.

9.2. O treinamento deve ser um curso oficial do fabricante abrangendo todas as funcionalidades da solução.

9.3. O treinamento poderá ser dividido em módulos de acordo com as funcionalidades disponíveis.

9.4. O treinamento deverá ser ofertado em Português e o material didático deverá ser em Português ou Inglês.

9.5. O material didático impresso deve ser oficial, sendo uma unidade para cada participante.

9.6. Deverá ser fornecido certificado System Engineer para cada participante que obtiver pelo menos 80% (oitenta por cento) de frequência e acertos nas avaliações/exames de conhecimento.

9.7. As despesas inerentes ao treinamento – local, instrutor, coffe-break, material, equipamentos, entre outros - são de responsabilidade da CONTRATADA.

10. DOS SERVIÇOS DE GARANTIA, ASSISTÊNCIA TÉCNICA E SUPORTE TÉCNICO.

10.1. A Contratada deverá prestar serviços de garantia, assistência técnica e suporte técnico, através do fabricante da Solução, em todos os produtos fornecidos, pelo período de 36 (trinta e seis) meses, a contar da data do recebimento definitivo dos produtos e serviços, compreendendo, entre outros:

10.1.1. Manutenção corretiva de hardware dos produtos fornecidos, incluindo a reparação de eventuais falhas, mediante a substituição de peças e componentes por outros de mesma especificação, novos de primeiro uso e originais, de acordo com os manuais e normas técnicas específicas para os mesmos;

10.1.2. Atualizações corretivas e evolutivas de software e firmware, incluindo pequenas atualizações de release, reparos de pequenos defeitos (bug fixing patches);

10.1.3. Ajustes e configurações conforme manuais e normas técnicas do fabricante; 6.1.4. Demais procedimentos destinados a recolocar os equipamentos em perfeito estado de funcionamento;

10.1.4. Assistência técnica especializada para investigar, diagnosticar e resolver incidentes e problemas relativos aos produtos fornecidos;

10.1.5. Fornecimento de informações e esclarecimentos de dúvidas sobre instalação, administração, configuração, otimização ou utilização dos produtos adquiridos.

10.2. A garantia de 36 (trinta e seis) meses, para todos os componentes ofertados na proposta, deverá ser comprovada pelo fabricante do equipamento (por meio de site, portal ou documentação).

10.3. Os serviços de garantia, assistência técnica e suporte técnico deverão ser prestados 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, 365 (trezentos e sessenta e cinco) dias por ano, no local onde os equipamentos se encontrarem instalados (on-site), por técnicos devidamente habilitados e credenciados pelo fabricante, com nível de certificação compatível com as atividades a serem executadas, e sem qualquer ônus adicional.

10.4. A Contratada deverá disponibilizar canal de atendimento para abertura de chamados técnicos, mediante número 0800 ou número local (nas cidades onde se encontrarem instalados os equipamentos). Adicionalmente, poderá ser disponibilizado serviço de abertura de chamado via site ou e-mail.

10.5. Para cada chamado técnico, a Contratada deverá informar um número de controle (protocolo) para registro, bem como manter histórico de ações e atividades realizadas.

10.6. Os chamados técnicos serão classificados por criticidade, de acordo com o impacto no ambiente computacional, conforme abaixo:

10.6.1. **PRIORIDADE ALTA:** Sistema indisponível ou com severa degradação de desempenho;

10.6.2. **PRIORIDADE MÉDIA**: Sistema disponível, com mau funcionamento, que importe baixa degradação de desempenho ou comprometimento em um de seus elementos que importe em risco para a disponibilidade do sistema.

10.6.3. **PRIORIDADE BAIXA:** Sistema disponível, sem impacto em seu desempenho ou disponibilidade; consultas gerais sobre instalação, administração, configuração, otimização, troubleshooting ou utilização.

10.7. O nível de severidade será informado pelo CONTRATANTE no momento da abertura do chamado.

10.8. O CONTRATANTE poderá escalar os chamados para níveis mais altos ou baixos, de acordo com a criticidade do problema. Nesse caso, os prazos de atendimento e de solução, bem como os prazos e percentuais de multa, serão automaticamente ajustados para o novo nível de prioridade.

10.9. Os serviços de suporte e assistência técnica em garantia deverão atender, respectivamente, os seguintes prazos de atendimento inicial e solução do incidente:

10.9.1. Os chamados de **PRIORIDADE ALTA** deverão ser atendidos em até 30 (trinta) minutos e solucionados em até 2 (duas) horas;

10.9.2. Os chamados de **PRIORIDADE MÉDIA** deverão ser atendidos em até 1 (uma) hora e solucionados em até 4 (quatro) horas;

10.9.3. Os chamados de **PRIORIDADE BAIXA** deverão ser atendidos em até 2 (duas) horas e solucionados em até 48 (quarenta e oito) horas.

10.10. O prazo de atendimento começará a ser contado a partir da hora do acionamento do suporte a partir da Central de Atendimento da CONTRATADA.

10.11. Entende-se por início de atendimento a hora de chegada do técnico de suporte ao local onde está o produto ou a intervenção remota.

10.11.1. Caso não seja possível a intervenção remota, seja por impossibilidade de comunicação, seja por impossibilidade de análise do problema, um técnico da CONTRATADA deverá realizar o atendimento on-site, obrigatoriamente.

10.12. Entende-se por término do atendimento a ocorrência de um dos eventos abaixo relacionados:

10.12.1. Solução definitiva;

10.13. Solução de contorno e escalonamento do chamado para um nível de menor severidade, mediante prévia aprovação do CONTRATANTE;

10.14. Solução de contorno e escalonamento do chamado para o fabricante, em caso de correção de falhas (bugs) ou da liberação de novas versões e patches de correção, desde que comprovados pelo fabricante da solução. Para esses problemas, a CONTRATADA deverá restabelecer o ambiente, através de uma solução paliativa, informando o CONTRATANTE em um prazo máximo de 24 (vinte e quatro) horas quando a solução definitiva será disponibilizada.

10.15. A solução definitiva deverá ser disponibilizada no prazo máximo de 60 (sessenta) dias úteis, no caso da necessidade de criação de um patch/fix.

10.16. O encerramento do chamado será dado por servidor da Contratante na conclusão dos serviços, após a disponibilização da solução para uso em perfeitas condições de funcionamento no local onde está instalada.

10.17. Caberá aos técnicos do fabricante ou da empresa autorizada pelo fabricante identificar os componentes, peças e materiais responsáveis pelo mau funcionamento dos produtos fornecidos.

10.18. Em caso de falhas irrecuperáveis de hardware ou impossibilidade de solução pela assistência técnica, a CONTRATADA deverá providenciar a troca por equipamento idêntico.

10.18.1. Casos em que se tornará obrigatória a substituição de equipamentos pela CONTRATADA:

10.18.1.1. Falha de hardware e/ou software que interrompa o funcionamento do equipamento por mais de 12 (doze) horas consecutivas;

10.19. Inoperância do equipamento, por tempo superior a 2 (duas) horas, em 2 (duas) ocasiões separadas por, no máximo, um período de 60 (sessenta) dias corridos.

10.19.1. Por questão de segurança, os equipamentos e softwares nunca deverão ser removidos das dependências da CONTRATANTE sem a remoção de dados ou regras sigilosas.

10.19.2. No caso de troca do produto por defeito, não haverá qualquer ônus adicional para o CONTRATANTE.

10.20. Relativamente à manutenção corretiva de hardware e software:

10.20.1. Os componentes danificados deverão ser substituídos, entregues, instalados e configurados, de modo a deixar o equipamento em perfeitas condições de uso e com todas as funcionalidades operacionais, nas dependências do CONTRATANTE, nos prazos de solução estabelecidos acima, sem a cobrança de quaisquer custos adicionais (frete, seguro, etc.);

10.20.2. Concluída a manutenção, a CONTRATADA fornecerá ao CONTRATANTE, documento em que conste a identificação do chamado técnico, data e hora de início e término da assistência técnica, descrição dos serviços executados, indicação da peça e/ou componente eventualmente substituído, assim como relato referente às condições inadequadas ao funcionamento do equipamento ou sua má utilização, fazendo constar a causa e as medidas para a sua correção.

10.20.3. Durante todo o período de garantia, a CONTRATADA atualizará ou disponibilizará para download, sem ônus adicionais para o CONTRATANTE, os softwares necessários ao funcionamento dos produtos fornecidos, fornecendo as novas versões ou releases lançados. Os softwares tratados neste item incluem vacinas de antivírus/anti-malware, assinaturas do filtro de conteúdo web, software de gerenciamento, firmwares de bios e drivers.

10.20.4. A atualização ou disponibilização para download deverá ocorrer em um prazo máximo de 15 (quinze) dias úteis, contados da data de lançamento da nova versão ou release. Caso a nova versão ou release seja disponibilizada para download, deverá a CONTRATADA prestar o suporte necessário para a instalação e configuração da mesma.

10.21. Qualquer manutenção e/ou intervenção por solicitação da CONTRATADA ou do fabricante, mesmo não implicando em inoperância da solução ou alteração de suas características, deverá ser agendada e acordada previamente com o CONTRATANTE.

10.22. Nos casos em que os produtos operem em alta disponibilidade a CONTRATADA e/ou fabricante deverão realizar o reparo ou troca do equipamento que apresente falha ou defeito ainda que o serviço não seja interrompido, sendo contados normalmente os prazos de atendimento.

10.23. A CONTRATADA não poderá impor qualquer limitação de quantitativo de chamados, seja diário, mensal, anual, ou de tempo de duração dos chamados, durante o período de prestação dos serviços.

10.24. O CONTRATANTE poderá acompanhar os chamados técnicos abertos pela CONTRATADA junto ao fabricante.

11. PRAZO DA ATA DE REGISTRO DE PREÇO: 12 (doze) meses.

12. PRAZO E LOCAL DE ENTREGA DO OBJETO:

12.1. O objeto contratual deverá ser entregue em conformidade com as especificações estabelecidas neste Termo de Referência, no prazo de 60(sessenta) dias, contado a partir do recebimento da nota de empenho ou instrumento hábil, no Almoxarifado Central da Prefeitura de Sobral: Rua Viriato de Medeiros, 1250, Centro, de segunda à sexta de 8:00 às 12:00 e de 13:00 às 16:00.

13. DAS DOTAÇÕES ORÇAMENTÁRIAS

13.1. As despesas decorrentes da Ata de Registro de Preços correrão pela fonte de recursos: 29.01.04.122.0101.1344.44905200.1920000000

Recursos Ordinários: Municipal

14. CONDIÇÕES DE PAGAMENTO

14.1. O pagamento advindo do objeto da Ata de Registro de Preços será proveniente dos recursos do órgão aderente ao registro de preços do SRP (Sistema de Registro de Preços) e será efetuado até 30 (trinta) dias contados da data da apresentação da nota fiscal/fatura devidamente atestada pelo gestor da contratação, mediante crédito em conta corrente em nome da contratada, preferencialmente no Itaú.

15. DAS OBRIGAÇÕES DA CONTRATADA

15.1. Responsabilizar-se pelos ônus resultantes de quaisquer ações, demandas, custos e despesas decorrentes de danos, ocorridos por culpa sua ou de qualquer de seus empregados e prepostos, obrigando-se, outrossim, por quaisquer responsabilidades decorrentes de ações judiciais movidas por terceiros, que lhe venham a ser exigidas por força de Lei, ligadas ao cumprimento do presente Edital e da Ata que vier a ser assinada;

15.4. Em nenhuma hipótese veicular publicidade ou qualquer outra informação acerca das atividades objeto deste Pregão, sem a prévia autorização da Administração da Prefeitura Municipal de Sobral;

15.5. Manter, durante a vigência da Ata de Registro de Preços, as condições de habilitação e qualificação exigidas na licitação;

15.6. Prestar esclarecimentos à Administração sobre eventuais atos ou fatos noticiados que a envolvam independentemente de solicitação.

16. DAS OBRIGAÇÕES DA CONTRATANTE

16.1. Efetuar as requisições, de conformidade com a discriminação constante deste Edital;

16.2. Prestar as informações e os esclarecimentos que venham a ser solicitados pela(s) licitante(s) vencedora(s)

16.3. Efetuar os pagamentos nas condições pactuadas.

17. DAS SANÇÕES

17.1. O descumprimento total ou parcial das obrigações assumidas pelo licitante vencedor, sem justificativa aceita pela Secretaria solicitante, resguardados os preceitos legais pertinentes, poderá acarretar, nas seguintes sanções:

a) Multa compensatória no percentual de 20% (vinte por cento), calculada sobre o valor total estimado da aquisição, pela recusa em assinar a Ata de registro de preços no prazo máximo de 05 (cinco) dias, após regularmente convocada, sem prejuízo da aplicação de outras sanções previstas no art. 87 da Lei nº. 8.666/93 e alterações;

b) Multa de mora no percentual correspondente a 0,5% (cinco décimos por cento), calculada sobre o valor total estimado da aquisição, por dia de inadimplência, mesmo que parcial, até o limite de 02 (dois) dias úteis, caracterizando inexecução parcial;

c) Multa compensatória no percentual de 20% (vinte por cento), calculada sobre o valor total estimado da aquisição, pela inadimplência além do prazo acima, caracterizando inexecução total do mesmo;

d) Advertência;

e) Suspensão temporária de participar em licitação e impedimento de contratar com a Prefeitura Municipal de Sobral por prazo de até 02 (dois) anos; e

f) Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição, ou até que seja promovida a reabilitação, perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o licitante vencedor ressarcir a Administração pelos prejuízos resultantes e após decorridos o prazo da sanção aplicada.

17.2. A aplicação das sanções previstas neste Edital não exclui a possibilidade de aplicação de outras, previstas na Lei nº. 8.666/93 e alterações, inclusive responsabilização do licitante vencedor por eventuais perdas e danos causados à Administração.

17.3. A multa deverá ser recolhida no prazo máximo de 10 (dez) dias corridos, a contar da data do recebimento da comunicação.

17.4. O valor da multa poderá ser descontado da Nota Fiscal ou crédito existente na Secretaria solicitante, em favor do licitante vencedor.

17.5. Caso o valor da multa seja superior ao crédito existente, a diferença será cobrada na forma da lei.

17.6. As multas e outras sanções aplicadas só poderão ser relevadas, motivadamente e por conveniência administrativa, mediante ato da Administração Municipal, devidamente justificado.

17.7. As sanções aqui previstas são independentes entre si, podendo ser aplicadas isoladas ou cumulativamente, sem prejuízo de outras medidas cabíveis.

17.8. Em qualquer hipótese de aplicação de sanções será assegurado ao licitante vencedor o contraditório e ampla defesa

18. DA FISCALIZAÇÃO

18.1. A execução contratual será acompanhada e fiscalizada pela Sr. **José Reinaldo Duailibe Mendonça Junior** designado para este fim pela contratante, de acordo com o estabelecido no art. 67, da Lei Federal nº 8.666/1993, a ser informado quando da lavratura do instrumento contratual.

19. PRAZO DE VIGÊNCIA E DE EXECUÇÃO DO CONTRATO

19.1. O prazo de vigência do contrato será de 12 (doze) meses, contados a partir da sua assinatura, na forma do parágrafo único, do art. 61, da Lei Federal nº 8.666/1993.

19.2. A publicação resumida do instrumento de contrato dar-se-á na forma do parágrafo único, do art. 61, da Lei Federal nº 8.666/1993.

19.3. O prazo de execução do objeto deste contrato é de 12 (doze) meses, contado a partir do recebimento da Ordem de Serviço.

19.4. O prazo de execução poderá ser prorrogado nos termos do § 1º do art. 57 da Lei Federal nº 8.666/1993.

20. DAS CONDIÇÕES DE EXECUÇÃO DOS SERVIÇOS

20.1. O serviço só estará caracterizado mediante o recebimento da Nota de Empenho e Ordem de Serviço pelo fornecedor.

20.2. O CONTRATADO ficará obrigado a atender todos os pedidos efetuados durante a vigência desta Ata de Registro de Preços, mesmo que a entrega deles decorrente estiver prevista para data posterior à do seu vencimento.

20.3. Se a qualidade do serviço não corresponder às especificações exigidas no Edital do Pregão Presencial nº 024/PMCSA-SMDET/2019 que precedeu à Ata de Registro de Preços nº 051/PMCSA-SMDET/2019, o serviço rejeitado será informado ao contratado, para que seja refeito o serviço imediatamente, independentemente da aplicação das penalidades cabíveis.

20.4. Cada serviço realizado deverá ser efetuado mediante solicitação da Secretaria solicitante, através de emissão de Nota de Empenho e Ordem de Serviço.

20.5. A cada serviço realizado deverá ser entregue a Nota Fiscal correspondente.

20.6. A empresa contratada, quando do recebimento da Ordem de Serviço feita pela requisitante, deverá colocar, na cópia que necessariamente o acompanhar, a data e a hora em que o recebeu, além da identificação de quem o recebeu.

20.7. A cópia da Ordem de Serviço referida no item anterior deverá ser devolvida para a requisitante, a fim de ser anexada aos processos correspondentes.

20.8. Manter, durante a vigência da Ata de Registro de Preços, as condições de habilitação e qualificação exigidas na licitação.

Sobral/CE, 28 de janeiro de 2020.

Pablo Parente Ribeiro Tomaz
Coordenador de Gestão das Aquisições Públicas e
Administração Patrimonial - CAPAP/SEGET

De Acordo:

Silvia Kataoka de Oliveira
Secretaria da Ouvidoria, Gestão e Transparência