# ANEXO II - ESPECIFICAÇÕES TÉCNICAS

## AQUISIÇÃO DE FIREWALL

### 1. DEFINIÇÃO DO OBJETO

Este termo de referência tem como objeto aquisição de firewall NGFW com prevenção de ameaças avançadas e suporte e garantia para 5 anos para toda solução, conforme especificações técnicas, quantidades e condições constantes deste Termo de Referência.

### 2. JUSTIFICATIVA

Atualmente, preconiza-se em sistemas de segurança uma unicidade nos processos de gerenciamento de recursos de segurança da informação, transformando a solução em um sistema ágil, integrado e com visibilidade 360 dos eventos de segurança da informação. O SESC necessita amplicar a capacidade dos equipamentos que estão por vencer devido a constante modernização de sistemas informatizados e uma crescente demanda por requisições que culminam inteferindo na plataforma de segurança existente, além de que, precisamos agregar funcionalidades que permitam amplicar o espectro de segurança na organização indo de encontro ao PDTI da organização que prevê a modernização dos sistemas de informação.

Os pilares de segurança da informação sofreram alterações na era da informação, sendo eles caracterizados pelos seguintes atributos: disponibilidade, integridade, confidencialidade, autenticidade e não-repúdio. Segurança é um processo contínuo que não se conclui. Novos tipos de ataques cibernéticos são descobertos quase que diariamente. Vulnerabilidades de softwares são divulgadas todos os dias. Os processos referentes à segurança precisam ser revistos diariamente através de relatórios e acompanhamentos, e obviamente, os softwares envolvidos com a segurança da rede de dados precisam ser atualizados na mesma velocidade.

*Firewall* é um dispositivo composto de software e/ou hardware, que limita o acesso à rede. Seu objetivo é permitir somente a transmissão e a recepção de dados autorizados na rede. O firewall pode ser usado para ajudar a impedir que, a rede ou um computador seja acessado sem autorização. Assim, é possível evitar que informações sejam capturadas ou que sistemas tenham seu funcionamento prejudicado pela ação de hackers. O firewall é um grande aliado no combate a vírus e cavalos-de-tróia, uma vez que é capaz de bloquear portas que, eventualmente, sejam usadas pelas "pragas digitais" ou então bloquear acesso a programas não autorizados.

A contratação mostra-se imprescindível em virtude da crescente demanda por segurança no acesso à rede. Atualmente são diversos tipos de ataques que são conhecidos por

profissionais de segurança, ainda conseguem obter sucesso pela não prevenção, sendo assim, o SESC tem como objetivo contratar não somente os ativos, mas o suporte e garantia da solução, mantendo a base de ameaças atualizada, garantindo assim a segurança de suas informações, o que considerado o ativo mais valioso de uma organização.

A aquisição será parcialmente custeada pelo DN através do PNI (GO-P150-38, GO-P150-44, GO-P150-50) referente aos itens que atenderão as unidades SESC Centro, SESC Faiçalville e SESC Cidadania. A aquisição dos itens que atenderão a Administração Regional será custeada pelo orçamento próprio do DR-Goiás. A contratação mostra-se imprescindível em virtude da crescente demanda por segurança no acesso à rede. Atualmente são diversos tipos de ataques que são conhecidos por profissionais de segurança, ainda conseguem obter sucesso pela não prevenção, sendo assim, o SESC tem como objetivo contratar não somente os ativos, mas o suporte e garantia da solução, mantendo a base de ameaças atualizada, garantindo assim a segurança de suas informações, o que considerado o ativo mais valioso de uma organização. A contratação mostra-se imprescindível em virtude do crescente de uso de dados, aplicações online, crescimento da utilização de mídias sociais, podendo fornecer um ganho muito grande a instituição e para nossos clientes alunos e hospedes.

## 3. DAS QUANTIDADES DEMANDADAS

| LOTE 1 | | | |
|---|---|---|---|
| **ITEM** | **DESCRIÇÃO** | **QUANTIDADE** | **UNIDADE** |
| 1 | APPLIANCE FIREWALL TIPO I COM SUPORT E GARANTIA PARA 5 ANOS | 2 | UNIDADE |
| 2 | APPLIANCE FIREWALL TIPO II COM SUPORTE E GARANTIA PARA 5 ANOS | 4 | UNIDADE |
| 3 | LICENÇA DE SOFTWARE FIREWALL TIPO I COM SUPORTE E GARANTIA PARA 5 ANOS | 2 | LICENÇA |
| 4 | LICENÇA DE SOFTWARE FIREWALL TIPO II COM SUPORTE E GARANTIA PARA 5 ANOS | 4 | LICENÇA |
| 5 | INSTALAÇÃO FIREWALL TIPO I | 2 | SERVIÇO |
| 6 | INSTALAÇÃO FIREWALL TIPO II | 4 | SERVIÇO |

### 3.1 – DAS QUANTIDADES DETALHADAS

| LOTE 1 | | | | |
|---|---|---|---|---|
| **ITEM** | **UNIDADES** | **DESCRIÇÃO** | **QNT.** | **TIPO** |
| 1 | Administração Regional | APPLIANCE FIREWALL TIPO I COM SUPORT E GARANTIA PARA 5 ANOS | 2 | PRODUTO |
| 2 | SESC Cidadania | APPLIANCE FIREWALL TIPO II COM SUPORT E GARANTIA PARA 5 ANOS | 2 | PRODUTO |
| 3 | SESC Faiçalville | APPLIANCE FIREWALL TIPO II COM SUPORT E GARANTIA PARA 5 ANOS | 1 | PRODUTO |
| 4 | SESC Centro | APPLIANCE FIREWALL TIPO II COM SUPORT E GARANTIA PARA 5 ANOS | 1 | PRODUTO |
| 5 | Administração Regional | LICENÇA SOFTWARE FIREWALL TIPO I COM SUPORTE E GARANTIA PARA 5 ANOS | 2 | LICENÇA |
| 6 | SESC Cidadania | LICENÇA SOFTWARE FIREWALL TIPO II COM SUPORTE E GARANTIA PARA 5 ANOS | 2 | LICENÇA |
| 7 | SESC Faiçalville | LICENÇA SOFTWARE FIREWALL TIPO II COM SUPORTE E GARANTIA PARA 5 ANOS | 1 | LICENÇA |
| 8 | SESC Centro | LICENÇA SOFTWARE FIREWALL TIPO II COM SUPORTE E GARANTIA PARA 5 ANOS | 1 | LICENÇA |
| 9 | Administração Regional | INSTALAÇÃO FIREWALL TIPO I | 2 | SERVIÇO |
| 10 | SESC Cidadania | INSTALAÇÃO FIREWALL TIPO II | 2 | SERVIÇO |
| 11 | SESC Faiçalville | INSTALAÇÃO FIREWALL TIPO II | 1 | SERVIÇO |
| 12 | SESC Centro | INSTALAÇÃO FIREWALL TIPO II | 1 | SERVIÇO |

## 4. DAS ESPECIFICAÇÕES TÉCNICAS OBRIGATÓRIAS/CARACTERÍSTICAS GERAIS

**4.1.** É permitido a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

**4.2.** A solução deverá ser compatível com SNMP para monitoração;

**4.3.** A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;

**4.4.** Na data da proposta e durante a vigência do contrato, nenhum dos modelos ofertados poderá estar/ser listado no site do fabricante em listas de end-of-life, end-of-support e/ou end-of-sale.

## 5. FORNECIMENTO SERVIÇO DE SOLUÇÃO PARA PROTEÇÃO DE PERÍMETRO – TIPO I

### 5.1. Características Físicas do Appliance

**5.1.1.** Suportar througput Threat Prevention 2.5 Gbps ou superior;

**5.1.2.** Suportar througput Next Generation Firewall 5.5 Gbps ou superior;

**5.1.3.** Suportar througput IPS 6.5 Gbps ou superior;

**5.1.4.** Suportar througput Firewall 12 Gbps ou superior;

**5.1.5.** Suportar througput VPN site to site de 2.7 Gbps ou superior;

**5.1.6.** Deverá suportar no mínimo 90.000 novas conexões por segundo;

**5.1.7.** Deverá suportar no mínimo 8.000.000 conexões simultâneas;

**5.1.8.** Deverá suportar os protocolos de roteamento OSPFv2, OSPFv3, BGP e RIP;

**5.1.9.** Deverá suportar Policy-based routing;

**5.1.10.** Deverá possuir pelo menos 8 (oito) interfaces 10/100/1000Base-T RJ-45;

**5.1.11.** Deverá possuir pelo menos 4 (quatro) interfaces 10GBase-F SFP+;

**5.1.12.** Deverá possuir 1 (uma) interface USB;

**5.1.13.** Deverá possuir 1 (uma) interface console serial do tipo RJ-45;

**5.1.14.** Deverá possuir pelo menos 32 GB memória RAM ou superior;

**5.1.15.** Deverá possuir pelo menos 240GB SSD storage cada Applience;

**5.1.16.** Deverá suportar Dual Stack IPv4/IPv6 e NAT64;

**5.1.17.** Deverá suportar NAT66, NAT64 e NAT46;

**5.1.18.** Deve estar licenciado todos os serviços disponíveis no appliance (Firewall, VPN Site to Site, VPN Client to Site, Application Control, Intrusion Prevention System, URL Filtering, Antivirus and Anti-Bot, SandBox);

**5.1.19.** Deve estar licenciado e suportar acesso remoto Client-to-Site ilimitado ou com a licença de maior capacidade;

**5.1.20.** Os appliances de segurança devem suportar operar em cluster ativo-ativo ou ativo-passivo sem a necessidade de licenças adicionais;

**5.1.21.** Deve ser estar licenciados todas interfaces e habilitadas para uso imediato, incluindo seus transceivers/transceptores conforme o quantitativo de interfaces/transceivers ora requisitados neste Termo de Referência;

**5.1.22.** A licitante deverá apresentar junto a proposta comercial declaração confirmando que a empresa é autorizada a revender, fornecer, instalar e configurar os equipamentos ofertados, assim como, prestar suporte e garantia. Caso não seja o fabricante a licitante deverá apresentar declaração do mesmo.

## 6. FORNECIMENTO SERVIÇO DE SOLUÇÃO PARA PROTEÇÃO DE PERÍMETRO – TIPO II

### 6.1. Características físicas do appliance

**6.1.1.** Suportar througput Threat Prevention 1.5 Gbps ou superior;

**6.1.2.** Suportar througput Next Generation Firewall 3.2 Gbps ou superior;

**6.1.3.** Suportar througput IPS 3.5 Gbps ou superior;

**6.1.4.** Suportar througput Firewall 4.8 Gbps ou superior;

**6.1.5.** Suportar througput VPN site to site de 3.2 Gbps ou superior;

**6.1.6.** Deverá suportar no mínimo 55.000 novas conexões por segundo;

**6.1.7.** Deverá suportar no mínimo 2.400.000 conexões simultâneas;

**6.1.8.** Suporte de 1.3 Gbps de thoughput com as funcionalidades de prevença de ameaças, que contempla as funcionalidades de Firewall, Controle de URL e aplicação web, IPS, Antivirus, Anti-malware e solução de prevença de ameaças avançadas (Zero-Day);

**6.1.9.** Deverá suportar os protocolos de roteamento OSPFv2, BGP e RIP.

**6.1.10.** Deverá suportar Policy-based routing.

**6.1.11.** Deverá possuir pelo menos 16 (dezesseis) interfaces 10/100/1000Base-T RJ-45.

**6.1.12.** Deverá possuir pelo menos 1 (uma) interface dedicada de 1Gb de fibra para WAN;

**6.1.13.** Deverá possuir pelo menos 1 (uma) interace dedicada de 1Gb de fibra para DMZ;

**6.1.14.** Deverá possuir 1 (uma) interface USB;

**6.1.15.** Deverá possuir 1 (uma) interface console serial do tipo RJ-45 ou USB-C, como também todos os cabos necessários para acesso na respectiva interface;

**6.1.16.** A licitante deverá apresentar junto a proposta comercial declaração confirmando que a empresa é autorizada a revender, fornecer, instalar e configurar os equipamentos ofertados, assim como, prestar suporte e garantia. Caso não seja o fabricante a licitante deverá apresentar declaração do mesmo.

### 6.2. Características das políticas de Firewall dos tipos I e II.

**6.2.1.** Deverá suportar controles por zona de segurança.

**6.2.2.** Controles de políticas por porta e protocolo.

**6.2.3.** Controle de políticas através de Geo-Localização;

**6.2.4.** Criação de políticas baseada em usuários;

**6.2.5.** Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound);

**6.2.6.** Suporte a criação de VLAN;

**6.2.7.** A solução deve suportar DHCP;

**6.2.8.** Deve suportar NAT estático e dinâmico;

**6.2.9.** Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links.

**6.2.10.** Deve suportar o balanceamento de, no mínimo, dois links;

**6.2.11.** A solução deve operar em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Bridge, camada 2 (l2) e camada 3 (l3);

**6.3. IPS dos tipos I e II.**

**6.3.1.** Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio appliance sem a necessidade de uso de quaisquer interfaces ou dispositivos externos.

**6.3.2.** Deve ser possível agendar para que o mecanismo de inspeção receba e implemente atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;

**6.3.3.** A solução de IPS deve possuir mecanismo através de poucos cliques e interface amigável, que identifica quando o equipamento está com processamento muito alto. Assim, o administrador consegue identificar e mitigar o problema, sem modificar as proteções individuais já criadas e customizadas;

**6.3.4.** Caso o equipamento não tenha conexão a Internet, deve ser possível realizar de forma manual a importação do pacote de atualização das assinaturas através do proprio equipamento;

**6.3.5.** Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo pelo menos, os seguintes ataques conhecidos: SQL Injection, ICMP Denial of Service, força a bruta a scanning de portas CIFS, Port overflow, Non Compliant DNS, Non Compliant SMTP, Non Compliant CIFS, Non Compliant MS-SQLServer, IKE aggressive Exchange;

**6.3.6.** Deve ser capaz de bloquear tráfego SSH em DNS tunneling;

**6.3.7.** A solução deverá ser capaz de inspecionar e proteger apenas hosts internos ou inspecionar todo o tráfego;

**6.3.8.** Solução deve proteger contra ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning);

**6.3.9.** A solução deverá possuir dois perfis pré-configurados de fábrica para uso imediato e permitir a customização de um perfil;

**6.3.10.** Em cada proteção de segurança, deve estar incluso informações como: categoria, tipo de impacto na ferramenta, severidade, e tipo de ação que a mesma irá executar;

**6.3.11.** Deve criar regras de exceção no IPS para que a assinatura não faça a inspeção de um tráfego específico por Proteção, origem, destino, serviço ou porta;

**6.3.12.** Deve ser possível visualizar a lista de proteções disponíveis no appliance com os detalhes

**6.4. Controle de Aplicação e URL Filtering dos tipos I e II.**

**6.4.1.** A solução deverá contar com ferramentas de visibilidade e controle de aplicações WEB e Filtro URL integrada no próprio appliance de segurança que permite a criação de políticas de liberação ou bloqueio baseando-se em aplicações WEB e URL;

**6.4.2.** A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser realizada através do gerenciamento dedicado;

**6.4.3.** Deve ser possível configurar através de poucos cliques e interface amigável o bloqueio a sites e aplicações que representem um risco de segurança e estão categorizadas como spyware, phishing, botnet, spam, anonymizer ou hacking;

**6.4.4.** Deve ser possível configurar através de poucos cliques e interface amigável o bloqueio a sites com conteúdo inapropriado como sexo, violência, armas, jogos e álcool;

**6.4.5.** Deve configurar regras para permitir ou bloquear aplicações ou páginas da Internet por:

**6.4.5.1.** Usuário do Active Directory

**6.4.5.2.** IP

**6.4.5.3.** Rede

**6.4.6.** Deve ser possível configurar através de poucos cliques e interface amigável o bloqueio de compartilhamento de arquivos com origem usualmente ilegais como aplicações torrents e peer-to-peer;

**6.4.7.** Deve ser possível configurar manualmente o bloqueio de aplicações ou categorias de sites de aplicações indesejadas;

**6.4.8.** Deve ainda ser possível adicionar uma URL ou aplicação que não está na base de dados;

**6.4.9.** Deve ser possível limitar o consumo de banda por download e upload baseado nas aplicações;

**6.4.10.** Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linkedin, twitter, gmail, dropbox, whatsapp, etc;

**6.4.11.** Na própria interface de gerência web deve ser possível realizar a recategorização de uma URL.

**6.4.12.** A base de aplicações deve ser superior a 4100 aplicações e aproximadamente 60 milhões de URLs categorizadas;

**6.4.13.** Deve ser possível customizar e também definir a frequência com que serão exibidas as mensagens para os usuários nas seguintes ações:

**6.4.13.1.** Aceitar e informar

**6.4.13.2.** Bloquear e informar

**6.4.13.3.** Perguntar

**6.5. Identificação de Usuários dos tipos I e II.**

**6.5.1.** A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logging;

**6.5.2.** A solução deve possibilitar ao administrador realizar a integração com o AD através de um assistente de configuração na própria interface gráfica do produto;

**6.5.3.** A solução deve identificar usuários das seguintes fontes:

**6.5.3.1.** Active Directory - o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;

**6.5.3.2.** Autenticação via navegador - Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;

**6.5.4.** A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

**6.5.5.** Na integração com o AD, a operação de cadastro deve ser realizada na própria interface web de gerência, de maneira simples e sem utilização de scritps de comando;

**6.6. Funcionalidades de prevenção de ameaças dos tipos I e II.**

**6.6.1.** A solução deve incluir ferramenta própria ou solução de terceiros para mitigar / bloqueio a comuniação entre os hosts infectados com bot e operador remoto;

**6.6.2.** A solução deve bloquear arquivos potencialmente maliciosos infectados com vírus;

**6.6.3.** A solução de proteção contra vírus e bot devem compartilhar a mesma política para facilitar o gerenciamento;

**6.6.4.** As proteções devem ser ativadas baseadas em critério de nível de confiança, ações da proteção e impacto de performance;

**6.6.5.** Deve ser possível habilitar a trilha das proteções para não logar, criar um log ou gerar um alerta;

**6.6.6.** Deve ser possível que o mecanismo de inspeção receba e implemente atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;

**6.6.7.** Deve ser possível criar regras de exceção para que a engine não faça a inspeção de um tráfego específico por escopo, proteção e definir a ação e log para cada uma delas;

**6.6.8.** A solução de Anti-Virus deve suportar protocolos HTTP, SMTP, POP3, IMAP e FTP em qualquer porta;

**6.6.9.** Deve ser possível definir uma política de inspeção para os tipos de arquivos por:

**6.6.9.1.** Inspecionar tipos de arquivos conhecidos que contém malware;

**6.6.9.2.** Inspecionar todos os tipos de arquivos;

**6.6.9.3.** Inspecionar tipos de arquivos de famílias específicas;

**6.6.10.** Deve bloquear acesso a URLs com malware.

**6.6.11.** Deve ser possível customizar a página exibida para o usuário quando a URL contiver um malware e o acesso for bloqueado.

**6.6.12.** Deve suportar referencia cruzada com CVE;

**6.7. Funcionalidades de VPN Site to Site dos tipos I e II.**

**6.7.1.** A solução deve prover acesso seguro criptografado entre dois sites através da Internet;

**6.7.2.** A solução deve estabelecer VPN com o site remoto do próprio fabricante ou de terceiros;

**6.7.3.** A solução deve suportar autenticação com senha ou certificado;

**6.7.4.** Deve suportar criptografia AES 128 e 256;

**6.7.5.** Deve possuir mecanismo para monitorar a saúde do túnel remoto;

**6.7.6.** Quando o túnel for estabelecido entre dispositivos do mesmo fabricante este deve possuir protocolo proprietário para testar se o túnel está ativo;

**6.7.7.** A solução deve suportar DPD (Dead Peer Detection) para minimizar a quantidade de mensagens trocadas para verificar a disponibilidade do Peer;

**6.7.8.** A solução deve suportar CA Externa de terceiros;

**6.7.9.** Permitir através da Gerência web a criação e utiização de certificados para acessos VPN site-to-site;

**6.8. Funcionalidades de prevenção de ameaças avançadas (Zero-Day) dos tipos I e II.**

**6.8.1.** Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;

**6.8.2.** O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;

**6.8.3.** Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise;

**6.8.4.** Deve suportar a inspeção de arquivos trafegados nos protocolos HTTP, SMTP, POP3 e IMAP;

**6.8.5.** O sistema de análise “In Cloud” ou local deve prover informações através dos logs sobre as ações do malware no sistema operacional do ambiente de Sandboxing, contendo nome do artefato, e outras informações que podem definir o tipo de ataque que foi realizado;

**6.8.6.** Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar), Zip, RAR, TGZ e 7-ZIP no ambiente de sandbox;

**7. SUPORTE E GARANTIA**

**7.1. PARA O HARDWARE:**

**7.1.1.** A CONTRATADA deverá oferecer garantia mínima de 60 (sessenta) meses para todos os itens que fazem parte da solução, contados a partir da entrega dos equipamentos. A garantia deverá ser do fabricante.

**7.1.2.** A garantia inclui a substituição dos componentes da solução com defeitos de fabricação no prazo máximo de 72 (setenta e duas) horas a contar da comunicação do fato, sem qualquer ônus para o CONTRATANTE. Neste caso, as novas unidades empregadas na substituição das defeituosas ou danificadas deverão ter prazo de garantia igual ou superior ao das substituídas.

**7.1.3.** A CONTRATADA deverá fornecer suporte técnico pelo período de 60 (sessenta) meses, nas seguintes condições:

**7.1.4.** Atendimento 24 horas por dia, 7 dias por semana, inclusive feriados;

**7.1.5.** O suporte técnico será acionado em caso de quaisquer indisponibilidades da solução, devendo haver o atendimento inicial no prazo máximo de 1(uma) hora contados a partir

da abertura do chamado para casos críticos (severidade máxima), prazo máximo de 04 (quatro) horas para casos com severidade média, e o fechamento do mesmo em até 72 (setenta e duas) horas;

**7.1.6.** O suporte técnico será acionado em caso de dúvidas no funcionamento e quaisquer problemas que não prejudiquem a operação normal do equipamento, mas que exijam intervenção técnica. Nesse caso, o atendimento inicial deverá ser realizado no prazo máximo de 6 (seis) horas a partir da abertura do chamado;

**7.1.7.** Havendo necessidade de atendimento local, este deverá ser realizado em até 96 (noventa e seis) horas a partir da abertura do chamado.

**7.1.8.** Durante o período de garantia a CONTRATADA executará, sem ônus adicionais, correções de bugs de hardware e/ou software;

**7.1.9.** A CONTRATADA deverá fornecer durante o período de garantia acesso a:

**7.1.10.** Atualizações de versão e releases dos softwares e firmwares que fazem parte da solução fornecida;

**7.1.11.** Atualizações das bases de assinaturas da funcionalidade de todos os módulos de segurança;

**7.1.12.** As ferramentas e equipamentos necessários à manutenção serão de responsabilidade da CONTRATADA.

**7.2. PARA LICENCIAMENTO DE SOFTWARE:**

**7.2.1.** A CONTRATADA deverá oferecer garantia mínima de 60 (sessenta) meses para todos os itens que fazem parte da solução, contados a partir da entrega dos equipamentos. A garantia deverá ser do fabricante.

**7.2.2.** Para licenciamento de software a CONTRATADA deverá apresentar carta do fabricante confirmando que é revenda autorizada de software de licenciamento, inclusive para médias e grandes organizações e que possui autorização para comercialização e suporte da solução ofertada, estando apta a fornecer e prestar garantia e suporte (on-site).

**7.2.3.** Para serviço de suporte técnico:

**7.2.3.1.** Os serviços deverão ser executados por técnicos da CONTRATADA, no mínimo capacitados com os certificados em nível de especialista e 2 anos de experiência, de acordo com o serviço ou produto que necessitar de suporte.

**7.2.3.2.** A CONTRATADA terá prazo de um ano para prover certificação aos seus profissionais, sempre que houver atualização de versão dos produtos, ou sempre

que o fabricante disponibilizar nova certificação para determinado produto ou serviço que faça parte da solução ofertada para o SESC.

## 8. CRITÉRIO DE JULGAMENTO

**8.1.1.** Observadas as demais condições deste Termo de Referência, o julgamento desta licitação será feito pelo critério menor preço por Lote.

**8.1.2.** Justificamos a contratação do certame em MENOR VALOR POR LOTE devido à sua necessidade de integração e sua interdependência, ou seja, a exigência de compatibilidade entre as partes e gestão integrada das entregas para garantir o seu funcionamento, dado que a sua implementação é bastante complexa.

**8.1.3.** A contratação por MENOR VALOR POR LOTE torna-se imprescindível, pois tecnicamente e gerencialmente é inviável que todos os serviços sejam fornecidos por diferentes CONTRATADAS, uma vez que traz ônus direto de maior custo gerencial para controle do Sesc-Go, além do maior custo gerencial para gestão contratual, constituindo todos estes benefícios em vantagem técnica.

**8.1.4.** Além do supramencionado, no modelo de atendimento adotado, a não-separação em itens distintos se deu devido à necessidade de ser uma solução completamente integrada que possa tratar as especificidades de cada um dos itens de acordo com as suas métricas, acordos de nível de serviço, especialização de equipes de profissionais, regime de atendimento, além da específica contribuição de cada item para o resultado final da contratação. Neste sentido, o objeto possui características de dependências entre os serviços a serem prestados, sendo certo que seu parcelamento aumentaria os riscos de execução insatisfatória do serviço.

**8.1.5.** A aquisição em MENOR VALOR POR LOTE embasa-se no Parecer nº 2086/00, elaborado no Processo nº 194/2000 do TCDF, da lavra do Professor Jorge Ulisses Jacoby Fernandes, o qual ensina que “a regra do parcelamento deve ser coordenada com o requisito que a própria lei definiu: só se pode falar em parcelamento quando há viabilidade técnica para sua adoção. (...) Um exame atento dos tipos de objeto licitados pela Administração Pública evidência que embora sejam divisíveis, há interesse técnico na manutenção da unicidade, da licitação ou do item da mesma. Não é, pois, a simples divisibilidade, mas a viabilidade técnica que dirige o processo decisório. (...) Se um objeto, divisível, sob o aspecto econômico for mais vantajoso, mas houver inviabilidade técnica em que seja licitado em separado, de nada valerá a avaliação econômica. Imagine-se ainda esse elementar exemplo do automóvel: se por exemplo as peças isoladamente custassem mais barato, mesmo assim, seria recomendável o não

parcelamento, pois sob o aspecto técnico é a visão do conjunto que iria definir a garantia do fabricante, o ajuste das partes compondo todo único, orgânico e harmônico". Segundo Marçal Justen Filho, "a obrigatoriedade do fracionamento respeita limites de ordem técnica e econômica. Não se admite o fracionamento quando tecnicamente isso não for viável ou, mesmo, recomendável. O fracionamento em lotes deve respeitar a integridade qualitativa do objeto a ser executado. (...) a unidade do objeto a ser executado não pode ser destruída através do fracionamento" (JUSTEN FILHO, Marçal. Comentários à Lei de Licitações e Contratos Administrativos. 11.ed. Brasília: 2005, Dialética.

**8.1.6.** Carvalho Carneiro esclarece acerca do conceito de viabilidade técnica e econômica, informando que "a viabilidade técnica diz respeito à integridade do objeto, não se admitindo o parcelamento quando tal medida implicar na sua desnaturação, onde em risco a satisfação do interesse público em questão" (CARNEIRO, Daniel Carvalho. O parcelamento da contratação na lei de licitações. Revista Diálogo Jurídico, ano IV, n.3., setembro/2004, p.85/95).

**8.1.7.** Quando analisado sob os aspectos técnicos vemos configurado o relacionamento e a interdependência entre produtos e os serviços a serem contratados, onde não se faz possível estabelecer os limites, por serem extremamente tênues, de onde se iniciam e terminam as repercussões entre um e outro, especialmente por se ter como meta alcançar a maturidade, a disponibilidade e a gestão de riscos de um mesmo ambiente, para o qual cada item contribuirá em aspectos distintos, sendo respectivamente, a sua sustentação, o atendimento aos usuários e melhoria contínua dos ambientes, bem como a garantia de entrega de informação com qualidade e a disponibilização de ferramentas de inteligência de negócio para os gestores e usuário.

**8.1.8.** Para a adequada execução dos serviços ora contratados é fundamental que esteja assegurada a unidade conceitual de todas as etapas técnicas, direcionado para o resultado esperado, que é a disponibilidade do ambiente sistêmico, englobando todos os aspectos necessários ao pleno atendimento das necessidades dos usuários desta instituição.

**8.1.9.** Ressalta-se que não há restrição de competitividade ao realizar o agrupamento tal como definido aqui, uma vez que os fornecedores do produto e serviços são habilitados a atender a todos os itens especificados.

**8.1.10.** Dada a necessidade de completa integração entre as partes da solução, o objeto possui características de maiores dependências entre alguns produtos e serviços a serem prestados, sendo certo que um maior parcelamento aumentaria os riscos de execução

insatisfatória do serviço, podendo comprometer o funcionamento da solução que se pretende obter.

**8.1.11.** Concluindo-se que todos os componentes da solução pretendida deverão ser fornecidos em MENOR VALOR POR LOTE. Nesse sentido, a opção da CONTRATANTE, em respeito à legislação vigente e na busca pela economicidade, optou por garantir a integração dos componentes da solução a partir da implantação e execução do projeto. Dessa forma, há garantia de que todos os serviços prestados terão compatibilidade nas devidas execuções.

## 9. LOCAL DE ENTREGA, FATURAMENTO E INSTALAÇÃO

### 9.1. LOCAL DE FATURAMENTO

**Razão Social:** SERVICO SOCIAL DO COMERCIO - SESC

**CNPJ:** 03.671.444/0001-47 **I.E.:** Isento

Endereço: Rua 19 Nº 260, Centro, Goiânia, Goiás. CEP: 74030-090.

### 9.2. LOCAL DE ENTREGA E INSTALAÇÃO

**9.2.1.** A entrega, de produtos e serviços, deverá ser realizada, em até 90 dias corridos, em horário comercial, mediante agendamento prévio, na Gerência de Tecnologia da Informação – SESC, Endereço: Rua 31-A, Nº 43, Bloco C, Setor Aeroporto, Goiânia, Goiás, CEP: 74075-470, (62) 3219-5180. A entrega deverá ser feita somente ao servidor (a) responsável, indicado pelo Gestor do Contrato no ato do agendamento.

**9.2.2.** A Instalação deverá acontecer em até 30 dias corridos após a entrega dos produtos.

## 10. DA SUBCONTRATAÇÃO

**10.1.** A contratada não poderá transferir a terceiros, por qualquer forma, nem mesmo parcialmente, as obrigações assumidas, nem subcontratar qualquer das prestações a que está obrigada.

## 11. EXIGENCIAS DE HABILITAÇÃO

**11.1.** Documentos relativos à HABILITAÇÃO JURÍDICA

**a)** Ato Constitutivo, Estatuto ou Contrato Social em vigor, devidamente registrado, em se tratando de sociedades comerciais, e no caso de sociedades por ações, acompanhado dos documentos de eleição dos seus administradores e respectivas alterações, se houver, podendo ser substituídos por certidão simplificada expedida pela Junta Comercial da sede da licitante; ou,

**b)** Comprovante de inscrição do Ato Constitutivo, no caso de sociedades civis, acompanhada de prova da diretoria em exercício. Este documento poderá ser substituído por certidão, em breve relatório, expedida pelo Registro Civil das Pessoas Jurídicas.

**c)** Documento comprobatório do representante legal da licitante:

**1.** Cópia da cédula de identidade do representante legal.

**2.** Procuração, caso a licitante se faça representar por procurador.

**11.2.** Documentos relativos à REGULARIDADE FISCAL

**a)** Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ) do Ministério da Fazenda – CNPJ/MF, cujo ramo de atividade seja compatível com o objeto da presente licitação;

**b)** Prova de inscrição no Cadastro de Contribuintes Estadual e/ou Municipal relativo ao domicilio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

**c)** Certidão Conjunta Negativa ou Positiva com Efeitos de Negativa, de Débitos Relativos a Tributos Federais e à Dívida Ativa da União, que abrange inclusive as contribuições sociais;

**d)** Certidão Negativa de Tributos Estaduais, ou Positiva com Efeitos de Negativa;

**e)** Certidão Negativa de Tributos Municipais, ou Positiva com Efeitos de Negativa;

**f)** Certidão de Regularidade Fiscal (CRF) junto ao Fundo de Garantia por Tempo de Serviço (FGTS), no cumprimento dos encargos instituídos por lei (exceto para o Empresário Individual-MEI);

**11.3.** Documentos relativos à QUALIFICAÇÃO TÉCNICA

**11.3.1.** Comprovação de aptidão para o desempenho de atividade pertinente e compatível com o objeto da licitação, por meio da apresentação de 01 (um) ou mais atestados fornecidos por pessoa jurídica, no mínimo 12 (doze) meses, de direito público ou privado, no qual conste a prestação de serviço e/ou a realização de fornecimento da mesma natureza ou similar ao objeto aqui licitado. O atestado deverá conter informações que permitam á identificação correta do contratante e do prestador do serviço, tais como:

a) Nome, CNPJ e endereço do emitente da certidão;

b) Nome, CNPJ e endereço da empresa que prestou o serviço ao emitente; e

c) Identificação do signatário (nome, cargo ou função que exerce junto à emitente).

d) Prestação de serviços de suporte técnico à solução de FIREWALL, em ambiente corporativo, na modalidade 24 x 7 (vinte e quatro horas, sete dias por semana).

**11.3.2.** Entende-se por atividade pertinente e compatível com o objeto da licitação o fornecimento de pelo menos 50% do total exigido neste Termo de Referência.

**11.3.3.** Declaração do fabricante junto a proposta comercial informando que os profissionais da licitante a serem alocados no atendimento ao SESC possuem experiência na execução de suporte técnico à solução de Firewall com IPSEC VPN, Advanced Networking and Clustering, Application Control, URL Filtering, Data Loss Prevention, IPS, Anti-Virus, Anti-Bot, Anti-Spam and Email Security, Management Network Policy Management, Endpoint Policy Management, Logging and Status, e Monitoring.

**11.3.4.** Quanto aos atestados e declarações exigidos para qualificação técnica, considerar que:

**11.3.4.1.** O atestado deverá referir-se a serviços prestados no âmbito da atividade econômica principal ou secundária especificadas no contrato social vigente da licitante;

**11.3.5.** Caso não seja o fabricante, a licitante deverá apresentar declaração do fabricante da solução ofertada, informando que é revenda autorizada no Brasil, estando apta a comercializar, prestar suporte e garantia dos produtos e serviços ofertados.

**11.4.**Documentos relativos à QUALIFICAÇÃO ECONOMICO-FINANCEIRA

a) Certidão negativa de falência ou concordata, expedida pelo distribuidor da sede do licitante, emitida a menos de 90 (noventa) dias da data de abertura do certame.

**11.5.**Documentos relativos à REGULARIDADE TRABALHISTA

a) Certidão Negativa de Débitos Trabalhistas – CNDT, expedida pelo Tribunal Superior do Trabalho.

## 12. OBRIGAÇÕES ENTRE AS PARTES

### 12.1.OBRIGAÇÕES DA CONTRATADA

**12.1.1.** A Contratada deverá apresentar a comprovação do vínculo de trabalho, o qual poderá ser efetuado por meio de contrato social, se sócio; da certidão de registro da licitante no referido Conselho Profissional, se nela constar o nome do profissional indicado; pelos documentos citados pela legislação trabalhista, como Carteira de Trabalho e Previdência Social, Contrato de Trabalho.Quaisquer substituições dos profissionais nomeados somente serão efetuadas quando aprovadas pela CONTRATANTE, por outros de igual ou superior capacidade técnica, devidamente comprovada, nos termos deste termo de referencia.

**12.1.2.** A contratada cumprirá fielmente com as obrigações assumidas por meio deste Termo de Referência, podendo a contratante aplicar ao vencedor as penalidades previstas, em caso de não cumprimento do estabelecido.

**12.1.3.** Correrá por conta da contratada qualquer prejuízo causado ao produto em decorrência do transporte.

**12.1.4.** A

**12.1.5.** Cabe à contratada o cumprimento dos prazos de entrega, nas datas, condições e local definido, nas quantidades contratadas.

**12.1.6.** Em nenhuma hipótese a contratada poderá alegar desconhecimento, incompreensão, dúvidas ou esquecimento de qualquer detalhe especificado neste Termo de Referência.

**12.1.7.** Substituir sem custos adicionais para o Sesc todo o produto inadequado para o uso ou em desacordo com o padrão exigido neste Termo de Referência.

**12.1.8.** Enquanto não ocorrer a substituição ou troca do objeto desta licitação, a empresa será considerada em atraso e, em consequência, sujeita as penalidades.

**12.1.9.** Atender prontamente a quaisquer exigências do Sesc, inerentes ao objeto do presente Termo de Referência;

**12.1.10.** Cabe à contratada consultar com antecedência os seus fornecedores quanto aos prazos de entrega do produto especificado, não cabendo, portanto, a justificativa de atraso do fornecimento devido ao não cumprimento da entrega por parte do fornecedor.

**12.1.11.** Cabe contratada responsabilizar-se por despesas, tributos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, fretes, seguros, deslocamento de pessoal,

prestação de garantia e quaisquer outras que incidam ou venham a incidir na execução do contrato.

## 13. OBRIGAÇÕES DA CONTRATANTE

**13.1.1.** Os pagamentos serão realizados em até 15 (quinze) dias subsequentes à entrega da nota fiscal, desde que os materiais ou serviços tenham sido conferidos e aceitos pelo Sesc/GO.

**13.1.2.** A contratante realizará a conferência e a fiscalização na entrega do produto, assegurando-se da qualidade, quantidade e especificações do item solicitado.

**13.1.3.** Comunicar a contratada, por escrito, sobre imperfeições, falhas, ou irregularidades verificadas no objeto fornecido, para que seja substituído.

**13.1.4.** Acompanhar e fiscalizar o cumprimento das obrigações da contratada, através de comissão/servidor especialmente designado, conforme tópico 20. FISCALIZAÇÃO.

**13.1.5.** O Sesc/GO reserva o direito de não receber os produtos em desacordo com as especificações e condições constantes neste termo.

## 14. DAS PENALIDADES

**14.1.** Em caso de inadimplemento total, parcial, sem motivo de força maior, a licitante estará sujeita, no que couber, e garantida a prévia defesa, às penalidades previstas na legislação aplicável, para as seguintes hipóteses:

**14.1.1.** Por atraso injustificado ou por inexecução parcial:

**a)** Advertência;

**b)** Multa de 0,3% (zero vírgula três por cento) ao dia incidente sobre o valor correspondente ao material ou serviço objeto desta licitação;

**c)** Suspensão temporária de participar em licitação e impedimento de contratar com o Sesc, por um prazo de até 2 (dois) anos.

**14.1.2.** Por inexecução total do objeto desta licitação:

**a)** Advertência;

**b)** Multa de 10% (dez por cento) sobre o valor total do Contrato; e

**c)** Suspensão temporária de participar em licitação e impedimento de contratar com o Sesc, por um prazo de até 2 (dois) anos.

**14.2.** As multas estabelecidas neste item são independentes e terão aplicação cumulativa e consecutivamente, de acordo com as normas que regeram a licitação, mas somente serão definitivas depois de exaurida a fase de defesa prévia da empresa adjudicada.

**14.3.** Quando não pagos em dinheiro pela empresa adjudicada, os valores das multas eventualmente aplicadas serão deduzidos pelo Sesc, dos pagamentos devidos e, quando for o caso, cobrado judicialmente.

**14.4.** Quando se tratar de inexecução parcial, o valor da multa será proporcional ao produto que deixou de ser entregue / serviço que deixou de ser executado.

**14.5.** Caso haja a recusa injustificada em assinar o Contrato no prazo de 03 (três) dias úteis, a contar da data da convocação, a empresa estará sujeita a penalidade prevista no tópico

14.1.2, alínea “c” e dará ao Sesc o direito de homologar e adjudicar esta licitação aos licitantes remanescentes, na ordem de classificação.

**14.6.**O prazo de convocação para assinatura do contrato poderá ser prorrogado uma vez, por igual período, quando solicitado pela empresa, durante o seu transcurso, desde que ocorra motivo justificado e aceito pelo Sesc.

**14.7.**Em caso de reincidência por atraso injustificado será a empresa penalizada nos termos do art. 32, da Resolução Sesc nº. 1.252/2012.

## 15. DA PROPOSTA

**15.1.** A proposta deverá ser elaborada em papel timbrado, devidamente assinada e datada, obedecendo ao edital e seus anexos;

**15.2.** Preço unitário por item e valores totais, indicados em moeda corrente nacional (com apenas duas casas decimais após a vírgula), sendo preços fixos e irreajustáveis, incluindo todos e quaisquer impostos incidentes, descontos, frete, mão de obra, emolumentos, contribuições previdenciárias, fiscais, sociais e parafiscais, que sejam devidos em decorrência, direta ou indireta, da entrega do objeto da presente licitação;

**15.3.** Razão Social completa da licitante e CNPJ, os quais deverão ser os mesmos constantes da documentação;

**15.4.** Valor total que será expresso em real e por extenso.

**15.5.** O prazo de validade da proposta, não poderá ser inferior a 90 (noventa) dias;

**15.6.** A omissão de qualquer uma das exigências desta solicitação, poderá implicar na desclassificação da proposta;

## 16. FISCALIZAÇÃO

**Fiscal:** Lucas Reges Barros
CPF: 041.603.421-75
Analista de Infraestrutura e Redes

**Suplente:** Saúle Tassara Bortolani
Matrícula: CPF: 706.932.421-91
Chefe da Seção Infraestrutura e Suporte

## 17. RESPONSÁVEIS TÉCNICOS

**Lucas Reges Barros**
Analista de Infraestrutura e Redes

**Saúle Tassara Bortolani**
Chefe da Seção Infraestrutura e Suporte

**Tiago Silva Santos**
Gerente de T.I

Goiânia, 16 de maio de 2022.