ESTADO DE GOIÁS
ORGANIZACAO DAS VOLUNTARIAS DE GOIAS - O V G
GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

TERMO DE REFERÊNCIA

Processo n°: 201900058002499 - SEI

Assunto: Contratação de empresa para fornecimento de equipamentos de segurança do tipo Firewall

A ORGANIZAÇÃO DAS VOLUNTÁRIAS DE GOIÁS-OVG, pessoa jurídica de direito privado, qualificada como Organização Social (OS), sediada na Rua T-14, nº 249, Setor Bueno, CEP 74.230-130, nesta Capital, devidamente inscrita no CNPJ/MF sob o nº 02.106.664/0001-65, vem através do presente Termo de Referência apresentar as especificações para a contratação de empresa para fornecimento de equipamentos de segurança do tipo Firewall, de acordo com a legislação específica vigente.

A contratação será regida pelo REGULAMENTO PARA AQUISIÇÃO DE BENS, MATERIAIS, SERVIÇOS, LOCAÇÕES, IMPORTAÇÕES E ALIENAÇÕES, disponível no site da OVG http://www.ovg.org.br e demais condições estabelecidas neste Termo, também disponível no site da OVG.

1. OBJETO

1.1 Contratação de empresa para fornecimento de equipamentos de segurança do tipo Firewall NGFW de aplicação web composta de appliances físicos, appliance de gerenciamento centralizado da solução e software com licenciamento de uso permanente, incluindo instalação, atualização e configuração da ferramenta com repasse de conhecimento para 02 colaboradores e suporte técnico sob demanda, conforme especificações e condições constantes no Formulário de Pedido (000010377202) da Gerência de Tecnologia da Informação – GTI dos autos nº 201900058002499 - SEI..

1.2 O presente instrumento tem como objeto a aquisição conforme quantitativo descrito na tabela abaixo:

Item	Descrição	Quantidade
1	HARDWARE FIREWALL TIPO 1 - Firewall de Próxima Geração Tipo 1 - Solução em cluster de alta disponibilidade - HA (ativo-passivo ou ativo-ativo), composta de 02 (dois) appliances (um ativo e um passivo) - Com 24 (vinte e quatro) meses de suporte e garantia de hardware.	01 un.
2	SOFTWARE FIREWALL TIPO 1 - Pacote de licenças de Firewall, IPS, Antivírus, Anti-spyware, Filtro de Web, Proteção contra ameaças avançadas, firewall de aplicação web para appliance de Firewall, Console de Gerência Administrativa e Centralização de Logs e Relatórios das soluções de Firewall de Próxima Geração Tipo 1 em cluster, pelo prazo de 24 (vinte e quatro)meses.	01 un.
3	HARDWARE FIREWALL TIPO 2 - Firewall de Próxima Geração Tipo 2 - Solução standalone - Com 24 (vinte e quatro) meses de suporte e garantia de hardware.	08 un.

4	SOFTWARE FIREWALL TIPO 2 - Pacote de licenças de Firewall, IPS, Antivírus, Anti-spyware, Filtro de Web, Proteção contra ameaças avançadas, firewall de aplicação web para appliance de Firewall, pelo prazo de 24 (vinte e quatro) meses.	08 un.
5	SERVIÇO DE INSTALAÇÃO, ATUALIZAÇÃO E CONFIGURAÇÃO DA FERRAMENTA COM REPASSE DE CONHECIMENTO PARA 02 COLABORADORES Serviços de capacitação sendo (16 horas) com profissional certificado pelo fabricante da solução Firewall de Próxima Geração, Gerenciamento, Centralização e Monitoração de Logs Centralizado.	01 un.

1.3 Todos equipamentos deverão ser novos, sem uso e deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas;

1.4 Não serão admitidos configurações e ajuste que impliquem no funcionamento do equipamento fora as condições normais recomendadas pelo fabricante do equipamento ou dos componentes. Tais como, alterações de frequência de clock (overclock), características de disco ou de memória, e drivers não recomendados pelo fabricante do equipamento.

1.4.1 Todos itens da solução apresentada deverão ser fabricados e licenciados pelo mesmo fabricante.

1.5 AQUISIÇÃO DE SOLUÇÃO DE SEGURANÇA DE REDE:

1.5.1 Deverão ser fornecidas as licenças para atualização de todos os componentes de software, vacinas de antivírus / *malwares, endpoints, softwares de criptografia de armazenamento em nuvem* e assinaturas de IPS, filtro de conteúdo web, controle de aplicações e proteção de firewall de aplicação web sem custo adicional, pelo período mínimo de 24 (vinte e quatro) meses.

1.5.2 Para os itens que representem bens materiais, a **CONTRATADA** deverá fornecer produtos novos, sem uso anterior.

1.5.3 Deverá ser fornecido por cada *appliance* físico que compõe a plataforma de segurança, entende-se o hardware, software e as licenças necessárias para o seu funcionamento.

1.5.4 Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.

1.5.5 Deverá fornecer alta disponibilidade (HA), entende-se que a solução firewall de **tipo 1** deverá ser composta ao menos por 02 (dois) *appliances*, licenciados para funcionamento em redundância.

1.5.6 Deverá ser capaz de executar a totalidade das capacidades exigidas para cada *appliance,* para cada função, não sendo aceitos somatórias para atingir os limites mínimos.

1.5.7 Deverá o hardware e o software fornecidos não estar em listas de *end-of-sale, end-of-support, end-of-engineering-support* ou *end-of-life* do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.

1.6 HARDWARE FIREWALL TIPO 1 - CARACTERÍSTICAS ESPECÍFICAS DE DESEMPENHO E HARDWARE

1.6.1 Deverá possuir todos os serviços ativos Next-Generation Firewall (NGFW) para proteção de informação perimetral e de rede interna que inclui stateful firewall com capacidade para operar em alta disponibilidade (HA) em modo ativo-passivo ou ativo-ativo para controle de tráfego de dados por identificação de usuários e por camada 7, com controle de aplicação, administração de largura de banda (QoS), VPN IPsec e SSL, IPS, prevenção contra ameaças de vírus, *malwares*, Filtro de URL, criptografia de e-mail, inspeção de tráfego criptografado e proteção de firewall de aplicação Web. Deverá ser fornecida console de gerenciamento dos equipamentos e centralização de logs em hardware específico.

1.6.2 Deverá possuir a performance mínima de 19 Gbps de *throughput* (Taxas de transferências) para firewall.

1.6.3 Deverá possuir a performance mínima de 3.2 Gbps de *throughput* (Taxas de transferências) de NGFW e IPS

1.6.4 Deverá possuir a performance mínima de 2.5 Gbps de *throughput* (Taxas de transferências) para controle de AV/proxy.

1.6.5 Deverá possuir a performance mínima de 1.5 Gbps de *throughput* (Taxas de transferências) de VPN.

1.6.6 Deverá possuir suporte, de no mínimo, 8.000.000 de conexões simultâneas.

1.6.7 Deverá possuir suporte, de no mínimo, 130.000 novas conexões por segundo.

1.6.8 Deverá possuir o número irrestrito quanto ao máximo de usuários licenciados.

1.6.9 Deverá possuir armazenamento interno de no mínimo 120 (cento e vinte) GB SSD para sistema operacional, quarentena local, logs e relatórios.

1.6.10 Deverá possuir no mínimo 8 (oito) GB de memória RAM, ou tecnologia compatível a garantir o pleno funcionamento da solução

1.6.11 Deverá possuir no mínimo 12 (doze) interfaces de rede 1000Base-TX.

1.6.12 Deverá possuir no mínimo 2 (duas) interfaces de rede 1 Gbps SFP.

1.6.13 Deverá possuir 1 (uma) interface do tipo console ou similar.

1.6.14 Deverá possuir 2 (duas) fontes 100-240VAC ou equivalente que garantam a redundância de energia.

1.6.15 Deverá possuir HA (modo de alta disponibilidade) deve suportar o uso de dois equipamentos em modo ativo-passivo ou modo ativo-ativo e deve possibilitar monitoramento de falha de link.

1.6.16 Deverá suportar segmento de rede do tipo WAN ou de link externo.

1.6.17 Deverá suportar segmento de rede do tipo WAN, secundário com possibilidade de ativação de recurso para redundância de WAN com balanceamento de carga e WAN Failover por aplicação.

1.6.17.1 Deverá suportar no mínimo balanceamento de 03 (três) links.

1.6.18 Deverá suportar segmento de rede do tipo LAN ou rede interna podendo ser configurado como DMZ (Zona desmilitarizada)

1.6.19 Deverá suportar segmento de rede do tipo LAN ou rede interna ou Porta de sincronismo para funcionamento em alta disponibilidade

1.6.20 Deverá suportar VPN Client-to-Site IPsec com licenciamento, no mínimo, para 50 usuários simultâneos;

1.6.21 Deverá suportar VPN SSL e deve ser licenciada para, no mínimo, 8 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para no mínimo, 300 usuários simultâneos, com aquisição de licença futura;

1.6.22 Deverá suportar no mínimo 1.000 túneis de VPN IPSEC simultâneos

1.7 HARDWARE FIREWALL TIPO 2 - CARACTERÍSTICAS ESPECÍFICAS DE DESEMPENHO E HARDWARE

1.7.1 Deverá possuir todos os serviços ativos UTM (Proteção Anti-Malware e Anti-virus, IDS, IPS e Controle de Aplicação).

1.7.2 Deverá possuir performance mínima de 7.5 Gbps de throughput (Taxas de transferências) para firewall.

1.7.3 Deverá possuir performance mínima de 1 Gbps de throughput (Taxas de transferências) de NGFW e IPS.

1.7.4 Deverá possuir performance mínima de 1,5 Gbps de throughput (Taxas de transferências) para controle de AV/proxy.

1.7.5 Deverá possuir performance mínima de 1 Gbps de throughput (Taxas de transferências) de VPN.

1.7.6 Deverá possuir suporte a, no mínimo, 5.500.000 de conexões simultâneas.

1.7.7 Deverá possuir suporte a, no mínimo, 80.000 novas conexões por segundo.

1.7.8 Deverá possuir o número irrestrito quanto ao máximo de usuários licenciados.

1.7.9 Deverá possuir armazenamento interno de no mínimo 64 (sessenta e quatro) GB SSD para sistema operacional, quarentena local, logs e relatórios.

1.7.10 Deverá possuir no mínimo 06 (seis) GB de memória RAM, ou tecnologia compatível a garantir o pleno funcionamento da solução

1.7.11 Deverá possuir no mínimo 08 (oito) interfaces de rede 1000Base-TX.

1.7.12 Deverá possuir no mínimo 01 (uma) interface de rede 1 Gbps SFP.

1.7.13 Deverá possuir 01 (uma) interface do tipo console RJ 45 ou serial ou USB.

1.7.14 Deverá possuir 02 (duas) fontes 100-240VAC.

1.7.15 Deverá suportar segmento de rede do tipo WAN ou de link externo.

1.7.16 Deverá suportar segmento de rede do tipo WAN, secundário com possibilidade de ativação de recurso para redundância de WAN com balanceamento de carga e WAN Failover por aplicação.

1.7.16.1 Deverá possuir equipamento mínimo de balanceamento de 03 (três) links.

1.7.17 Deverá suportar segmento de rede do tipo LAN ou rede interna.

1.7.18 Deverá suportar segmento de rede do tipo LAN ou rede interna podendo ser configurado como DMZ (Zona desmilitarizada)

1.7.19 Deverá suportar segmento de rede do tipo LAN ou rede interna ou Porta de sincronismo para funcionamento em alta disponibilidade

1.7.20 Deverá a VPN SSL ser licenciada para, no mínimo, 02 (dois) usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para no mínimo, 25 usuários simultâneos, com aquisição de licença futura;

1.7.21 Suportar no mínimo 10 (dez) túneis de VPN IPSEC simultâneos licenciados;

1.7.22 Deverá o hardware e o software fornecidos não estar em listas de *end-of-sale, end-of-support, end-of-engineering-support* ou *end-of-life* do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.

1.8 CARACTERÍSTICAS GERAIS PARA FIREWALLS DE PRÓXIMA GERAÇÃO

1.8.1 Deverá a solução consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW) Firewall **tipo 1** e UTM (Proteção Anti-Malware e Anti-virus, IDS, IPS e Controle de Aplicação) Firewall **tipo 2,** e console de gerência, monitoração e logs.

1.8.2 Deverá oferecer as funcionalidades de backup/restore tanto da configuração quanto do firmware/sistema operacional através da interface gráfica, assim como permitir ao administrador agendar procedimentos de backups da configuração em determinado dia e hora.

1.8.3 Deverá por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões e UTM entende-se: Proteção Anti-Malware e Anti-virus, IDS, IPS e Controle de Aplicação.

1.8.4 Deverá suportar ás funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação.

1.8.5 Deverá plataforma ser otimizada para análise de conteúdo de aplicações em camada 7.

1.8.6 Deverá suportar monitoramento através de SNMP v2 e v3;

1.8.7 Deverá ter suporte a definição de VLAN no firewall, conforme padrão IEEE 802.1q e ser criar subinterfaces lógicas associadas a VLANs e estabelecer regras de filtragem (Stateful Firewall) entre elas;

1.8.8 Deverá suportar configuração de link-aggregation de interfaces suportando o protocolo 802.3ad para aumento de throughput (taxa de transferência).

1.8.9 Deverá suportar configuração de port-redundacy de interfaces para a alta disponibilidade de interfaces;

1.8.10 Não serão permitidas soluções baseadas em sistemas operacionais abertos (OpenSource) como Free BSD, Debian ou mesmo Linux.

1.8.11 Deverá suportar arquitetura de armazenamento de logs redundante, permitindo a configuração de equipamentos distintos;

1.8.12 Deverá O software ser fornecido em sua versão mais atualizada.

1.8.13 Deverá ser permitido atualização de software e enviar avisos de atualização automáticos.

1.8.14 Deverá o sistema permitir a definição de redes, serviços, hosts períodos de tempos, usuários e grupos, clientes e servidores.

1.8.15 Deverá o backup e a restauração das configurações ser feito localmente, via FTP ou e-mail com frequência diária, semanal ou mensal, podendo também ser realizado por demanda.

1.8.16 Deverá as notificações ser realizadas via email e SNMP.

1.8.17 Deverá suportar SNMP e Netflow.

1.8.18 Deverá o firewall ser stateful, com inspeção profunda de pacotes (deep packet inspection).

1.8.19 Deverá possuir zonas divididas pelo menos em WAN, LAN e DMZ, sendo necessário que as zonas LAN e DMZ possam ser customizáveis.

1.8.20 Deverá as políticas de NAT ser customizáveis para cada regra.

1.8.21 Deverá a proteção contra flood (transbordar) ter proteção contra DoS (Denial of Service), DdoS (Distributed DoS) e bloqueio de portscan.

1.8.22 Deverá possuir proteção contra anti-spoofing.

1.8.23 Deverá suportar IPv4 e IPv6.

1.8.24 Deverá suportar os tunelamentos IPV6, 6in4, 6to4, 4in6 e IPv6 Rapid Deployment (6rd) de acordo com a RFC 5969.

1.8.25 Deverá ter Suporte aos roteamentos estáticos, dinâmico (RIP, BGP e OSPF) e multicast (PIM-SM e IGMP).

1.8.26 Deverá suportar a definição de VLANs no firewall conforme padrão IEEE 802.1q e tagging de VLAN.

1.8.27 Deverá suportar a solução, configurar os serviços de DNS, Dynamic DNS, DHCP e NTP;

1.8.28 Deverá suportar o traffic shapping (QoS) e ser baseado em rede ou usuário.

1.8.29 Deverá a solução permitir o tráfego de cotas baseados por usuários para upload/download e pelo tráfego total, sendo cíclicas ou não-cíclicas.

1.8.30 Deverá suportar os dispositivos de proteção com a capacidade de operar de forma simultânea mediante o uso de suas interfaces físicas nos seguintes modos:

1.8.30.1 Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);

1.8.30.2 Modo sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

1.8.30.3 Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;

1.8.30.4 Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;

1.8.30.5 Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.

1.8.31 Deverá possuir DHCP Server interno;

1.8.32 Deverá suporta o encaminhamento de pacotes UDPs multicast/broadcast entre diferentes interfaces e zonas de segurança como DHCP Relay, suportando os protocolos e portas:

1.8.32.1 Time service—UDP porta 37

1.8.32.2 DNS—UDP porta 53

1.8.32.3 DHCP—UDP portas 67 e 68

1.8.32.4 Net-Bios DNS—UDP porta 137

1.8.32.5 Net-Bios Datagram—UDP porta 138

1.8.32.6 Wake On LAN—UDP porta 7 e 9

1.8.32.7 mDNS—UDP porta 5353

1.8.33 Deverá suportar os seguintes tipos de NAT:

1.8.33.1 Nat dinâmico (Many-to-1);

1.8.33.2 Nat dinâmico (Many-to-Many);

1.8.33.3 Nat estático (1-to-1);

1.8.33.4 Nat estático bidirecional 1-to-1;

1.8.33.5 Tradução de porta (PAT);

1.8.33.6 NAT de origem;

1.8.33.7 NAT de destino;

1.8.33.8 NAT de origem e NAT de destino simultaneamente.

1.8.34 Deverá suportar mecanismo contra-ataques de falsificação de endereços (IP Spoofing)

1.8.35 Deverá possuir mecanismo de sincronismo de horário através do protocolo NTP. Para tanto o appliance deve realizar a pesquisa em pelo menos 03 servidores NTP .

1.8.36 Deverá possuir gerenciamento de tráfego de entrada ou saída, por serviços, endereços IP e regra de firewall, permitindo definir banda mínima e máxima garantida.

1.8.37 Deverá Implementar 802.1p e classe de serviços CoS (Class of Service) de DSCP (Differentiated Services Code Points);

1.8.38 Deverá suportar protocolos de roteamento RIP, RIPng, OSPF e BGP;

1.8.39 Deverá suportar IPv4, com roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

1.8.40 Deverá suportar IPv6, assim como criação de regras com objetos que utilizem endereços IPv4 e IPv6.

1.8.41 Deverá possui suporte a log via syslog;

1.8.42 Deverá possuir mecanismo de aplicação e de correções e atualizações para o firewall remotamente através da interface gráfica;

1.8.43 Deverá permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall.

1.8.44 Deverá permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento;

1.8.45 Deverá permitir a visualização de estatísticas do uso de CPU do appliance o através da interface gráfica remota em tempo real;

1.8.46 Deverá implementar segurança fim-a-fim usando solução de criptografia que de maneira automática forneça proteção a redes WANs privadas que transitam por redes públicas compartilhadas;

1.8.47 Deverá suportar e implementar QoS com classificação, marcação e priorização de tráfego com base em endereço IP de origem/destino, portas TCP/UDP de origem e destino, DSCP (Differentiated Services Code Point), tipo de aplicação camada 7 e traffic shaping nas interfaces;

1.8.48 Deverá ter capacidade de realizar a saída local de internet para alguns tráfegos selecionados a partir, de no mínimo, dos parâmetros de IP, porta e URL;

1.8.49 A comutação dos caminhos deve ocorrer de maneira dinâmica e automática baseada nas políticas previamente aplicadas.

1.8.50 Implementar tecnologia de reconhecimento de aplicações conhecidas (DPI), como Office 365, Facebook e Youtube, como também subaplicações associadas como Facebook Messenger e Office 365 Outlook.

1.9 CONTROLE POR POLÍTICAS DE FIREWALL

1.9.1 Deverá suportar controles por: porta e protocolos TCP/UDP, origem/destino e identificação de usuários.

1.9.2 Deverá o controle de políticas monitorar as políticas de redes, usuários, grupos e tempo, bem como identificar as regras não-utilizadas, desabilitadas, modificadas e novas políticas.

1.9.3 Deverá as políticas ter controle de tempo de acesso por usuário e grupo, sendo aplicadas por zonas, redes e por tipos de serviços.

1.9.4 Deverá o ter controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.

1.9.5 Deverá o ter controle de políticas por países via localização por IP.

1.9.6 Deverá ter suporte a objetos e regras IPV4 e IPV6.

1.9.7 Deverá ter suporte a objetos e regras *multicast*.

1.10 PREVENÇÃO DE AMEAÇAS

1.10.1 Deverá ter a proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus, *Anti-Malware* e Firewall de Proteção Web (*WAF*) integrados no próprio *appliance* de Firewall ou entregue em múltiplos *appliances* desde que obedeçam a todos os requisitos desta especificação.

1.10.2 Deverá realizar a inspeção profunda de pacotes (DPI *deep packet inspection*) para prevenção de intrusão (IPS) e deve incluir assinaturas de prevenção de intrusão (IPS).

1.10.3 Deverá ter as assinaturas de prevenção de intrusão (IPS) customizadas.

1.10.4 Deverá ter exceções por usuário, grupo de usuários, IP de origem ou de destino devem ser possíveis nas regras;

1.10.5 Deverá suportar granularidade nas políticas de IPS Antivírus e *Anti-Malware*, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens, com customização completa;

1.10.6 Deverá a proteção *Anti-Malware* bloquear todas as formas de vírus, *web malwares*, *trojans* e *spyware* em HTTP e HTTPS, FTP e *web-emails*.

1.10.7 Deverá a proteção Anti-Malware realizar a proteção com emulação *JavaScript* ou equivalente.

1.10.8 Deverá ter proteção em tempo real contra novas ameaças criadas.

1.10.9 Deverá possuir *engines* de anti-vírus independentes e de diferentes fabricantes para a detecção de *malware*, podendo ser configuradas isoladamente ou simultaneamente.

1.10.10 Deverá permitir o bloqueio de vulnerabilidades.

1.10.11 Deverá permitir o bloqueio de *exploits* conhecidos.

1.10.12 Deve detectar e bloquear o tráfego de rede que busque acesso a *contact command* e servidores de controle utilizando múltiplas camadas de DNS, *AFC* e firewall.

1.10.13 Deverá incluir proteção contra ataques de negação de serviços.

1.10.14 Deverá ser imune e capaz de impedir ataques básicos como: *SYN flood, ICMP flood, UDP Flood*, etc.

1.10.15 Deverá suportar bloqueio de arquivos por tipo.

1.10.16 Deverá registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.

1.10.17 Deverá identificar o país de onde partiu a ameaça.

1.10.18 Deverá ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas de segurança considerando uma das opções ou a combinação de todas elas: usuários, grupos de usuários, origem, destino, zonas de segurança.

1.10.19 Deverá o firewall de aplicação Web (*WAF*) ter a função de *reverse proxy*, com a função de *URL hardening* realizando *deep-linking* e prevenção dos ataques de *path traversal* ou *directory traversal*.

1.10.20 Deverá o firewall de aplicação Web (*WAF*) realizar *cookie signing* com assinaturas digitais, roteamento baseado por caminho, autenticações reversas e básicas para acesso do servidor.

1.10.21 Deverá o firewall de aplicação Web (*WAF*) possuir a função de balanceamento de carga de visitantes por múltiplos servidores, com a possibilidade de modificação dos parâmetros de performance do *WAF* e permissão e bloqueio de *ranges* de IP

1.10.22 Deverá ter no mínimo a proteção contra os seguintes ataques, mas não limitado a: *SQL injection* e *Cross-site scripting*.

1.11 ALTA DISPONIBILIDADE DO FIREWALL TIPO 01

1.11.1 Deverá a solução ser entregue operando em alta disponibilidade no modo Ativo/Standby, com as implementações de Failover.

1.11.2 Deverá a solução ter capacidade de fazer monitoramento fisico das interfaces dos membros do cluster.

1.11.3 Deverá a solução permitir o uso de endereço MAC virtual para evitar problemas de expiração de tabela ARP em caso de Failover.

1.11.4 Deverá a solução possibilitar a sincronização de todas as configurações realizadas na caixa principal do cluster, incluído mas não limitado a objetos, regras, rotas, VPNs e politicas de segurança.

1.11.5 Deverá a solução permitir visualizar no equipamento principal, o status da comunicação entre o peers do cluster, status de sincronização das configurações, status atual equipamento backup.

1.12 REDES VIRTUAIS PRIVADAS - VPN

1.12.1 Deverá possuir Criptografia 3DES, AES 128 e AES 256;

1.12.2 Deverá possuir Autenticação com MD5, SHA-1, SHA-256 e SHA-384; VPN IPsec deve suportar: DES e 3DES, Autenticação MD5 e SHA-1;*Diffie-Hellman Group 1, Group 2, Group 5 e Group 14*; Algoritmo Internet Key Exchange (IKE); AES 128, 192 e 256 (*Advanced Encryption Standard*); SHA 256, 384 e 512; Autenticação via certificado PKI (X.509) e *Pre-shared key* (PSK).

1.12.3 Deverá possuir Algoritmo Internet Key Exchange (IKE);

1.12.4 Deverá possuir Autenticação via certificado IKE PKI;

1.12.5 Deverá possuir interoperabilidade com outros fabricantes de acordo com o padrão IPSEC através de RFC`s;

1.12.6 Deverá possuir solução VPNs L2TP, incluindo suporte para iPhone, Windows phone, Android com suporte a cliente L2TP;

1.12.7 Deverá suportar VPNs baseadas em políticas e VPNs baseadas em roteamento estático e dinâmico.

1.12.8 Deverá suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.

1.12.9 Deverá possuir a solução de incluir e a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos;

1.12.10 Deverá permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário;

1.12.11 Deverá permitir que seja criado políticas de roteamentos estáticos utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego sendo este visto pela regra de roteamento, como uma interface simples de rede para encaminhamento do tráfego.

1.12.12 Deverá suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet;

1.12.13 Deverá permitir estabelecer um túnel SSL VPN com uma solução de autienticação via LDAP, *Active Directory, Radius, eDirectory, TACACS+* e via base de dados local;

1.12.14 Deverá possuir o acesso via o portal de usuário para o download e configuração do cliente SSL para Windows

1.12.15 Deverá permitir criar políticas de controle de aplicações, IPS, Antivírus, *Anti-Malware* e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

1.12.16 Deverá suportar autenticação via AD/LDAP, *Token* e base de usuários local;

1.12.17 Deverá ser disponibilizado o acesso remoto ilimitado, até o limite suportado de túneis VPN pelo equipamento, sem a necessidade de aquisição de novas licenças e sem qualquer custo adicional para o licenciamento de clientes SSL para estações Windows.

1.13 CONTROLE E PROTEÇÃO DE APLICAÇÕES

1.13.1 Deverá os dispositivos de proteção de rede possuir a capacidade de reconhecer aplicações por assinaturas e camada 7, utilizando portas padrões (80 e 443), portas não padrões, *port hopping* e túnel através de tráfego SSL encriptado.

1.13.2 Deverá reconhecer pelo menos 2000 aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a tráfego relacionado a *peer-to-peer*, redes sociais, acesso remoto, *update* de software, serviços de rede, VoIP, streaming de mídia, proxy e tunelamento, mensageiros instantâneos, compartilhamento de arquivos, web e-mail e update de softwares.

1.13.3 Deverá reconhecer pelo menos as seguintes aplicações: *4Shared File Transfer, Active Directory/SMB, Citrix ICA, DHCP Protocol, Dropbox Download, Easy Proxy, Facebook Graph API, Firefox Update, Freegate Proxy, 1.FreeVPN Proxy, Gmail Video, Chat* Streaming, Gmail WebChat, Gmail WebMail, Gmail-Way2SMS WebMail, Gtalk Messenger, Gtalk Messenger File Transfer, Gtalk-Way2SMS, HTTP Tunnel Proxy, HTTPort Proxy, LogMeIn Remote Access, NTP, Oracle database, RAR File Download, Redtube Streaming, RPC over HTTP Proxy, Skydrive, Skype, Skype Services, skyZIP, SNMP Trap, TeamViewer Conferencing e File Transfer, TOR Proxy, Torrent Clients P2P, Ultrasurf Proxy, UltraVPN, VNC Remote Access, VNC Web Remote Access, WhatsApp, WhatsApp File Transfer e WhatsApp Web.

1.13.4 Deverá realizar o escaneamento e controle de *micro app* incluindo, mas não limitado a: *Facebook (Applications, Chat, Commenting, Events, Games, Like Plugin, Message, Pics Download e Upload, Plugin, Post Attachment, Posting, Questions, Status Update, Video Chat, Video Playback, Video Upload, Website), Freegate Proxy, Gmail (Android Application, Attachment), Google Drive (Base, File Download, File Upload), Google Earth Application, Google Plus, LinkedIN (Company Search, Compose Webmail, Job Search, Mail Inbox, Status Update), SkyDrive File Upload e Download, Twitter (Message, Status Update, Upload, Website), Yahoo (WebMail, WebMail File Attach) e Youtube (Video Search, Video Streaming, Upload, Website)*

1.13.5 Deverá o escaneamento de *micro app* deverá ser habilitado via console gráfica (GUI) e via comando de linha (CLI).

1.13.6 Deverá o tráfego criptografado SSL, de-criptografar de pacotes a fim de possibilitar a leitura de *payload* para checagem de assinaturas de aplicações conhecidas pelo fabricante.

1.13.7 Deverá atualizar a base de assinaturas de aplicações automaticamente.

1.13.8 Deverá reconhecer aplicações em IPv6.

1.13.9 Deverá limitar a banda usada por aplicações (*traffic shaping*).

1.13.10 Deverá os dispositivos de proteção de rede possuir a capacidade de identificar o usuário de rede com integração ao Microsoft , sem a necessidade de instalação de agente no *Domain Controller*, nem nas

estações dos usuários.

1.13.11 Deverá ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras.

1.13.12 Deverá os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades abaixo:

1.13.12.1 Deverá ter capacidade para realizar filtragens/inspeções dentro de portas TCP conhecidas por exemplo porta 80 http, buscando por aplicações que potencialmente expõe o ambiente como: P2P, Kazaa, Morpheus, BitTorrent ou messengers

1.13.12.2 Deverá controlar o uso dos serviços de Instant Messengers como MSN, YAHOO, Google Talk, ICQ, de acordo com o perfil de cada usuário ou grupo de usuários, de modo a definir, para cada perfil, se ele pode ou não realizar download e/ou upload de arquivos, limitar as extensões dos arquivos que podem ser enviados/recebidos e permissões e bloqueio de sua utilização baseados em horários pré-determinados pelo administrador será obrigatório para este item.

1.13.13 Deverá controlar software FreeProxy tais como ToR, Ultrasurf, Freegate,etc.

1.13.14 Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

1.13.15 Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;

1.13.16 Deverá atualizar a base de assinaturas de aplicações automaticamente;

1.13.17 Deverá limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;

1.13.18 Deverá a solução de controle de aplicação WEB deve criar regras granulares possibilitando adicionar tipos de aplicação WEB e categorias por regra, sendo assim criando controle granular de qualquer tipo de acesso não permitido pela empresa;

1.13.19 Deverá implementar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e protocolos;

1.13.20 Deverá possibilitar que o controle de portas seja aplicado para todas as aplicações;

1.13.21 Deverá possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, uTorrent, etc.) possuindo granularidade de controle/políticas para os mesmos;

1.13.22 Deverá possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Facebook e bloquear chat;

1.13.23 Deverá possibilitar a diferenciação de aplicações Proxies possuindo granularidade de controle/políticas para os mesmos;

1.13.24 Deverá ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

1.13.24.1 Nível de risco da aplicação.

1.13.24.2 Categoria de aplicações.

1.14 CONTROLE E PROTEÇÃO WEB

1.14.1 Deverá permitir especificar política de navegação Web por tempo, ou seja, a definição de regras para um determinado dia da semana e horário de início e fim, permitindo a adição de múltiplos dias e horários na mesma definição de política por tempo. Esta regra de tempo pode ser recorrente ou em uma única vez.

1.14.2 Deverá possuir a criação de políticas por usuários, grupos de usuários, IPs e redes;

1.14.3 Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando URLs através da integração com serviços de diretório, autenticação via LDAP, *Active Directory*, *Radius*, *E-directory* e base de dados local;

1.14.4 Deverá permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

1.14.5 Deverá possuir pelo menos 90 categorias de URLs;

1.14.6 Deverá suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

1.14.7 Deverá ser capaz de forçar o uso da opção Safe Search em sites de busca;

1.14.8 Deverá ser capaz de categorizar as URLs a partir de base ou cache de URLs locais ou através de consultas dinâmicas na nuvem do fabricante, independentemente do método de classificação a categorização não deve causar atraso na comunicação visível ao usuário;

1.14.9 Deverá suportar a criação categorias de URLs customizadas;

1.14.10 Deverá suportar a opção de bloqueio de categoria HTTP e liberação da categoria apenas em HTTPS.

1.14.11 Deverá permitir a customização de página de bloqueio;

1.14.12 Deverá suportar a inclusão nos logs do produto de informações das atividades dos usuários;

1.14.13 Deverá salvar nos logs as informações adequadas para geração de relatórios indicando usuário, tempo de acesso, bytes trafegados e site acessado.

1.15 IDENTIFICAÇÃO DE USUÁRIOS

1.15.1 Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticando via LDAP, *Active Directory, Radius, eDirectory, TACACS+* e via base de dados local, para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários.

1.15.2 Deverá permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (*Captive Portal*).

1.15.3 Deverá 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.

1.15.4 Deverá permitir autenticação em modos: transparente, autenticação proxy (NTLM e Kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, MAC OS X e Linux 32/64.

1.15.5 Deverá possuir a autenticação Single sign-on para, pelo menos, os sistemas de diretórios *Active Directory* e *eDirectory*.

1.15.6 Deverá possuir portal do usuário para que os usuários tenham acesso ao uso de internet pessoal, troquem senhas da base local e façam o download de softwares para as estações presentes na solução.

1.16 QUALIDADE DE SERVIÇO - QoS

1.16.1 Deverá ter a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações.

1.16.2 Deverá a *solução suportar Traffic Shaping* (Qos) e a criação de políticas baseadas em categoria web e aplicação por: endereço de origem; endereço de destino; usuário e grupo do LDAP/AD.

1.16.3 Deverá ser configurado o limite e a garantia de upload/download, bem como ser priorizado o tráfego total e *bitrate* de modo individual ou compartilhado.

1.16.4 Deverá suportar priorização *Real-Time* de protocolos de voz (VoIP).

1.17 GERÊNCIA ADMINISTRATIVA CENTRALIZADA

1.17.1 Deverá possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos através de uma única console central, com administração de privilégios e funções.

1.17.2 Deverá o gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.

1.17.3 Deverá estar licenciada para gerenciar as soluções de firewall de próxima geração **Tipo1.**

1.17.4 Deverá ser fornecidas soluções virtuais ou via *appliances* desde que obedeçam a todos os requisitos desta especificação.

1.17.5 Deverá ser centralizada a gerência de todas as políticas do firewall e configurações para as soluções de firewall de próxima geração **Tipo1**, sem necessidade de acesso direto aos equipamentos.

1.17.6 Deverá permitir a criação de Templates para configurações.

1.17.7 Deverá possuir indicadores do estado de equipamentos e rede.

1.17.8 Deverá emitir alertas baseados em *thresholds* customizáveis, incluindo também alertas de expiração de subscrição, mudança de *status* de *gateways*, uso excessivo de disco, eventos ATP, IPS, ameaças de vírus, navegação, entre outros.

1.17.9 Deverá permitir a criação de grupos de equipamentos por nome, modelo, *firmware* e regiões.

1.17.10 Deverá ter controle de privilégios administrativos, com granularidade de funções (VPN admin, App e Web admin, IPS admin, etc);

1.17.11 Deverá ter controle das alterações feitas por usuários administrativos, comparar diferentes versões de configurações e realizar o processo de *roll back* de configurações para mudanças indesejadas;

1.17.12 Deverá ter logs de auditoria de uso administrativo e atividades realizadas nos equipamentos.

1.17.13 Deverá ter integração com a solução de logs e relatórios, habilitando o provisionamento automático de novos equipamentos e a sincronização dos administradores da centralização da gerência com a centralização de logs e relatórios.

1.17.14 Deverá permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o firewall, cada um responsável por determinadas tarefas da administração;

1.17.15 Deverá fornecer gerência remota, com interface gráfica nativa;

1.17.16 Deverá a interface gráfica possuir assistentes para facilitar a configuração inicial e a realização das tarefas mais comuns na administração do firewall, incluindo a configuração de VPN IPSECs, NAT, perfis de acesso e regras de filtragem;

1.17.17 Deverá possuir mecanismo que permita a realização de cópias de segurança (backups) e sua posterior restauração remotamente, através da interface gráfica, sem necessidade de se reinicializar o sistema;

1.17.18 Deverá permitir a visualização de estatísticas do uso de CPU, memória da máquina onde o firewall está rodando e tráfego de rede em todas as interfaces do Firewall através da interface gráfica remota, em tempo real e em forma tabular e gráfica;

1.17.19 Deverá possibilitar o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo;

1.17.20 Deverá possuir interface orientada a linha de comando para a administração do firewall a partir do console ou conexão SSH sendo está múltiplas sessões simultâneas.

1.17.21 Deverá possuir mecanismo que permita inspecionar o tráfego de rede em tempo real (sniffer) via interface gráfica, permitindo a filtragem dos pacotes por protocolo, endereço IP origem e/ou destino e porta IP origem e/ou destino, usando uma linguagem textual;

1.17.22 Deverá permitir a visualização do tráfego de rede em tempo real nas interfaces de rede do Firewall

1.18 GERÊNCIA DE LOGS E RELATÓRIOS

1.18.1 Deverá possuir solução de logs e relatórios centralizados, possibilitando a consolidação total de todas as atividades da solução através de uma única console central.

1.18.2 Deverá estar licenciada para gerenciar as soluções de firewall de próxima geração do **Tipo 1 e Tipo 2.**

1.18.3 Deverá ser fornecidas soluções virtuais ou via *appliances* desde que obedeçam a todos os requisitos desta especificação, com armazenamento mínimo de 1TB de dados.

1.18.4 Deverá prover relatórios baseados em usuários, com visibilidade sobre acesso a aplicações, navegação, eventos ATP, downloads e consumo de banda, independente em qual rede ou IP o usuário esteja se conectando.

1.18.5 Deverá possibilitar a identificação de ataques como a identificação de malware identificados pelos eventos ATP, usuários suspeitos, tráfegos anômalos incluindo tráfego ICMP e consumo não-usual de banda.

1.18.6 Deverá disponibilizar download dos relatórios gerados

1.18.7 Deverá fornecer relatórios históricos para análises de mudanças e comportamentos.

1.18.8 Deverá conter customizações dos relatórios para inserção de logotipos próprios.

1.18.9 Deverá fornecer relatórios de *compliance* SOX, HIPAA e PCI.

1.18.10 Deverá permitir a exportação via PDF ou Excel.

1.18.11 Deverá fornecer relatórios sobre os acessos de procura no Google, Yahoo, Bing e Wikipedia.

1.18.12 Deverá fornecer relatórios de tendências.

1.18.13 Deverá fornecer logs em tempo real, de auditoria e arquivados.

1.18.14 Deverá possuir mecanismo de procura de logs arquivados.

1.18.15 Deverá ter acesso baseado em Web com controles administrativos distintos.

1.18.16 Deverá ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas.

1.18.17 Deverá possibilitar a geração de pelo menos os seguintes tipos de relatório com cruzamento de informações, mostrados em formato HTML: máquinas acessadas X serviços bloqueados, usuários X URLs acessadas, usuários X categorias Web bloqueadas (em caso de utilização de um filtro de conteúdo Web);

1.18.18 Deverá possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (em caso de existência de um filtro de conteúdo Web), maiores emissores e receptores de e-mail;

1.18.19 Deverá permitir o envio dos relatórios, através de e-mail para usuários predefinidos;

1.18.20 Deverá possuir relatórios pré-definidos na solução e permitir a criação de relatórios customizados;

1.18.21 Deverá possibilitar a geração dos relatórios sob demanda e através de agendamento diário, semanal e mensal. No caso de agendamento, os relatórios deverão ser publicados de forma automática

1.18.22 Deverá fornecer interface gráfica para no mínimo 5 usuários;

1.18.23 Deverá a interface gráfica possuir mecanismo que permita a gerência e emissão de relatórios de forma remota

1.18.24 Deverá prover mecanismo de visualização de eventos em tempo real das funções de segurança, com uma prévia sumarização para fácil visualização de no mínimo as seguintes informações:

1.18.24.1 Aplicações mais utilizadas;

1.18.24.2 Usuários com maior atividade;

1.18.24.3 Estatísticas de uso;

1.18.24.4 Principais aplicações por taxa de transferência de bytes;

1.18.24.5 Principais hosts por número de ameaças identificadas;

1.18.25 Prover mecanismo de consulta às informações registradas integrado à interface de administração;

1.18.26 Possibilitar o armazenamento de seus registros (log e/ou eventos)

1.18.27 Possibilitar a recuperação dos registros de log e/ou eventos armazenados em máquina remota, através de protocolo criptografado, de forma transparente através da interface gráfica;

1.19 PROTEÇÃO CONTRA VIRUS

1.19.1 Deverá possuir módulo de antivírus e anti-bot integrado no próprio appliance de segurança;

1.19.2 Deverá a solução ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede;

1.19.3 Deverá implementar interface gráfica WEB segura, utilizando o protocolo HTTPS.

1.19.4 Deverá implementar interface CLI segura através do protocolo SSH;

1.19.5 Deverá possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream;

1.19.6 Deverá a solução permitir criar regras de exceção de acordo com a proteção;

1.19.7 Deverá a solução ser capaz de proteger contra ataques para DNS.

1.19.8 Deverá a solução ser capaz de prevenir acesso a websites maliciosos.

1.19.9 Deverá a solução ser capaz de realizar inspeção de tráfego SSL e SSH.

1.19.10 Deverá a solução receber atualizações de um serviço baseado em cloud.

1.19.11 Deverá a solução ser capaz de bloquear a entrada de arquivos maliciosos.

1.19.12 Deverá possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP, IMAP e CIFS;

1.20 CERTIFICAÇÕES EXIGIDAS DA SOLUÇÃO

1.20.1 O fabricante do hardware da solução deverá possuir pelo menos uma das seguintes certificações: ICSA Labs, ICSA Firewall ou ICSA Antivírus ou detecção AV do Gateway.

1.20.2 O hardware da solução deverá ser homologado pela ANATEL.

1.21 SERVIÇO DE INSTALAÇÃO, ATUALIZAÇÃO E CONFIGURAÇÃO DA FERRAMENTA COM REPASSE DE CONHECIMENTO PARA 02 COLABORADORES

1.21.1 A capacitação deverá ser realizada no idioma português do Brasil.

1.21.2 O material didático utilizado para a capacitação deverá estar no idioma inglês ou português do Brasil.

1.21.3 A capacitação deverá possuir uma carga horária mínima de 16 (dezesseis) horas.

1.21.4 A capacitação deverá abordar, no mínimo, sobre a instalação, configuração, administração e resolução de problemas da solução ofertada.

1.21.5 A capacitação será realizada nas instalações da CONTRATANTE.

1.21.6 O licitante vencedor irá capacitar 02 (dois) colaboradores da CONTRATANTE.

1.22 GARANTIA E SUPORTE TÉCNICO

1.22.1 Garantia

1.22.1.1 A solução ofertada deverá estar coberta por garantia total fornecida pelo fabricante pelo prazo de 24 (vinte e quatro) meses.

1.22.1.2 O licitante vencedor deverá apresentar o Certificado de Garantia emitido pelo fabricante, no prazo de até 30 (trinta) dias corridos, a contar da data de recebimento definitivo da solução.

1.22.1.3 O licitante vencedor deverá possibilitar a abertura de chamado técnico diretamente no fabricante da solução.

1.22.1.4 O licitante vencedor deverá disponibilizar o acesso direto à base de dados de conhecimento do fabricante da solução que contenha informações de assistência, orientação para instalação, desinstalação, configuração, atualização de firmware e software, aplicação de correções (patches), diagnóstico, avaliações e resolução de problemas, e demais atividades relacionadas à correta operação, e funcionamento da solução.

1.22.1.5 O licitante vencedor deverá semestralmente revisar as atualizações de softwares (drivers, firmwares e microcódigos de todos os appliances contratados), que caso necessário, poderá ser realizada através de assistência remota para este item.
1.22.1.5.1 Os serviços de atualizações de firmwares somente deverão ocorrer para os eventos classificados como críticos.
1.22.1.5.2 Deverão ser entregues semestralmente análises e recomendações de patches e versões publicadas.

1.22.1.6 Os serviços cobertos pela garantia de hardware e software (exceto o disposto no item 1.25.1.4) deverão ser prestados nas instalações da CONTRATANTE (sistema ONSITE), pela empresa fabricante e/ou pelo licitante vencedor, sendo que os técnicos deverão ser certificados pelo fabricante da solução.

1.22.1.7 A empresa fabricante e/ou pelo licitante vencedor deverá fornecer a seus técnicos as ferramentas e instrumentos necessários à execução dos serviços, bem como produtos ou materiais indispensáveis à manutenção do equipamento.

1.22.1.8 A empresa fabricante e/ou pelo licitante vencedor deverá garantir atualizações do produto e suporte técnico (telefone, e-mail ou acesso remoto) pelo período de 24 (vinte e quatro) meses.

1.22.1.9 A substituição de equipamento defeituoso deverá ocorrer atendendo aos limites de tempo de SLA constados neste Termo de Referência, após a abertura de Ordem de Serviço pelo gestor de contrato ou notificação automática do sistema na central de atendimento do licitante vencedor ou fabricante.

1.22.1.10 A garantia iniciará a partir da data de recebimento definitivo da solução.

1.22.1.11 Em caso de defeito nos componentes dos equipamentos da aquisição em tela, além de solucionar o problema que causou o chamado, o técnico deverá revisar as partes elétricas e eletrônicas, efetuar limpeza interna, ajustes, regulagens, eliminação de eventuais defeitos, reparos, testes e substituição de peças defeituosas.

1.22.1.12 Caberá à empresa fabricante e/ou pelo licitante vencedor substituição de todas e quaisquer peças ou componentes necessários à total recuperação do equipamento, sem quaisquer ônus adicionais para CONTRATANTE.
1.22.1.12.1. Todas e quaisquer peças ou componentes utilizados para recuperação do equipamento, conforme citado no item anterior, deverão ser novas e originais;

1.22.1.13 Os serviços de garantia de funcionamento e assistência técnica deverão ser realizados diretamente pela empresa fabricante e/ou pelo licitante vencedor.

1.22.1.14 A garantia será prestada pela empresa fabricante e/ou pelo licitante vencedor nos endereços onde os EQUIPAMENTOS estiverem instalados, no horário local compreendido entre 08h00 (oito horas) e 18h00 (dezoito horas), de segunda a sexta-feira. Caso o problema comprometa a execução dos serviços, o fornecedor deverá realizar o atendimento a qualquer horário, com a presença de um técnico indicado pelo gestor do contrato.

1.22.1.15 A empresa fabricante e/ou pelo licitante vencedor deverá contar com central de atendimento para abertura de chamados, preferencialmente 0800, para abertura de chamado, devendo ser gerado número da solicitação para cada pedido realizado.

1.22.1.16 O chamado deverá ser iniciado em até 02 (duas) horas após ser registrado.

1.22.1.17 A empresa fabricante e/ou pelo licitante vencedor deverá oferecer, no mínimo, canais de comunicação e ferramentas adicionais de suporte online como “chat”, “e-mail” e página de suporte técnico

na Internet com disponibilidade de atualizações e “hotfixes” de drivers, BIOS, firmware, ferramentas de troubleshooting.

1.22.1.18 Anotar em registro próprio todas as ocorrências relacionadas com a garantia dos equipamentos, determinando o que for necessário à regularização dos defeitos observados;

1.22.1.19 Todos os equipamentos deverão atender integralmente as exigências das especificações técnicas do Termo de Referência em tela.

1.22.2 Suporte Técnico

1.22.2.1 Suporte 24x7 (24 horas por dia 7 dias por semana) tanto para suporte técnico Remoto e Telefônico.

1.22.2.2 Os serviços de suporte técnico serão prestados por profissionais especializados nas ferramentas contratadas.

1.22.2.3 O início das atividades de suporte técnico se dará após finalização da instalação e configuração e se restringem as ferramentas contratadas nessa proposta.

1.22.3 Níveis mínimos de SLA

1.22.3.1 Severidade Alta

1.22.3.1.1 Será considerado severidade alta nos casos onde ocorrer parada total dos equipamentos.

1.22.3.1.2 Prazo de máximo para atendimento/solução de 05 (cinco) Horas.

1.22.3.1.3 Serão abertos chamados, no caso de severidade alta, também, das 18h00 às 08h00 , através do modo telefônico.

1.22.3.2 Severidade Média

1.22.3.2.1 Será considerado severidade média nos casos onde o equipamento primário esteja parado/danificado.

1.22.3.2.2 Prazo de máximo para atendimento/solução de 12 (doze) Horas.

1.22.3.3 Severidade Baixa

1.22.3.3.1 Será considerado severidade baixa nos casos demais casos, como atualização de firmware e software, aplicação de correções (patches), entre outros.

1.22.3.3.2 Prazo de máximo para atendimento/solução de 24 (vinte e quatro) Horas.

1.23. Modelos de Referência - Em pesquisa de mercado encontramos as seguintes soluções que atendem ao Termo de Referência

1.23.1 Solução da marca Sophos com equipamentos modelo XG230 e X135.

1.23.2 Solução da marca SonicWall com equipamentos NGF NSa 2650 e NGF SOHO 250.

2. JUSTIFICATIVA

2.1 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.

2.2 Firewall é um dispositivo composto de software e/ou hardware, que limita o acesso à rede, dando credenciais de acesso apenas a aqueles que realmente devem fazer o acesso a informação. 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 vulnerabilidades que, eventualmente, sejam usadas para a entrada de "pragas digitais", é possível realizar o controle a nível de aplicação através de bloqueio ao acesso de programas não autorizados.

2.3 A compra mostra-se imprescindível em virtude da crescente demanda por segurança no acesso à rede mundial de computadores (internet). Atualmente, são diversos os tipos de ataques que são conhecidos na internet e ainda, assim, hackers conseguem obter sucesso pela não prevenção e a presença de equipamentos modernos e ativos que minimizam estes riscos, sendo assim, a OVG no intuito de aprimorar seus fundamentos de segurança da informação, tem como objetivo contratar não somente os ativos de rede (firewalls), mas, também, o suporte e garantia da solução, mantendo a base de ameaças atualizada, garantindo assim a proteção de seu bem mais precioso que são as informações armazenadas nesta Organização.

3. CONDIÇÕES PARA PARTICIPAÇÃO NO PROCESSO E HABILITAÇÃO

3.1 Poderão participar do presente processo de contratação quaisquer empresas interessadas, cujo ramo de atividade guarde pertinência e compatibilidade com o objeto pretendido.

3.2 As empresas interessadas em participar da presente contratação deverão encaminhar à Gerência de Compras, via e-mail ou na própria Gerência, além das Certidões de Regularidade, os documentos relacionados a seguir, conforme determinado no item 7.7 do Regulamento de Compras da OVG: Inscrição do Cadastro Nacional de Pessoa Jurídica – CNPJ, última alteração do Contrato ou Estatuto Social, desde que devidamente consolidada ou Contrato e Estatuto de Constituição acompanhado da última alteração contratual, documentos pessoais dos sócios ou dirigentes (RG e CPF), Procuração e documentos pessoais (RG e CPF) para representante da CONTRATADA, quando não forem os seus sócios que assinarão o Contrato a ser firmado.

3.3 Todas as empresas poderão apresentar propostas, mas somente serão contatados para negociação as que estiverem em situação regular com as Certidões de Regularidade com as Fazendas Públicas Federal (Fiscal e Previdenciária), Estadual (Estado de Goiás), Municipal (do Tomador e da Sede do fornecedor do serviço), FGTS (Caixa) e Certidão Trabalhista, salvo o disposto no item 7.12 do Regulamento para Aquisição de Bens, Materiais, Serviços, Locações, Importações e Alienações da OVG.

3.4 Em caso de descumprimento dos itens acima dispostos, as empresas serão automaticamente inabilitadas para Contratação, salvo em caso da exceção acima descrita.

3.5 Não será admitido neste processo a participação de fornecedor/prestador de serviços em processo de falência, sob concurso de credores, em dissolução ou em liquidação, ou ainda que se relacionem com dirigentes que detenham poder decisório na OVG, bem como com os elencados no Art. 08-C da Lei 15.503/2005.

3.6 Os participantes deverão fornecer todas as informações, mesmo que não solicitadas no Termo de Referência, relativas aos produtos ou serviço oferecido, como, por exemplo, manuais técnicos, rede credenciada de manutenção ou garantia, manual de instalação, características especiais de funcionamento ou prestação do serviço, etc.

3.7 As empresas interessadas em participar da presente contratação deverão fornecer os objetos a que se refere este Termo de Referência de acordo estritamente com as especificações aqui descritas, sendo de sua inteira responsabilidade a substituição do mesmo quando constatado no seu recebimento não estar em conformidade com as referidas especificações.

4. DAS PROPOSTAS

4.1 As propostas serão analisadas quanto ao cumprimento dos seguintes requisitos e deverão conter:
4.1.1 Razão social da proponente, CNPJ, endereço completo, inclusive eletrônico (e-mail), inscrição estadual e municipal;
4.1.2 Apresentar a descrição detalhada dos produtos, com o correspondente marca, modelo, valor unitário e total, incluindo o portfólio/folder do produto ofertado;
4.1.3 As propostas terão validade mínima de 60 (sessenta) dias corridos, contados da data da entrega na Gerência de Aquisição de Bens, Produtos e Serviços;
4.1.4 Os produtos/serviços deverão ser orçados com valores fixos para o período de vigência da contratação, apresentando preços correntes de mercado, sem quaisquer acréscimos em virtude de

expectativa inflacionária ou de custos financeiros, compreendidos todas as despesas incidentes sobre o objeto, tais como impostos, fretes, seguros, taxas, etc. e deduzidos os descontos eventualmente concedidos;
4.1.5 Juntamente com as referidas propostas deverá ser apresentado Atestado de capacidade técnica para comprovação de aptidão para fornecimento do objeto deste Termo de Referência, através de no mínimo 01 (um) atestado fornecido por pessoa jurídica de direito público ou privado, para a qual a interessada já tenha fornecido material de natureza compatível com o presente objeto.

4.2 Na Proposta deverá ser informado a conta bancária para pagamento (Banco, Agência e Conta).

4.3 Os preços apresentados nas propostas devem incluir todos os custos e despesas, tais como: custos diretos e indiretos, tributos incidentes, taxa de administração, serviços, encargos sociais, trabalhistas, seguros, treinamento, lucro, transporte, entrega e outros necessários ao cumprimento integral dos objetos deste Termo de Referência.

4.4 Será contratada a empresa que oferecer o menor valor global.

4.5 A OVG poderá em despacho fundamentado desclassificar propostas que apresentarem valores irrisórios ou excessivos em relação ao item cotado.

5. DO PRAZO DE ENTREGA E FORMA DE RECEBIMENTO

5.1 Os objetos desta aquisição deverão ser entregues em até 60 (sessenta) dias a contar da solicitação da OVG, respeitando-se as observações contidas em cada item constante deste Termo de Referência;
5.1.1 O serviço de instalação, atualização e configuração da ferramento com repasse de conhecimento para 02 colaboradores ocorrerá em até 15 (quinze) dias corridos após a entrega definitiva dos equipamentos e solicitação deste serviço pela OVG.
5.2. Entende-se por entrega as seguintes atividades: o transporte dos produtos embalados para a SEDE da OVG, a entrega dos volumes, o desembalar, a verificação visual do produto, um novo embalo e devolução, se for o caso;
5.2.1. Correrão por conta da CONTRATADA as despesas com a entrega conforme descrito no item anterior.
5.2.2. Os equipamentos deverão ser entregues de segunda a sexta-feira, exceto feriados, no horário de 08h00 às 12h00 e de 14h00 às 18h00, na sede da Organização das Voluntárias de Goiás – OVG, cito: Av. T-14, nº 249 - Qd 169 Lts 8/10 - Setor Bueno - 74230-130 - Goiânia – GO, Telefones: 3201-9455 / 3201-9405.

5.3. Os produtos serão objeto de inspeção, que será realizada por um profissional da GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO – GTI, conforme procedimentos a seguir:
5.3.1. Abertura das embalagens;
5.3.2. Comprovação de que o produto atende às especificações mínimas exigidas e/ou aquelas superiores oferecidas pela CONTRATADA;
5.3.3. Colocação do produto em funcionamento;
5.3.4. Teste dos componentes;
5.3.5. O período de inspeção será de até 04 (quatro) dias úteis;
5.3.6. Nos casos de sinais externos de avaria de transporte ou de mau funcionamento do produto, verificados na inspeção do mesmo, este deverá ser substituído por outro com as mesmas características, no prazo de até 15 (quinze) dias corridos, a contar da data de realização da inspeção;
5.3.7. Nos casos de substituição do produto, iniciar-se-ão os prazos e procedimentos estabelecidos neste Termo de Referência;

5.3.8 Correrão por conta da CONTRATADA as despesas com o frete, transporte, seguro e demais custos advindos da entrega dos produtos

5.3.9 As entregas não serão parciais, sendo as EMPRESAS/VENCEDORAS obrigadas a entregar todos os itens de uma só vez.

5.4. Será emitido Contrato ou Instrumento Equivalente para a aquisição do objeto em tela.

6. OBRIGAÇÕES DA CONTRATADA

6.1 Garantir a entrega dos equipamentos e softwares, bem como a execução dos serviços, nos prazos acordados e conforme estabelecido neste Termo de Referência;

6.2 Manter, durante a execução do contrato, todas as condições de habilitação e qualificação exigidas neste Termo de Referência, necessárias para que todos os acordos sejam concluídos com utilização eficiente dos recursos disponíveis;

6.3 Acatar e obedecer às normas de utilização e segurança das instalações;

6.4 Cumprir integralmente as cláusulas contratuais;

6.5 Responsabilizar-se pelos vícios e danos decorrentes do produto, de acordo com os artigos 12, 13, 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

6.6 Manter os seus técnicos informados quanto às normas disciplinares da OVG, exigindo sua fiel observância, especialmente quanto à utilização e segurança das instalações;

6.7 Manter os seus técnicos identificados por crachás, quando em trabalho, devendo substituir imediatamente aquele que seja considerado inconveniente à boa ordem ou que venha a transgredir as normas disciplinares da CONTRATADA;

6.8 Comunicar por escrito qualquer anormalidade, prestando à CONTRATADA os esclarecimentos julgados necessários;

6.9 Comprometer em manter em sigilo, ou seja, não revelar ou divulgar as informações confidenciais ou de caráter não público, recebidas durante e após a prestação dos serviços na CONTRATADA, tais como: informações técnicas, operacionais, administrativas, econômicas, financeiras e quaisquer outras informações, escritas ou verbais, fornecidas ou que venham a ser de nosso conhecimento, sobre os serviços licitados, ou que a ele se referem;

6.10 Todos os equipamentos deverão atender integralmente as exigências das especificações técnicas do Termo de Referência em tela.

7. OBRIGAÇÕES DA CONTRATANTE

7.1 Proporcionar à CONTRATADA os espaços físicos, instalações e os meios de comunicação necessários ao desempenho das atividades exigidas no Contrato ou instrumento equivalente, quando executados no ambiente físico da OVG;

7.2 Fornecer em tempo hábil, as informações necessárias e relevantes à execução do contrato ou instrumento equivalente;

7.3 Estabelecer normas e procedimentos de acesso às instalações da OVG;

7.4 Aprovar e receber os produtos/serviços executados pela CONTRATADA, quando de acordo com o contrato ou instrumento equivalente;

7.5 Acompanhar e fiscalizar o fiel cumprimento dos prazos e das condições de realização do presente contrato ou instrumento equivalente, comunicando à CONTRATADA as ocorrências, que a seu critério, exijam medidas corretivas;

7.6 Permitir acesso dos técnicos da CONTRATADA aos equipamentos e à OVG para execução dos serviços de implantação do projeto e suporte do ambiente computacional, desde que devidamente identificados;

7.7 Designar funcionário habilitado para a fiscalização e acompanhamento da execução dos serviços.

7.8 Receber o objeto no prazo e condições estabelecidas no termo de referência e seus anexos;
7.9 Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;
7.10 Comunicar à CONTRATADA, por e-mail ou portal de chamados WEB da CONTRATADA, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;
7.11 Acompanhar e fiscalizar o cumprimento das obrigações da CONTRATADA,
7.12 Efetuar o pagamento à CONTRATADA no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no termo em tela e seus anexos;
7.13 A CONTRATANTE não responderá por quaisquer compromissos assumidos pela CONTRATADA

com terceiros, ainda que vinculados à execução do presente Termo de Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da Contratada, de seus empregados, prepostos ou subordinados.

8. PENALIDADES

8.1 O fornecedor que descumprir com suas obrigações, injustificadamente, ficará sujeito às penalidades seguintes, as quais serão graduadas de acordo com a sua gravidade: impedimento e suspensão do direito de participar da seleção de fornecedores, multa, rescisão e outras previstas em legislação pertinente.

8.2 Nenhuma sanção será aplicada sem o devido contraditório, que prevê defesa prévia do interessado e recurso nos prazos definidos no Regulamento.

8.3 Após as aplicações de penalidades cabíveis, serão adotadas as medidas necessárias para a cobrança da multa, rescisão do contrato ou instrumento equivalente, registro do impedimento ou representação ao Ministério Público, conforme o caso.

9. DO PAGAMENTO

9.1 O pagamento será efetuado em até 28 (vinte e oito) dias após a emissão válida do documento fiscal correspondente (nota fiscal), devidamente preenchido, atestado e acompanhado das Certidões que comprovem a sua devida Regularidade Fiscal.

9.1.1 O documento fiscal somente será atestado e encaminhado para pagamento após o aceite formal da conclusão da entrega de toda a solução, o que contempla a entrega dos equipamentos e realização dos serviços de instalação, configuração, atualização e capacitação.

9.2 Todo e qualquer pagamento será efetuado, regra geral, através de transferência em conta corrente, devendo, portanto, os participantes informar banco, agência e nº de conta em sua proposta.

10. DISPOSIÇÕES FINAIS

10.1 O presente processo não importa necessariamente em contratação, podendo a OVG revogá-lo, no todo ou em parte, por razões de interesse privado, mediante ato escrito e fundamentado disponibilizado no site para conhecimento dos participantes. A OVG poderá, ainda, prorrogar, a qualquer tempo, os prazos para recebimento das propostas ou para sua abertura.

10.2 O fornecedor/prestador de serviço é responsável pela fidelidade e legitimidade das informações prestadas e dos documentos apresentados em qualquer fase do processo. A falsidade de qualquer documento apresentado ou a inverdade das informações nele contidas implicará na sua imediata desclassificação, ou caso tenha sido o vencedor, a rescisão do Contrato ou da Ordem de Compra, sem prejuízo das demais sanções cabíveis.

10.3 É facultado à OVG, em qualquer fase da contratação, promover diligências com vistas a esclarecer ou a complementar a instrução do processo.

10.4 Os fornecedores/prestadores de serviço intimados para prestar quaisquer esclarecimentos adicionais deverão fazê-lo no prazo determinado pela Gerência de Aquisição de Bens, Produtos e Serviços, sob pena de desclassificação.

10.5 As normas que disciplinam este Termo de Referência serão sempre interpretadas em favor da ampliação da disputa entre os proponentes, desde que não comprometam o interesse da OVG, a finalidade e a segurança da contratação.

10.6 A documentação apresentada pelos participantes fará parte do processo e não será devolvida ao proponente.

10.7 Os casos omissos neste Termo serão resolvidos pelas Diretorias Geral e Administrativa/Financeira, a qual a Gerência de Aquisição de Bens, Produtos e Serviços - GAPS está subordinada.

10.8 A Gerência de Aquisição de Bens, Produtos e Serviços atenderá aos interessados no horário comercial, de segunda a sexta feira, exceto feriados, na Gerência de Aquisição de Bens, Produtos e Serviços, localizada Rua T-14 esq. com T-38, nº 249 - Setor Bueno, Fone: 3201-9496 – CEP: 74.230-130, Goiânia–GO.

Documento assinado eletronicamente por **PEDRO HENRIQUE SOARES XIMENES**, **Assessor (a)**, em 31/03/2020, às 09:16, conforme art. 2º, § 2º, III, "b", da Lei 17.039/2010 e art. 3ºB, I, do Decreto nº 8.808/2016.

A autenticidade do documento pode ser conferida no site **http://sei.go.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=1** informando o código verificador **000012352367** e o código CRC **4A08C6E6**.

GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO
RUA T-14 249 - Bairro SETOR BUENO - CEP 74230-130 - GOIANIA - GO - S/C (62)3201-9405

Referência: Processo nº 201900058002499 SEI 000012352367