ESTADO DE GOIÁS
ORGANIZAÇÃO DAS VOLUNTÁRIAS DE GOIÁS - O V G
GERÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

TERMO DE REFERÊNCIA

Termo de Referência Nº 001/2025 -GTI - V2

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 o fornecimento do objeto descrito abaixo, de acordo com a legislação específica vigente.

A contratação será regida pelo REGULAMENTO PARA AQUISIÇÃO DE BENS, MATERIAIS, SERVIÇOS, LOCAÇÕES, IMPORTAÇÕES E ALIENAÇÕES – NORMA E PROCEDIMENTO – NP Nº. 006 de 25 de abril de 2024 disponível no site da OVG http://www.ovg.org.br e demais condições estabelecidas neste Termo.

1. OBJETO

1.1. Contratação de empresa para o fornecimento de solução de segurança do tipo Firewall de próxima geração (*Next Generation Firewall* - NGFW) completamente licenciada, com suporte especializado e treinamento oficial, pelo período de 60 (sessenta) meses, conforme quantitativos e descrições dispostas na tabela abaixo:

ITEM	Produto/Serviço	Descrição	Quantidade solicitada
01	Solução de firewall com gestão centralizada	Software de gerenciamento remoto da solução	1
02		Firewall Tipo 01 em HA	2
03		Firewall Tipo 02	3
04		Firewall Tipo 03	7
05	Treinamento Oficial do Firewall NGFW		1
06	Serviço de suporte especializado 24x7		1
07	Implantação e migração		1

2. DESCRIÇÃO DA NECESSIDADE

2.1. Comunicamos a necessidade de troca dos atuais firewalls Sophos, presentes na Organização, devido sua obsolescência e ao encerramento do suporte e garantia do fabricante (*end-of-life*).

2.2. Estes equipamentos não possuem licenciamento comercializável deixando-os com desempenho insuficiente para atender as demandas atuais de segurança, inclusive expondo a Organização a diversos riscos cibernéticos, sendo afetada a SEDE e as unidades CISF, CIGO, CIVV, EBV-1, EBV-2, GPROS/SEDE (Produção), GBA e PJTF, com possibilidade de paralização dos seguintes sistemas e recursos tecnológicos:

a) Sistemas de Controle de Doações;

b) de Gestão e Controle de Catracas dos Restaurantes;

c) Serviços executados aos beneficiários, tais como:

- Inscrição do ProBEM;
- Ações de atendimento aos jovens em situação de vulnerabilidade, como programa Meninas de Luz, e relacionados às atividades voltadas à terceira idade como, Centro DIA, ILPI.

d) Atividades no Banco de alimentos;

e) Gerenciamento de Voluntários e Parcerias Sociais;

f|) Casa do Interior de Goiás;

g) Gerencia de Benefícios sociais;

h) e outras ações desenvolvidas pela OVG, tanto as itinerantes atendimento as populações em vulnerabilidade social nos municípios do interior, quanto ao acompanhamento social das famílias necessitadas, causando prejuízos a sociedade goiana.

2.3. A contratação em tela objetiva a substituição por novos equipamentos firewalls para os pontos citados nos itens 2.2 e aquisição para 02 novas unidades: Chefatura (PROBEM) e EBV-3 (em construção).

2.4. A solução pleiteada inclui completo licenciamento; suporte no regime 24x7 para atender às necessidades das Unidades de Atendimento da OVG; suporte especializado, e o treinamento oficial do fabricante visando a transferência de conhecimento aos colaboradores que estarão diretamente envolvidos na administração da solução.

3. **DA ESPECIFICAÇÃO E DO QUANTITATIVO DO OBJETO**

3.1. **Das Características Gerais da Solução**

3.1.1. A solução ofertada deverá permitir o gerenciamento centralizado de todos os equipamentos;

3.1.2. Deverá ser composta de hardware ("*appliance*") de proteção de rede com funcionalidades de proteção de próxima geração e software licenciado, do mesmo fabricante;

3.1.2.1. Não serão admitidos equipamento servidores ("rack servers") e sistemas operacionais de uso genérico, como Microsoft Windows ou distribuições Linux;

3.1.2.2. Não serão admitidos soluções ofertadas do tipo software livre;

3.1.3. Os equipamentos e softwares deverão ser novos, de primeiro uso, e disponibilizados em suas versões mais atualizadas;

3.1.3.1. Nenhum dos modelos ofertados poderá estar listado no site da fabricante da solução como item “end-of-life”, “end-of-sale” ou outros status que denotem que a solução se encontra em processo de descontinuidade pelo seu fabricante.

3.1.4. Deverá ser do mesmo fabricante e possuir fonte de alimentação bivolt (100-240 VAC – 50/60 Hz);

3.1.4.1. Cada fonte de alimentação deverá ser capaz de sozinha suprir todo o equipamento em sua completa atividade;

3.1.4.2. Cada fonte deverá acompanhar cabo de alimentação (*power chord*), padrão 3 pinos NBR 14.136, com comprimento mínimo de 1,5 fim (um metro e meio);

3.1.5. Os equipamentos deverão ser próprios para montagem em rack 19” e deverão acompanhar o kit de suporte e fixação apropriados ou demais itens que sejam necessários para sua utilização em rack 19";

3.1.6. Os equipamentos de segurança, bem como, a gerência centralizada, deverão suportar monitoramento através de SNMP v2 e v3;

3.1.7. Deverá ser compatíveis com protocolos IPv4, IPV6, e de roteamento OSPFv2, e RIPv2;

3.1.8. Deverá possuir, no mínimo, 01 (uma) interface console do tipo UBS-C ou Ethernet (RJ-45);

3.1.9. Deverá possuir todas as interfaces de rede licenciadas e habilitadas para uso imediato;

3.1.10. Deverá permitir a integração com Active Directory;

3.1.11. Possuir as seguintes funcionalidades de Firewall:

3.1.11.1. A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede;

3.1.11.2. Deverá permitir a realização de upgrade via SCP, SFTP e https via interface WEB;

3.1.11.3. Deverá possuir pelo menos suporte a, no mínimo, VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast, DHCP Relay, DHCP Server;

3.1.11.4. Deverá possuir suporte a diferentes tipos de NAT, como Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;

3.1.11.5. Deverá possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

3.1.11.6. Deverá permitir a criação de regras de firewall e NAT utilizando nos campos de origem e destino, objetos de serviços online atualizáveis de forma dinâmica;

3.1.11.7. Deverá permitir o envio de logs para sistemas de monitoração externos;

3.1.11.8. Deverá prover mecanismo contra ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;

3.1.11.9. Deverá permitir a roteamentos unicast e multicast simultaneamente em uma única instância (contexto) de firewall.

3.1.11.10. Deverá permitir Autenticação integrada via Kerberos.

3.1.11.11. Deverá possuir a capacidade de operar através de uma única instancia de Firewall de forma simultânea mediante o uso das suas interfaces físicas nos seguintes modos: transparente, *mode sniffer* (monitoramento e análise o trafego de rede), camada 2 (L2) e camada 3 (L3);

3.1.11.12. Deverá permitir salvar as configurações das politicas para serem aplicadas em horários pré-definidos;

3.1.11.13. Deverá suportar redundância e balanceamento de links, tendo capacidade a no mínimo 3 links de internet.

3.1.11.14. Deverá suportar configurar um valor de *threshold* baseando-se em critérios mínimos como fator de decisão nas regras de balanceamento dos links.

3.1.11.15. Deverá permitir a configuração do tempo de checagem para cada um dos links.

3.1.12. Deverá permitir, sem ônus adicional, todas as atualizações de versão e releases dos softwares e firmwares que fazem parte da solução ofertada, durante todo o período do contrato;

3.2. **Do Software de gerenciamento Remoto da solução:**

3.2.1. O software de gestão poderá ser fornecido à parte dos equipamentos, para instalação em máquinas Físicas e/ou Virtuais, ou poderá ser fornecido como modelo SaaS (Software as a Service);

3.2.2. Deverá ser completamente licenciado para todo o período de vigência;

3.2.3. Deverá permitir a gestão centralizada e remota de todos os equipamentos descritos neste TR, do mesmo fabricante, independente se instalado em unidades distantes geograficamente;

3.2.4. Deverá permitir a gestão de novos equipamentos, mesmo se comprados posteriormente;

3.2.5. Deverá permitir a utilização simultânea de, no mínimo, 06 (seis) usuários;

3.2.6. Deverá ser fornecido com a integralidade de suas funções habilitadas, sem necessidade de aquisição posterior de licenças de software adicionais;

3.2.7. Deverá ser acessível via Autenticação de usuário, com suporte mínimo a, autenticação local com SSL e autenticação externa via LDAP, em especial por integração com Active Directory;

3.2.8. Deverá permitir o acesso de múltiplos usuários simultaneamente na solução;

3.2.9. Deverá permitir a validação de configurações de regras por meio de mecanismos e/ou ferramentas de diagnóstico, permitindo identificar erros nas políticas de segurança.

3.2.10. Deverá suportar a validação de regras antes de sua efetiva aplicação e deve realizar uma análise de regras já configuradas na solução que entrem em conflito ou que sobreponham/sejam sobrepostas pela regra que está sendo salva;

3.2.11. Deverá permitir auditar detalhadamente os logs, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

3.2.12. Deverá permitir salvar e exportar as configurações da solução, para fins de backup e restore;

3.2.13. Deverá permitir a reversão de mudanças de configuração, possibilitando a restauração da última configuração válida por meio de backups armazenados de forma automáticos.

3.2.14. Deverá permitir também o rollback de atualizações de sistema operacional, suportando no mínimo o rollback para a última versão do sistema operacional instalada antes da última atualização;

3.2.15. Deve mostrar os status dos firewalls em alta disponibilidade;

3.2.16. Deverá permitir configurar o envio de mensagens de alerta por parte da solução, via SNMP e via e-mail, permitindo assim o monitoramento do Firewall NGFW por meio de solução externa de monitoramento;

3.2.17. Caso a solução possua licenças relacionadas a capacidade de log indexados e armazenamento, deve ser ofertado a maior capacidade suportada ou ilimitada;

3.2.18. Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução;

3.2.19. Deverá ser capaz de gerenciar e administrar todas as funções descritas neste TR;

3.2.20. Deverá possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;

3.2.21. Deverá permitir a centralização da administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento;

3.2.22. Deverá suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS);

3.2.23. Deverá permitir que todos os logs da solução sejam indexados tanto localmente quanto na gerência centralizada, e se for o caso, seu licenciamento deve ser o de maior capacidade;

3.2.23.1. Para logs indexados localmente o armazenamento deverá limitado a capacidade do equipamento ofertado;

3.2.23.2. Para Logs indexados na gerência centralizada deverá permitir a utilização de uma capacidade mínima de 1TB (um Terabyte), considerando a centralização dos logs de todos os equipamentos;

3.2.24. Deverá permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores;

3.2.25. Deverá suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;

3.2.26. Deverá permitir a visualização dos logs de uma regra específica em tempo real e na mesma tela de configuração da regra selecionada ou em tela especifica de logs;

3.2.27. Deverá possibilitar a integração com outras soluções de SIEM;

3.2.28. Deverá permitir criação de relatórios customizados via interface gráfica, sem necessidade de conhecer linguagens de banco de dados;

3.2.29. Deverá prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware), e URLs que passaram pela solução;

3.2.30. Deverá ser possível exportar os logs em CSV ou TXT;

3.2.31. Deverá possibilitar a geração de relatórios de eventos no formato PDF ou HTML;

3.2.32. Deverá ser capaz de segmentar a base de regras em uma estrutura em camadas;

3.2.33. Deverá ser capaz de aplicar proteções relacionadas a ameaças e regras de acesso separadamente;

3.2.34. Deverá combinar configuração de políticas e análise de logs em um único painel, para evitar erros alcançando maior confiabilidade na alteração de politicas;

3.2.35. Deverá permitir a gestão de logs como:

3.2.35.1. Possibilitar rotação de logs, ou seja, mecanismo para que logs antigos sejam removidos automaticamente;

3.2.35.2. Possuir recurso de pesquisa em texto livre nos logs;

3.2.35.3. Deverá permitir a consolidação dos logs e relatórios de todos os dispositivos administrados;

3.2.36. Deverá possibilitar a visualização dos logs de Firewall, navegação web, conteúdo de arquivos, prevenção de ameaças e Sandbox, todos a partir de um único local centralizado possibilitando a procura correlacionada de logs em uma única tela, como por exemplo pesquisar logs de Antivirus e navegação web simultaneamente na mesma query de pesquisa.

3.2.37. Deverá suportar, no mínimo, a geração dos seguintes relatórios:

3.2.37.1. Resumo e gráfico de aplicações utilizadas;

3.2.37.2. Principais aplicações por utilização de largura de banda;

3.2.37.3. Principais aplicações por taxa de transferência de bytes;

3.2.37.4. Principais hosts por número de ameaças identificadas;

3.2.37.5. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Malware) de rede vinculadas a este tráfego;

3.2.38. Deverá permitir a criação de relatórios personalizados;

3.2.39. Deverá permitir a análise e otimização de regras e objetos, incluindo informações sobre regras e objetos não utilizados.

3.2.40. Deverá permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc;

3.2.41. Deverá possuir capacidade de integração com soluções de terceiros via API e também suportar configurações através de RestAPI.

3.2.42. Deverá prover, no mínimo, as seguintes funcionalidade para análise avançada dos incidentes:

3.2.42.1. Visualizar quantidade de tráfego utilizado de aplicações e navegação;

3.2.42.2. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

3.2.43. Deverá exibir uma dashboard de todos os dispositivos integrados, indicando o status sobre a geração de relatórios, monitoramento de alterações e análise de logs;

3.2.44. Deverá executar o monitoramento de alterações, análise e otimização de regras de políticas de segurança;

3.2.45. Deverá possuir a funcionalidade de verificação de regras de acesso, através de uma consulta de origem, destino e serviço, a solução deve apresentar se o tráfego está permitido, bloqueado ou parcialmente permitido/bloqueado, demonstrando os dispositivos no caminho, roteamento e interfaces;

3.2.46. Deverá suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tanto gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos;

3.2.47. Deverá permitir a monitoração de itens de configuração do sistema operacional dos dispositivos gerenciados;

3.2.48. Deverá permitir a comparação de configurações entre diferentes dispositivos ou no mesmo dispositivo, seja por meio de funcionalidades nativas ou utilização de ferramentas externas.

3.2.49. Deverá permitir o agendamento para a geração de relatórios dos dispositivos gerenciados;

3.2.50. Deverá ser possível fornecer uma lista de usuários de VPN dos dispositivos gerenciados.

3.2.51. A comunicação entre a solução e os dispositivos de segurança deve ser autenticada e criptografada;

3.2.52. Deverá ser capaz de migrar as regras e políticas de um dispositivo suportado para um substituto, mesmo que de modelo e fabricante diferentes;

3.2.53. Cada alteração nos dispositivos, deve ser identificado, no mínimo:

3.2.53.1. Alterações nas Regras (Criação, Remoção, Modificação);

3.2.54. Cada alteração nos dispositivos, deve ser identificado, no mínimo:

3.2.54.1. Alterações nas Regras (Criação, Remoção, Modificação);

3.2.54.2. Alteração nos Objetos de Redes e Serviços;

3.2.54.3. Alterações de Rotas ou Interfaces;

3.2.54.4. Visibilidade de toda alteração de configuração nos dispositivos;

3.2.55. Deverá possuir mecanismo para detectar login de administradores em horários irregulares;

3.2.56. Deverá ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

3.2.57. Deverá permitir a integração com servidores de autenticação LDAP Microsoft Active Directory, ou via Radius;

3.2.58. Deverá permitir criar certificados digitais para acesso dos usuários VPN;

3.2.59. Deverá permitir criar certificados digitais para VPNs Site-to-Site;

3.2.60. Caso a solução possua licenciamento relacionado a capacidade de criação de certificados, deve ser contemplado a sua maior capacidade ou ilimitada;

3.2.61. Deverá permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconheça os usuários de forma transparente;

3.2.62. Deverá possibilitar a procura por IPs e redes, sendo que os resultados mostrem estes IPs e redes nos campos de origem e destino do logs na mesma tela de pesquisa.

3.2.63. Deverá possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU;

3.3. **Licenciamento Firewalls 60 meses**

3.3.1. Deverá garantir suporte aprimorado diretamente com o fabricante;

3.3.2. Deverá licenciar todos os equipamentos fornecidos pelo período total de 60 (sessenta) meses;

3.3.3. Os equipamentos deverão ser fornecidos o pacote de licenciamento mais completo disponível para a solução, incluindo as funções abaixo;

3.3.4. **Virtual Private Network - VPN:**

3.3.4.1. Deverá permitir a criação de túneis virtuais criptografados (VPN) para acesso a recursos da rede interna da OVG por meio de uma rede pública, como a Internet;

3.3.4.2. Deverá suportar, pelo menos, os modos de configuração VPN site-to-site, e VPN client-to-site

3.3.4.3. Para a configuração de VPN site-to-site, a solução Deverá permitir a criação de túneis mesmo quando a outra ponta utilizar uma solução de segurança Firewall distinta da fornecida, sendo compatível, no mínimo, com as soluções de Firewall Palo Alto Networks, Fortinet, CheckPoint, Cisco Systems, e Sophos;

3.3.4.4. Deverá suportar a implementação de VPN IPSec com uso de diferentes algoritmos de Autenticação e encriptação, com suporte mínimo aos algoritmos *Data Encrypon Standard* (DES), *Advanced Encrypon Standard* (AES), SHA-256, SHA-512, Internet Key Exchange (IKEv1 e v2);

3.3.4.5. Deverá permitir a criação de VPN IPSec site-to-site tanto em modo padrão, com um único túnel VPN conectando-se a um único site remoto, quanto em modo “multisites”, com conexão VPN simultânea a dois ou mais sites remotos;

3.3.4.6. Para a configuração de VPN SSL client-to-site, a solução deverá permitir o usuário realizar a conexão à rede interna da OVG por meio de uma aplicação cliente instalada no sistema operacional do equipamento, ou por interface web por meio de Autenticação segura;

3.3.4.7. Nesta conexão, a solução deverá permitir Autenticação de usuário via LDAP, incluindo Microsoft Active Directory ou base de usuários local;

3.3.4.8. Nesta conexão, a solução deverá permitir atribuição de endereço IP e atribuição de DNS nos clientes remotos de VPN;

3.3.4.9. O software cliente deverá ser compatível com, no mínimo, os sistemas operacionais Microsoft Windows (32 ou 64 bits) na versão igual ou superior a 8.1, e MacOS na versão igual ou superior a 10.15;

3.3.5. ***Quality of Service*** **(QoS):**

3.3.5.1. Deverá suportar a criação de políticas de QoS por endereço de origem, endereço de destino e por porta;

3.3.5.2. Deverá possibilitar a definição de classes por banda garantida, banda máxima e fila de prioridade;

3.3.5.3. Deverá disponibilizar estatísticas em tempo real para classes de QoS;

3.3.6. **Proteção contra Ameaças Avançadas - Zero Day**

3.3.6.1. Deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT;

3.3.6.2. Deverá ser composta por hardware e software específicos (*appliance*) com sistema operacional especializado em sua versão mais atualizada ou nuvem do próprio fabricante que possui o conceito de *sandboxing* para prevenção de ataques *zero-day*. Não serão aceitas soluções em servidores ou software livre;

3.3.6.3. Não será aceita solução que dependa da estrutura de *hypervisor* do OVG para a análise de ameaças de dia zero, como Vmware ESXi, Microsoft HyperV, entre outros;

3.3.6.4. Deverá permitir bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS) e FTP via MTA durante análise completa do arquivo no ambiente *sandbox*;

3.3.6.5. Deverá ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;

3.3.6.6. Deverá Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URL´s conhecidas;

3.3.6.7. Deverá fornecer a capacidade de analisar e identificar ameaças em arquivos antes da entrega ao cliente, utilizando mecanismos avançados como sandboxing, machine learning ou análise de comportamento, sem dependência exclusiva de assinaturas em sistema Windows e Office.

3.3.6.8. Deverá fornecer as máquinas virtuais (Windows e pacote Office) integralmente instalados e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema;

3.3.6.9. Deverá possuir todas as atualizações necessárias para seu correto funcionamento providas pelo fabricante;

3.3.6.10. Deverá permitir o envio do conteúdo para a solução de *Sandboxing* de forma automática, sem a necessidade da interação do usuário/administrador para que o processo de analise seja realizado;

3.3.6.11. Deverá implementar atualização da base de dados de forma automática, permitindo agendamentos para o período de cada atualização;

3.3.6.12. Deverá ser habilitada e funcionar de forma independente das outras funcionalidades de segurança;

3.3.6.13. Deverá implementar análise em *sandbox*, detecção e bloqueio de malwares em arquivos executáveis, DLLs, ZIP, criptografados em SSL, e em arquivos java (.jar e class);

3.3.6.14. Deverá permitir gerar o relatório das emulações contendo print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;

3.3.6.15. Deverá implementar mecanismo de exceção, permitindo a criação de regras por VLAN, sub-rede e endereço IP;

3.3.6.16. Deverá implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido, também deverá permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, seven-z, exe rtf, csv, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, doc, docx, dot, docm, dotx, dotm e gz;

3.3.6.17. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real e o bloqueio deve ser imediato, não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;

3.3.6.18. Possibilitar remoção de conteúdo ativo dinâmicos como macros, URL's, Java scripts e outros dos arquivos baixados, permitindo o download do arquivo original caso ele não seja malicioso;

3.3.6.19. Deverá permitir a criação de listas de liberação ('Whitelists') com base em identificadores seguros de arquivos

3.3.6.20. Para melhor administração da solução, a solução deve possibilitar as visualizações a nível de monitoração de número de arquivos emulados, e número de arquivos com malware.

3.3.6.21. Deverá possuir capacidade de apresentar em seus logs, visibilidade de acordo com o framework ATT&CK Mitre Matrix, pontuando características de táticas e técnicas de acordo com a ameaça detectada/bloqueada pela solução ou mostrar relatório do VirusTotal. Caso a solução não possua determinada capacidade, poderá ser integrada com outra solução de mercado, não sendo ela soluções abertas;

3.3.6.22. Deverá prover informação, seja por meio de relatório ou log, sobre as situações de tamanho máximo do arquivo emulado excedido, e tempo máximo de emulação excedido.

3.3.7. **Prevenção de Ameaças - IPS;**

3.3.7.1. Deverá suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento de firewall;

3.3.7.2. Deverá possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;

3.3.7.3. Deverá sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/passivo;

3.3.7.4. Deverá suportar granularidade nas políticas de 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;

3.3.7.5. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo proteção para evitar consumo excessivo de CPU, garantido que o tráfego essencial continue fluindo.

3.3.7.6. Deverá possuir os mecanismos de inspeção de IPS de Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP *Defragmentation*, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

3.3.7.7. Deverá detectar e bloquear a origem de *portscans*;

3.3.7.8. Deverá bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

3.3.7.9. Deverá possuir assinaturas para bloqueio de ataques de *buffer overflow*;

3.3.7.10. Deverá suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

3.3.7.11. Deverá suportar bloqueio de arquivos por tipo;

3.3.7.12. Deverá identificar e bloquear comunicação com *botnets*;

3.3.7.13. Deverá suportar referência cruzada com CVE;

3.3.7.14. Deverá fornecer um mecanismo automatizado para ativar ou gerenciar novas assinaturas vindas de atualizações;

3.3.7.15. Deverá suportar exceções de rede com base na origem, destino, serviço ou uma combinação dos três;

3.3.7.16. Deverá incluir um modo de solução de problemas que defina o perfil em uso para detectar apenas, sem modificar as proteções individuais;

3.3.7.17. Deverá permitir o administrador poder ativar automaticamente novas proteções, com base em parâmetros configuráveis (gravidade da ameaça, proteção do cliente, proteção do servidor);

3.3.7.18. Deverá registrar na console de monitoração as informações sobre ameaças identificadas, como: o nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

3.3.7.19. Deverá apresentar, em sua própria interface, um sumário de todos os equipamentos que estão sendo gerenciados, assim como, qual o perfil ou grupo

3.3.7.20. Deverá possuir mecanismos para análise do tráfego e conexões realizadas para aplicações, permitindo identificar e recomendar ajustes nas assinaturas do IPS, a fim de otimizar a proteção contra ataques para aplicações expostas no ambiente.

3.3.7.21. Deverá permitir que o administrador seja capaz de configurar quais comandos FTP são aceitos e quais são bloqueados na funcionalidade de IPS;

3.3.7.22. Deverá possuir pelo menos dois perfis pré configurados pelo fabricante que permitam sua utilização assim que o equipamento for configurado;

3.3.7.23. Deverá incluir proteção contra vírus em conteúdo ActiveX e applets Java e *worms*;

3.3.7.24. Deverá proteger contra os ataques do tipo *DNS Cache Poisoning,* e impedir que os usuários acessem endereços de domínios bloqueados;

3.3.7.25. Deverá possuir engine onde irá determinar de forma automatica, onde qualquer nova assinatura que for baixada na base local deverá atuar em modo de prevenção ou detecção, assim evitará qualquer tipo de alteração na base de assinatura atual;

3.3.7.26. O antivírus deve oferecer suporte à verificação de links dentro de e-mails.

3.3.7.27. A solução de anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede quando usuário estiver conectado com ambiente externo malicioso

3.3.7.28. A solução deve permitir criar regras de exceção de acordo com a proteção, a partir do log visualizado na interface gráfica da gerência centralizada;

3.3.7.29. Para melhor administração a solução deve possuir a granularidade na classificação das proteções de IPS através de: severidade ou nível de confiança da proteção impacto da performance referência de indústria terceira e status de download recente;

3.3.7.30. Deverá permitir a criação de listas de liberação ('Whitelists') com base em identificadores seguros de arquivos

3.3.7.31. Deverá permitir que os eventos devem identificar o país de onde partiu a ameaça;

3.3.7.32. Deverá suportar rastreamento de vírus em arquivos PDF;

3.3.7.33. Deverá suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);

3.3.7.34. Deverá possuir a capacidade de prevenção de ameaças não conhecidas;

3.3.7.35. Em caso de falha no mecanismo de inspeção do Antivírus, deve ser possível configurar se as conexões serão permitidas ou bloqueada

3.3.7.36. A solução de Antivírus e Anti-Malware deverá funcionar de forma independente, ou seja, caso sejam desabilitadas, elas não podem causar a interrupção de outras funcionalidades de segurança como prevenção de ameaças avançadas (zero-day);

3.3.7.37. A solução deverá suportar bloqueio de trafego do protocolo CIFS/SMB;

3.3.7.38. Deverá suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;

3.3.7.39. Deverá possibilitar a visualização dos países de origem e destino nos logs dos acessos;

3.3.7.40. Deverá possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos, sejam resolvidas pelo Firewall com endereços previamente definidos, para interceptar a comunicação e bloquear o acesso do usuário.

3.3.7.41. A solução de Anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede.

3.3.7.42. Deverá possuir funcionalidade de identificação de bloqueio de trafego malicioso comunicando com C&C (command & Control);

3.3.8. **Controle de aplicações e Filtro de conteúdo WEB (URL Filtering):**

3.3.8.1. Deverá permitir o controle e monitoramento do acesso a sites de internet por parte dos usuários clientes da rede OVG;

3.3.8.2. Deverá funcionar de forma integrada às demais funcionalidades da solução Firewall NGFW, incluindo a de controle avançado de aplicações e, em especial, ao controle por meio de identificação de usuários, permitindo a integração de base de controle de usuários externas, como LDAP/Active Directory, assim como através de base de repositório de usuários local da solução;

3.3.8.3. Deverá possuir a capacidade de identificar de forma transparente o usuário de rede com integração ao Microsoft Active Directory, permitindo a criação de politicas de segurança baseadas nas informações coletadas entre elas, usuários, IP, grupos de usuários do sistema do Active Directory;

3.3.8.4. Deverá permitir o controle por usuários, grupos de usuários, IPs e redes;

3.3.8.5. Quando da integração com controle de diretório de usuários externo, os logs de acesso aos sites coletados pela solução devem registrar a identificação do usuário de rede, permitindo a consulta integrada dos acessos entre o repositório externo de usuários e os logs da solução Firewall NGFW;

3.3.8.6. Deverá possuir capacidade de criação de Políticas de filtro de conteúdo web baseadas em diferentes parâmetros, com suporte mínimo os itens de parametrização, tais como, Usuários e grupo de usuários, Zona de segurança, Rede e sub-redes, Endereços IP, Por URL, Categoria de URL;

3.3.8.7. Deverá possuir o recurso de configuração de período de execução da política, permitindo estabelecer dias e faixas de horários específicas em que a política de filtragem de URL esteja habilitada ou desabilitada no ambiente;

3.3.8.8. A página de bloqueio padrão da solução deve ser customizada, permitindo, por exemplo, a inserção do logotipo da OVG e registro de instruções para abertura de chamados para eventual liberação de site bloqueado;

3.3.8.9. Deverá possuir funcionalidade 'anti-phishing' integrada ao filtro de conteúdo web, permitindo o bloqueio de acesso a sites identificados como phishing e, preferencialmente, prevenindo o envio de credenciais por meio do bloqueio ao site.

3.3.8.10. Deverá permitir a liberação de URLs bloqueadas (“white list”), incluindo a exclusão do bloqueio por categoria de URL;

3.3.8.11. Deverá permitir a exibição de página de alerta para acesso a sites listados em “blacklists” de URLs, mas que não estejam explicitamente bloqueados pelo filtro URL da solução, possibilitando que o usuário acesse um site potencialmente arriscado clicando num botão do tipo "Continuar" ou “Avançar”;

3.3.8.12. Deverá permitir a classificação de nível de risco de URLs, com suporte mínimo a três níveis de risco aplicáveis, equivalentes aos riscos de nível “baixo”, “médio” e “alto”;

3.3.8.13. A categorização de sites Deverá permitir a associação da URL a mais de uma única categoria, assim como o uso de caracteres coringas (“Wildcards”);

3.3.8.14. Deverá permitir a criação de categorias de URLs customizadas;

3.3.8.15. Deverá permitir a criação e o uso de categorias de exceção, ou seja, categorias que permitem a aplicação de regras de exceção para, por exemplo, liberar o acesso a determinado site enquadrado em categoria bloqueada por uma determinada política de filtragem de URL (“override policy”);

3.3.8.16. As categorias de URL, incluindo as categorias customizadas, podem ser reaproveitadas em outros módulos da solução Firewall NGFW, permitindo, por exemplo, que se crie uma política de QoS que se aplique a uma determinada categoria de URL;

3.3.8.17. Deverá possuir pelo menos categorias de aplicações WEB pré-definidas pelo fabricante;

3.3.8.18. Para solução de filtro de conteúdo e controle web, deve ser capaz de bloquear na mesma aplicação um conteúdo específico sem bloquear a aplicação principal (Ex.: Whatsapp Web, Whatsapp voice e Whatsapp file transfer.);

3.3.8.19. Deverá possui mecanismo de controle de aplicação web e URL que possui configuração de bloqueio e liberação da aplicação principal e/ou as suas subcategorias. Quando o administrador da solução desejar bloquear apenas as subcategorias do facebook, como facebook chat, vídeo, game, compartilhamento de arquivos ou outros. Ou seja, não deve ser bloqueado toda a categoria como “Facebook” ou "Redes sociais" que também pode implicar o bloqueio não só do Facebook, mas também bloqueará tudo que estiver relacionado às redes sociais, como LinkedIn, Twitter , YouTube, etc. A solução precisa ser baseada em bloqueio de aplicações WEB que a própria base possui, assim a inspeção ocorrerá em camada 7 analisando o payload do pacote.

3.3.8.20. Deverá possuir a base de assinaturas de aplicações atualizadas automaticamente;

3.3.8.21. Deverá permitir o controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;

3.3.8.22. Deverá permitir o reconhecimento de aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

3.3.8.23. Deverá suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

3.3.8.24. Deverá permitir a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

3.3.8.25. Deverá reconhecer pelo menos 1.000 (mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, *update* de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

3.3.8.26. Deverá permitir a descriptografia de tráfego criptografado (SSL) a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

3.3.8.27. Deverá permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, através da própria console ou através de portal do fabricante.

3.3.8.28. Deverá suportar o recebimento eventos de autenticação para a identificação de endereços IP e usuários;

3.3.8.29. Deverá permitir o controle, sem instalação de cliente de software, em máquinas/computadores que solicitem saída à internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no Firewall (Captive Portal);

3.3.8.30. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela PROPONENTE desde que atendido todos os requisitos desta especificação;

3.3.9. **SDWAN**

3.3.9.1. Deverá balancear o tráfego das aplicações entre múltiplos links simultaneamente;

3.3.9.2. Deverá oferecer orquestração centralizada de políticas e gerenciamento para SD-WAN, permitindo a configuração e o controle de políticas de rede a partir de um único ponto, garantindo desempenho otimizado, segurança aprimorada e fácil

administração em toda a rede.

3.3.9.3. Deverá prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;

3.3.9.4. Deverá permitir a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote ou todos ao mesmo tempo;

3.3.9.5. Deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por mínimo icmp;

3.3.9.6. Deverá possibilitar a definição do link de saída para uma aplicação específica;

3.3.9.7. Deverá possuir suporte a Policy based routing ou policy based forwarding;

3.3.9.8. Deverá possibilitar a agregação de túneis IPSec, realizando balanceamento por conexão entre os túneis;

3.3.9.9. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, Facebook, etc), impactando no bom uso das aplicações de negócio, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de criar políticas de controle de banda.

3.3.9.10. Além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o match em IPs de origem e destino, usuários e portas;

3.3.9.11. Deverá prover estatísticas em tempo real a respeito da performance do health check (packet loss, jitter e latência);

3.3.9.12. Deverá possibilitar roteamento distinto a depender do grupo de usuário selecionado na regra de SD-WAN;

3.3.9.13. Deverá fornecer criptografia AES de 128 bits ou AES de 256 bits em sua VPN;

3.3.9.14. Deverá habilitar a mesma interface WAN para enviar tráfego simultaneamente por meio de túneis IPSec SD-WAN e nativamente fora dos túneis via underlay.

3.3.9.15. Deverá permitir que o orquestrador esteja na nuvem do fabricante ou seja instalado em um servidor dedicado, virtualizado utilizando uma máquina virtual, ou equipamento específico da mesma fabricante;

3.3.10. Caso o modelo de licenciamento da solução ofertada não seja do tipo “modular”, o licenciamento deverá habilitar todas as funções supracitadas;

3.4. **Firewall Tipo 01 em HA**

3.4.1. Deverá ser configurado 02 (dois) dispositivos físicos (appliances) interconectados e operando em modo de alta disponibilidade com suporte mínimo aos modos de configuração Ativo-Ativo ou Ativo-Passivo, sem a necessidade de licenciamento adicional;

3.4.2. A operação de alta disponibilidade deverá ocorrer, no mínimo, pelos seguintes parâmetros de detecção de anomalia:

3.4.2.1. Falha de funcionamento do dispositivo;

3.4.2.2. Falha de link, sendo capaz de monitorar a comunicação do HA peer dentro do tempo predeterminado no tráfego das suas interfaces (interface monitoring);

3.4.3. Durante a operação em modo de alta disponibilidade, os dispositivos deverão, no mínimo, sincronizar as seguintes informações entre si:

3.4.3.1. Sessões;

3.4.3.2. Certificados digitais;

3.4.3.3. configurações registradas em suas políticas de Firewall, incluindo em seus objetos de rede;

3.4.3.4. Políticas de QoS e de VPN;

3.4.3.5. configurações de NAT;

3.4.4. Deverá possuir, no mínimo, as seguintes interfaces de conexão de rede:

3.4.4.1. 04 (quatro) interfaces de rede 10 Gbps, padrão SFP+;

3.4.4.2. Deverá acompanhar, no mínimo, 02 (dois) *transceivers* homologados pela fabricante e compatíveis com o equipamento ofertado;

3.4.4.3. 10 (dez) interfaces de rede Ethernet, padrão RJ-45, Gigabit Ethernet (1 Gbps), distintas das 04 interfaces SFP+ anteriormente exigidas;

3.4.5. Deverá possuir, no mínimo, 01 (uma) porta USB 3.0;

3.4.6. Deverá possuir, no mínimo, 01 (uma) fan (ventoinha) para refrigeração do equipamento.

3.4.7. Deverá possuir 02 (duas) fontes de alimentação redundantes;

3.4.8. Todas as capacidades técnicas de processamento e de performance constantes a seguir deverão ser comprovadas por meio de publicação oficial de domínio público da fabricante, como Manuais de Operação ou “Datasheets”, facilmente encontrados no site da fabricante. Não serão aceitos documentos elaborados por terceiros, ou publicações em sites de terceiros;

3.4.9. Deverá possuir, no mínimo, as seguintes capacidades técnicas de processamento e de performance (Throughput):

3.4.9.1. 5 Gbps (cinco Gigabyte por segundo) para funcionalidade de firewall, prevenção de ameaças (*Threat Prevention*), controle de aplicação, Filtro URL, antivírus, e prevenção de ameaças avançadas de Zero-day;

3.4.9.2. 10 Gbps (dez Gigabyte por segundo) considerando as funcionalidades de Firewall do tipo Next Generation Firewall (NGFW);

3.4.9.3. 11 Gbps (onze Gigabyte por segundo) para *Throughput* na ferramenta de IPS;

3.4.9.4. 6 Gbps (seis Gigabyte por segundo) para *Throughput* de tráfego de VPN com criptografia AES-128 ou similar;

3.4.9.5. 100.000 (cem mil) conexões por segundo;

3.4.9.6. Os valores e capacidades supracitadas são consideradas para cada equipamento, não sendo admitida a soma das capacidades dos membros do cluster de alta disponibilidade;

3.4.10. Deverá estar licenciado e suportar, no mínimo, 1000 (mil) usuários para VPN SSL

3.5. **Firewall Tipo 02**

3.5.1. Deverá possuir, no mínimo, as seguintes interfaces de conexão de rede:

3.5.1.1. 06 (seis) interfaces de rede Ethernet, padrão RJ-45, Gigabit Ethernet (1 Gbps);

3.5.2. Todas as capacidades técnicas de processamento e de performance constantes a seguir deverão ser comprovadas por meio de publicação oficial de domínio público da fabricante, como Manuais de Operação ou "Datasheets", facilmente encontrados no site da fabricante. Não serão aceitos documentos elaborados por terceiros, ou publicações em sites de terceiros;

3.5.3. Deverá possuir, no mínimo, as seguintes capacidades técnicas de processamento e de performance:

3.5.3.1. 340 Mbps (trezentos e quarenta Megabyte por segundo) para funcionalidade de firewall, prevenção de ameaças (*Threat Prevention*), Controle de aplicação, Filtro de URL, antivírus, Anti-Bot, e prevenção avançada de ameaças Zero-day;

3.5.3.2. 670 Mbps (seiscentos e setenta Megabyte por segundo) para *Throughput* na ferramenta de IPS;

3.5.3.3. 600 Mbps (seiscentos Megabyte por segundo) considerando as funcionalidades de Firewall do tipo Next Generation Firewall (NGFW);

3.5.3.4. 900 Mbps (novecentos Megabyte por segundo) para *Throughput* de tráfego de VPN com criptografia AES-128 ou similar;

3.5.3.5. 10.000 (dez mil) conexões por segundo;

3.5.4. Deverá estar licenciado e suportar, no mínimo, 100 (cem) usuários para VPN SSL

3.6. **Firewall Tipo 03**

3.6.1. Deverá possuir, no mínimo, as seguintes interfaces de conexão de rede:

3.6.1.1. 08 (oito) interfaces de rede Ethernet, padrão RJ-45, Gigabit Ethernet (1 Gbps);

3.6.1.2. 01 (uma) interface de rede 1Gbps, do tipo SFP;

3.6.2. Todas as capacidades técnicas de processamento e de performance constantes a seguir deverão ser comprovadas por meio de publicação oficial de domínio público da fabricante, como Manuais de Operação ou "Datasheets", facilmente encontrados no site da fabricante. Não serão aceitos documentos elaborados por terceiros, ou publicações em sites de terceiros;

3.6.3. Deverá possuir, no mínimo, as seguintes capacidades técnicas de processamento e de performance:

3.6.3.1. 600 Mbps (seiscentos Megabyte por segundo) para funcionalidade de firewall, prevenção de ameaças (*Threat Prevention*), Controle de aplicação, Filtro de URL, antivírus, Anti-Bot, e prevenção avançada de ameaças Zero-day;

3.6.3.2. 1 Gbps (um Gigabyte por segundo) para *Throughput* na ferramenta de IPS;

3.6.3.3. 970 Mbps (novecentos e setenta Megabyte por segundo) considerando as funcionalidades de Firewall do tipo Next Generation Firewall (NGFW);

3.6.3.4. 1.900 Mbps (um mil novecentos Megabyte por segundo) para *Throughput* de tráfego de VPN com criptografia AES-128 ou similar;

3.6.3.5. 15.000 (quinze mil) conexões por segundo;

3.6.4. Deverá estar licenciado e suportar, no mínimo, 200 (duzentos) usuários para VPN SSL

3.7. **TREINAMENTO OFICIAL DO FIREWALL NGFW**

3.7.1. A PROPONENTE deverá prover a transferência de conhecimento por meio de treinamento técnico oficial do fabricante realizado em centro de certificação credenciado, sobre a solução de Firewall NGFW ofertada neste Termo de Referência a ser ministrada a funcionários da OVG, que atuarão diretamente na administração e operação da solução após sua implementação;

3.7.2. A transferência de conhecimento se dará de forma a repassar para os responsáveis do CONTRATANTE as informações necessárias do produto adquirido e da solução instalada e configurada, como atividades práticas como: instalação, configuração, administração e monitoramento da solução, contemplando todos os aspectos essenciais de funcionamento, operação e gerenciamento;

3.7.3. O treinamento deverá ser realizado para 04 (quatro) funcionários da OVG que serão designados;

3.7.4. O instrutor deve ser profissional certificado pelo fabricante dos produtos e com experiência comprovada nos produtos fornecidos;

3.7.5. Deverá possuir duração mínima: 3 (três) dias ou 24 (vinte e quatro) horas;

3.7.6. Início do treinamento: Em até 40 (quarenta) dias corridos, contados após a conclusão da instalação, ativação das licenças e correta migração das configurações da antiga solução Sophos. O prazo inicial poderá ser estendido, em caso de indisponibilidade de treinamento oficial no período, desde que a prorrogação seja previamente solicitada à OVG, com antecedência mínima de 05 (cinco) dias úteis, antes da data prevista para início de sua execução;

3.7.7. Deverá ser ministrado em horário comercial, preferencialmente, na modalidade presencial, nas instalações do fabricante ou do parceiro autorizado, devendo este, ser centro de treinamento oficial credenciado junto ao fabricante;

3.7.7.1. Visando a garantia do serviço prestado para os colaboradores à OVG, o treinamento, caso presencial, deverá ocorrer em dois momentos, sendo que haverá a participação de 02 (dois) colaboradores por vez;

3.7.7.2. O segundo treinamento, caso presencial, a ser realizado aos colaboradores que ainda não participaram poderá ser agendado conforme disponibilidade do treinamento com o prazo máximo de 08 (oito) meses para sua realização;

3.7.7.3. No caso de treinamento presencial eventuais despesas de deslocamento, hospedagem e alimentação dos instrutores do curso serão de responsabilidade integral da PROPONENTE. Já as eventuais despesas de deslocamento, hospedagem e alimentação dos participantes do curso serão de responsabilidade integral da OVG;

3.7.7.4. Não haverá impedimento da realização do treinamento da modalidade remota, desde que, o curso seja oficial e ministrado por centro de treinamento credenciado junto ao fabricante;

3.7.7.5. No caso de treinamento na modalidade remota, não haverá escalonamento de participação dos colaboradores da OVG, ou seja, o treinamento será ministrado para todos os participantes;

3.7.8. Todo material didático a ser utilizado deverá ser fornecido pela PROPONENTE ou pelo fabricante, devendo esse ser uma documentação oficial do próprio fabricante, seja por meio de mídia física (livros, apostilas, etc.) ou digital (PDF). O material deverá ser cedido individualmente a cada participante, de modo que ele possa levar consigo e consultá-lo posteriormente;

3.7.9. Deverá abranger tanto teoria quanto exercícios práticos, voltados para conhecimento da arquitetura da solução, sua implantação, configuração e gerenciamento, além de tratamento de problemas típicos envolvendo a operação da solução;

3.7.10. O escopo básico do treinamento deverá conter:

3.7.10.1. Arquitetura da solução;

3.7.10.2. Configurações iniciais básicas;

3.7.10.3. Alta disponibilidade;

3.7.10.4. Controle de acesso dos administradores da solução;

3.7.10.5. Configuração de Interfaces;

3.7.10.6. Criação e gerenciamento de Zonas de Segurança, Políticas de Segurança e Endereçamento NAT;

3.7.10.7. Controle por identificação de Aplicações;

3.7.10.8. Controle por identificação de Usuários, com conexão a fontes externas de Autenticação;

3.7.10.9. Criação e gerenciamento de filtro URL;

3.7.10.10. Controle avançado de ameaças;

3.7.10.11. Configurações de VPN (SSL e IPSec);

3.7.10.12. Monitoramento e Relatórios;

3.7.10.13. Logging e Auditoria;

3.7.10.14. Metodologia de diagnóstico e resolução de problemas (*troubleshooting*)

3.7.11. Deverá ser emitido certificado comprobatório da participação de cada funcionário da OVG ao final do treinamento. A apresentação destes certificados é requisito obrigatório para a comprovação da execução do serviço, sendo o principal artefato a ser utilizado pela equipe técnica de contratação para validação do serviço;

3.7.12. A PROPONENTE deverá apresentar o programa de capacitação e o cronograma com antecedência mínima de 30 (trinta) dias úteis antes de começar a capacitação;

3.8. **Serviço de suporte especializado 24x7 com implantação e migração**

3.8.1. A CONTRATADA deverá fornecer número telefônico, e-mail ou portal Web dedicado a abertura de chamados e demais solicitações de suporte técnico;

3.8.2. Os serviços de suporte técnico deverão contemplar as manutenções corretivas e evolutivas para a solução e não poderão acarretar custos adicionais a OVG, além do contratado, durante todo o período de vigência, ou seja, a CONTRATADA deverá se responsabilizar pelo pleno funcionamento, mantendo-os em operação;

3.8.3. Os serviços de suporte técnico deverão ser prestados em regime 24x7, ou seja, 24 horas por dia todos os dias do ano, e deverão ser realizados de forma remota:

3.8.3.1. Entende-se por suporte remoto o serviço de atendimento aos chamados técnicos, executados por meio telefônico, web ou e-mail, via central de help desk, em período integral;

3.8.3.2. Caso haja alguma ocorrência de severidade crítica (*descrita no Quadro de Severidade - Subitem 3.8.9*), cuja solução não possa ser aplicada remotamente, a CONTRATADA deverá encaminhar um técnico até as dependências da OVG visando a pronta resolução, sem custos adicionais;

3.8.4. Em todo atendimento técnico solicitado deverá ser fornecido o número do chamado na sua abertura bem como o responsável pela abertura e os motivos ou problemas referentes ao chamado;

3.8.5. Para a execução de atendimento, é necessária a autorização da OVG para instalação ou desinstalação de quaisquer softwares ou componentes em computadores da Organização;

3.8.6. Os técnicos de suporte da CONTRATADA devem ser capacitados e certificados, pelo fabricante dos produtos a prestar atendimento de suporte técnico;

3.8.7. Ainda poderão ser executadas as seguintes tarefas em relação à prestação do serviço de suporte:

3.8.7.1. Resolução de dúvidas sobre o produto;

3.8.7.2. Sugestão de melhorias na configuração;

3.8.7.3. Ativação/desativação de funcionalidades;

3.8.7.4. Resolução de pequenos problemas e ajustes na solução;

3.8.7.5. Sugestão de melhoria no desempenho dos equipamentos e da rede;

3.8.8. As solicitações de chamados técnicos serão sempre realizados pela OVG, diretamente à CONTRATADA que, no caso de haver Assistência Técnica Terceirizada, deverá tomar todas as providências necessárias ao pleno atendimento do chamado, obedecendo rigorosamente os prazos e condições aqui estabelecidos.

3.8.9. A CONTRATADA deverá manter o serviço de suporte técnico, disponível para a abertura e acompanhamento de chamados em tempo integral, 24 (vinte e quatro) horas por dia todos os dias do ano, inclusive sábados, domingos e feriados, com início de atendimento e prazo de solução de acordo com o nível mínimo de serviço e de severidade exigido para o caso, conforme os índices de criticidade abaixo:

SEVERIDADE	DESCRIÇÃO	1º Atendimento	Solução Paliativa	Solução Definitiva
		PRAZOS EM TEMPO CORRIDO A PARTIR DA NOTIFICAÇÃO		
Critica	Sistema parado ou produto inoperante com impacto direto nas operações críticas de negócio. Aplicado quando há a indisponibilidade total ou frequente da solução.	02 (duas) horas	04 (quatro) horas	06 (seis) horas
Alta	Alto impacto no ambiente de produção ou grande restrição de funcionalidade com instabilidade no funcionamento da solução, perda de redundância ou impossibilidade de efetuar novas configurações ou diagnósticos.	04 (quatro) horas	08 (oito) horas	12 (doze) horas
Média	O defeito não gera impacto ao negócio, ocorre quando há indisponibilidade de alguma funcionalidade da solução ou ocorrência de evento causando impacto limitado.	06 (quatro) horas	12 (Oito) horas	24 (Vinte e Quatro) horas
Baixa	Aplicado para a instalação, configuração, upgrade, update e esclarecimentos técnicos relativos ao uso e aprimoramento do software.	08 (Oito) horas	16 (Doze) horas	72 (Setenta e duas) horas

3.8.10. Serão considerados para efeitos dos níveis exigidos:

3.8.10.1. Prazo para Início de Atendimento: Tempo decorrido entre a abertura do chamado efetuado pelo funcionário designado pela OVG na Central de Atendimento da CONTRATADA e o efetivo início dos trabalhos de suporte técnico.

3.8.10.2. Prazo de Solução Provisória: Tempo decorrido entre a abertura do chamado efetuado pelo funcionário designado pela OVG na Central de Atendimento da CONTRATADA e a aplicação de procedimentos para atenuar o nível de criticidade de forma temporária até a solução definitiva.

3.8.10.3. Prazo de Solução Definitiva: Tempo decorrido entre a abertura do chamado efetuado pelo funcionário designado pela OVG na Central de Atendimento da CONTRATADA e a efetiva recolocação da solução em seu pleno estado de funcionamento;

3.8.10.4. Os prazos para Atendimento e Solução Definitiva estabelecidos acima, não se referem a falhas de software que necessitem de apoio da infraestrutura da OVG; nestes casos, os prazos serão acordados entre a OVG e a CONTRATADA, de forma que sejam realizados no menor prazo possível;

3.8.10.5. A CONTRATADA poderá solicitar ainda um prazo adicional, quando bem justificada a real necessidade, em função, por exemplo, de complexidade do serviço a ser executado, ficando a critério da OVG aceitar ou não as justificativas e o novo prazo apresentado pela CONTRATADA;

3.8.10.6. Caso a justificativa não atenda à OVG, prevalecerá o prazo inicialmente estipulado;

3.8.10.7. Os serviços a serem realizados aos sábados, domingos e feriados não implicarão em nenhuma forma de acréscimo ou majoração nos valores dos serviços, razão pela qual será improcedente a reivindicação de restabelecimento de equilíbrio econômico-financeiro, bem como, horas extras ou adicionais noturnos;

3.8.11. Cabe exclusivamente à CONTRATADA estruturar sua equipe de trabalho na dimensão que atenda as condições estabelecidas para a prestação do serviço;

3.8.12. **Da Instalação dos equipamentos**

3.8.12.1. Após a entrega dos equipamentos, iniciar-se-á a etapa de instalação, com prazo máximo de 45 (quarenta e cinco) dias, conforme estabelece o cronograma de entrega no Item 7.1.1 deste Termo;

3.8.12.2. A CONTRATADA procederá com a instalação da solução para a realização dos testes de funcionamento, na presença e supervisão de técnicos do OVG, sendo posteriormente aferido e testado o seu perfeito funcionamento;

3.8.12.3. A Instalação/Configuração dos equipamentos deverá ocorrer nas dependências da OVG, podendo ser realizada por profissional da CONTRATADA de forma presencial ou remota sob acompanhamento de profissionais da OVG;

3.8.12.4. Caso a Instalação/Configuração seja remota, caberá aos profissionais da OVG a fixação dos equipamentos, inclusive sua conexão com a internet para visando o início das atividades pela CONTRATADA;

3.8.12.5. Os locais de Instalação/Configuração compreendem os endereços abaixo:

3.8.12.6. Unidade SEDE - Avenida T-14, nº 249, Setor Bueno – Goiânia/GO;

3.8.12.7. Unidade PJTF - Avenida Cristóvão Colombo com Rua Manágua, s/n, Jardim Novo Mundo – Goiânia/GO;

3.8.12.8. Unidade GBA - Alameda dos Ciprestes, Res. Barravento – Goiânia/GO (Acesso ao CEASA);

3.8.12.9. Unidade CISF - Av. Alameda do Contorno, nº 3.038, Jardim Bela Vista – Goiânia/GO;

3.8.12.10. Unidade CIVV - Rua 267 com 270-A, Setor Coimbra – Goiânia/GO;

3.8.12.11. Unidade EBV1 - Rua Palmares, entre CM-08 e CM-10, Setor Cândida de Morais – Goiânia/GO;

3.8.12.12. Unidade EBV2 - Avenida Contorno esq. com Rua 44, Setor Norte Ferroviário – Goiânia/GO;

3.8.12.13. Unidade EBV3 - Av. do Povo com Rua São Domingos, Qd. 33, Vila Mutirão II - Goiânia/GO;

3.8.12.14. Chefatura - Praça Dr. Pedro Ludovico Teixeira, nº 26 (Antiga Chefatura de Polícia – Praça Cívica) – Goiânia/GO;

3.8.12.15. Unidade CIGO - Rua R-03, nº 120, Setor Oeste – Goiânia/GO;

3.8.12.16. Unidade GPROS - Rua Benjamin Constant, Qd 114, 812, St. Campinas – Goiânia/GO;

3.8.12.17. Compreende-se, nesta etapa, a instalação de equipamentos, sistemas, softwares e aplicativos dos PRODUTOS ofertados pela CONTRATADA, bem como a migração das configurações existentes nos equipamentos Firewall SOPHOS (antigos) da OVG para os novos PRODUTOS ofertados;

3.8.12.18. A migração das regras de segurança deverá ser realizada de forma automatizada, quando possível, com uso de software/script desenvolvido especificamente para este fim, com vistas a minimizar o impacto de um possível erro humano nas migrações de configurações.

3.8.12.19. Durante a migração os equipamentos antigos da OVG deverão permanecer ativos, sendo desativados apenas após a completa migração e posterior validação das regras e funcionamento entre os técnicos da CONTRATADA e OVG;

3.8.12.20. Durante a migração a CONTRATADA deverá realizar a avaliação das regras em uso, e se for o caso, para melhoria do desempenho e eficácia das regras, propor e executar mudanças ou melhorias nas mesmas;

3.9. **Da Garantia**

3.9.1. Deverá ser fornecida garantia para os equipamentos ofertados junto a FABRICANTE, no mínimo, pelo período de 60 (sessenta) meses;

3.9.2. Deverá englobar a troca de peças em caso de falha nos equipamentos.

4. DAS CONDIÇÕES PARA PARTICIPAÇÃO NO PROCESSO E HABILITAÇÃO

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

4.1.1. Inscrição do Cadastro Nacional de Pessoa Jurídica – CNPJ;

4.1.2. Prova de regularidade para com a fazenda federal, mediante certidão conjunta de débitos relativos a tributos federais e da dívida ativa da união, que abranja inclusive a regularidade relativa às contribuições previdenciárias e sociais.

4.1.3. Prova de regularidade para com a fazenda estadual de Goiás, mediante certidão negativa de débitos relativos aos tributos estaduais.

4.1.4. Prova de regularidade relativa ao fundo de garantia por tempo deverá serviço – FGTS, através da apresentação do certificado de regularidade do FGTS – CRF.

4.1.5. Prova de regularidade com a Justiça do Trabalho – CNDT.

4.1.6. Prova de regularidade para com a fazenda municipal do tomador ou da sede do fornecedor, mediante certidão negativa de débitos relativos aos tributos municipais, no caso de obras e serviços.

4.2. Os participantes deverão fornecer todas as informações, mesmo que não solicitadas no Termo de Referência, relativas ao produto 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.

4.3. As empresas interessadas em participar da presente contratação deverão fornecer o objeto 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.

4.4. Não será admitido neste processo a participação de fornecedor/prestador deverá serviços em processo de falência, sob concurso de credores, em dissolução ou em liquidação.

4.5. **Não será admitido neste processo a participação de fornecedor/prestador deverá serviços 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, estando a proponente de acordo com os termos do presente Termo de Referência, no encaminhamento da proposta comercial.**

4.6. **Qualificação técnica mínima exigida:**

4.6.1. A PROPONENTE, junto com os documentos de habilitação, deverá comprovar capacitação técnico-operacional através de um ou mais atestados, expedidos por pessoa jurídica de direito público ou privado, mencionando que forneceu, de forma satisfatória, os produtos e serviços com características semelhantes às do objeto deste Edital;

4.6.2. A CONTRATANTE se resguarda no direito de diligenciar junto à pessoa jurídica emitente do atestado/declaração de capacidade técnica, visando a obter informações sobre os produtos fornecidos e/ou serviços prestados, cópias dos respectivos contratos/aditivos e/ou outros documentos comprobatórios do conteúdo declarado.

4.6.3. Caso a proponente não seja o próprio fabricante da solução, deverá apresentar comprovação de parceria junto à fabricante.

5. DAS PROPOSTAS COMERCIAIS

5.1. As propostas serão analisadas quanto ao cumprimento dos seguintes requisitos e deverão conter:

5.1.1. Razão social da proponente, CNPJ, endereço completo, inclusive eletrônico (e-mail);

5.1.2. Apresentar a descrição detalhada dos produtos/serviços, com o correspondente valor unitário e total;

5.1.3. As propostas terão validade mínima de 60 (sessenta) dias corridos, contados da data da entrega na Gerência de Aquisição de Bens, Produtos e Serviços.

5.1.4. Indicar a marca/fabricante do objeto ofertado.

5.1.5. Os produtos/serviços deverão ser orçados com valores fixos para o período de vigência da contratação, apresentando preços correntes de mercado, sem quaisquer acréscimos de custos financeiros e deduzidos os descontos eventualmente concedidos.

5.1.6. A proposta deverá ser apresentada em língua portuguesa e moeda nacional, com somente duas casas decimais após a vírgula.

5.2. 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, bem como a entrega e outros necessários ao cumprimento integral do objeto deste Termo de Referência.

5.3. A OVG poderá em despacho fundamentado desclassificar propostas que apresentarem valores inexequíveis.

6. DO TIPO DO JULGAMENTO

6.1. Será contratada a empresa que oferecer o menor preço global;

7. **DO PRAZO DE ENTREGA E FORMA DE RECEBIMENTO**

7.1. A solução deverá ser entregue conforme cronograma e prazo de entrega descritos no subitem 7.1.1, observando-se as condições deste Termo:

7.1.1. Cronograma de entrega de equipamentos e implantação da solução de segurança do tipo Firewall de próxima geração (*Next Generation Firewall* - NGFW):

Item	Descrição	Prazo
01	Entrega dos equipamentos e componentes que compõe a solução	até 60 dias após solicitação da OVG
02	Homologação da Solução	até 45 dias após a entrega dos equipamentos

7.2. Os produtos deverão ser entregues na Sede da OVG, localizada na Avenida T-14, nº 249, Setor Bueno, Goiânia-GO.

7.3. Os materiais/produtos deverão ser novos, de 1ª qualidade e entregues em perfeitas condições, não podendo estar danificado(s) por qualquer lesão de origem física ou mecânica que afete a sua aparência/embalagem, sob pena de não recebimento deles.

7.4. A contratada deverá estar ciente de que o ato do recebimento não implicará na aceitação do objeto que vier a ser recusado por apresentar defeitos, imperfeições, alterações, irregularidades e reiterados vícios durante o prazo de validade/garantia e/ou apresente quaisquer características discrepantes às descritas neste Termo de Referência.

7.5. Verificando-se defeito(s) no(s) produto(s), a empresa será notificada para sanar ou substituí-lo(s), parcialmente ou na sua totalidade, a qualquer tempo, no prazo máximo de 15 (quinze) dias, às suas expensas, ainda que constatado depois do recebimento definitivo.

7.5.1. Caso a contratada entregue o quantitativo inferior ao solicitado, a mesma deverá complementá-lo em até 02 (dois) dias

7.6. O objeto da contratação será acompanhado por funcionário responsável, designado pela OVG.

7.7. O transporte e a descarga dos produtos no local designado correrão por conta exclusiva da empresa contratada, sem qualquer custo adicional solicitado posteriormente.

7.8. A recusa injustificada da Contratada em entregar o objeto no prazo e/ou quantitativo estipulado caracteriza descumprimento total da obrigação assumida, sujeitando-o às penalidades previstas neste Termo.

7.9. Os serviços contratados poderão ser prestados tanto no ambiente da CONTRATADA quanto nas dependências do CONTRATANTE, variando a condição de acordo com os requisitos especificados. Em regra, visando evitar o deslocamento de colaboradores da OVG, os serviços que demandem interação presencial entre a equipe da CONTRATADA e o CONTRATANTE deverão ser executados, preferencialmente, no ambiente da ORGANIZAÇÃO DAS VOLUNTÁRIAS DE GOIÁS - OVG.

7.9.1. O endereço de referência para execução presencial é a Gerência de Tecnologia da Informação, localizada na Rua T-14, nº 249, Setor Bueno - Goiânia - Goiás.

7.9.2. A execução dos serviços deverá ser iniciada após a entrega dos equipamentos, respeitando as condições e prazos de atendimentos estabelecidos neste Termo de Referência.

7.10. A definição do horário de trabalho para a execução das atividades presencialmente nas instalações do CONTRATANTE ocorrerá, preferencialmente, considerando os horários de expediente a OVG, ou mediante acordo entre as partes, desde que atendidas as necessidades do CONTRATANTE.

7.11. As atividades que demandem qualquer tipo de serviço que possam gerar impacto no funcionamento da Organização e/ou de seus sistemas, deverão ser executadas prioritariamente fora do horário normal de expediente.

7.11.1. Sendo que, todo e qualquer serviço eventualmente executado fora do horário de expediente, aos sábados, domingos e feriados, seja no ambiente da CONTRATADA ou no ambiente do CONTRATANTE, não implicarão nenhum acréscimo ou majoração nos valores devidos à CONTRATADA.

8. **DO PAGAMENTO**

8.1. O pagamento será efetuado em até 30 (trinta) dias após entrega dos produtos/serviços e emissão válida do documento fiscal correspondente (nota fiscal, recibo ou equivalente), devidamente preenchido e atestado pelo Gestor indicado pela OVG.

8.2. Referente ao Item 06 do Objeto do Contrato (*Serviço de suporte especializado 24x7*), o valor a ser pago pelo serviço, será dividido em 05(cinco) parcelas anuais fixas, sendo que os pagamentos anuais deverão ocorrer em até 30 (trinta) dias após a emissão do documento fiscal (nota fiscal, recibo ou equivalente), correspondente ao respectivo ciclo da futura prestação do serviço.

8.3. O pagamento será efetuado, através de transferência em conta corrente, devendo, portanto, os participantes informar banco, agência e nº de conta em sua proposta.

8.3.1. A conta bancária deverá ser de titularidade da Contratada.

8.3.2. Deverá acompanhar as notas fiscais, regularidade fiscal e trabalhista exigidas para a contratação.

8.4. Os documentos que apresentarem incorreção, serão devolvidos à Contratada para regularização, reiniciando-se novos prazos para pagamentos, a contar da reapresentação devidamente corrigida.

8.5. Deverá constar nas notas fiscais a seguinte anotação: CONTRATO DE GESTÃO Nº. 001/2011-SEAD.

8.6. As notas fiscais deverão destacar as retenções de impostos conforme legislação.

9. **DAS OBRIGAÇÕES DA CONTRATADA**

9.1. Todos os encargos decorrentes da execução do ajuste, tais como: obrigações civis, trabalhistas, fiscais, previdenciárias assim como despesas com transporte distribuição e quaisquer outras que incidam sobre a contratação, serão de exclusiva responsabilidade da contratada.

9.2. Prestar todos os esclarecimentos que lhe forem solicitados pela OVG no que referir-se ao objeto, atendendo prontamente a quaisquer reclamações.

9.3. Providenciar a imediata correção das deficiências, falhas ou irregularidades constatadas, sem ônus para a OVG, caso verifique que os mesmos não atendem as especificações deste Termo.

9.4. Comunicar, por escrito e imediatamente, ao fiscal responsável, qualquer motivo que impossibilite a entrega do objeto, nas condições pactuadas.

9.5. Refazer, sem custo para a OVG, todo e qualquer procedimento, se verificada incorreção e constatado que o erro é da responsabilidade da contratada.

9.6. Garantir o funcionamento da solução, incluindo hardware e software, durante o período contratado, observando a execução dos serviços, nos prazos acordados e conforme estabelecido no Item 3.8.10 e 3.8.9 deste Termo de Referência;

9.7. Comunicar formalmente qualquer anormalidade, prestando à OVG os esclarecimentos julgados necessários;

9.8. Informar à OVG toda ocorrência que esteja prejudicando a prestação dos serviços e o cumprimento dos níveis de qualidade acordados;

9.9. Comprometer em manter sigilo, ou seja, não revelar ou divulgar as informações confidenciais ou de caráter não público recebidas durante e após a prestação dos serviços na OVG, tais como: informações técnicas (rede, IPs, sistemas), operacionais, administrativas, econômicas, financeiras e quaisquer outras informações, escritas ou verbais, fornecidas ou que venham a ser de conhecimento da OVG sobre os serviços contratados, ou que a ele se referem;

9.10. Executar continuamente serviços de operação e manutenção, durante a vigência do contrato, incluindo, mas não se limitando, as seguintes atividades:

9.10.1. Atualizações de Firmware;

9.10.2. Criação e otimização de regras de firewall, IPS;

9.10.3. Configuração e otimização dos equipamentos;

9.10.4. Realização de rotina de backup;

9.10.5. Integração com sistemas SIEM, ou demais ferramentas adquiridas posteriormente;

9.11. Implementar soluções preventivas e corretivas para evitar a repetição de incidentes/problemas/erros recorrentes;

10. **DAS OBRIGAÇÕES DO CONTRATANTE**

10.1. Dar conhecimento à contratada de quaisquer fatos que possam afetar a entrega do objeto.

10.2. Verificar se os produtos entregues pela contratada atendem todas as especificações contidas no Termo de Referência e Anexos.

10.3. Notificar à contratada, formalmente, caso os materiais estejam em desconformidade com o estabelecido no Termo de Referência e Anexos, para que essa proceda às correções necessárias.

11. **DA FORMALIZAÇÃO DA CONTRATAÇÃO**

11.1. O contrato terá vigência de 60 meses.

12. **DAS INFRAÇÕES E SANÇÕES ADMINISTRATIVAS**

12.1. A empresa declarada “provisoriamente” vencedora da cotação ou o contratado poderá ser responsabilizado e apenado, conforme descrito no item 17 do Regulamento para Aquisições da OVG.

13. **DA IMPUGNAÇÃO E DO RECURSO ADMINISTRATIVO**

13.1. O procedimento de aquisição de bens, serviços, locações, importações e alienações é passível de impugnação por irregularidade na aplicação do Regulamento, ou solicitação de esclarecimentos, devendo o pedido ser encaminhado via e-mail ao setor de Aquisição de Bens, Produtos e Serviços - GAPS até 24 (vinte e quatro) horas antes do encerramento do prazo para apresentação das propostas.

13.1.1. A resposta à impugnação ou pedido de esclarecimento será encaminhada via e-mail ao interessado.

13.2. O fornecedor ou prestador deverá serviço que não concordar com o resultado da habilitação/inabilitação e/ou do julgamento das propostas terá o prazo de 02 (dois) dias, contados a partir da comunicação da respectiva decisão para a propositura do recurso.

13.2.1. Nos demais casos, o prazo recursal de 02 (dois) dias dar-se-á a partir da publicação do contrato.

14. **DA GESTÃO E FISCALIZAÇÃO DO CONTRATO/ORDEM DE COMPRAS**

14.1. A gestão/fiscalização do Contrato ficará a cargo do setor solicitante da contratação ou a quem a Diretoria indicar, conforme descrito no item 16 do Regulamento para Aquisições da OVG.

15. **DO SIGILO E DE PROTEÇÃO DE DADOS – LEI Nº 13.709/2018**

15.1. A CONTRATANTE / CONTRATADA, além de guardarem sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato, se comprometem a adotar as melhores práticas para respeitar a legislação vigente e/ou que venha entrar em vigor sobre proteção de dados, sendo certo que se adaptará, inclusive, à Lei nº 13.709/2018, Lei Geral de Proteção de Dados (LGPD).

15.2. A CONTRATANTE e CONTRATADA se obrigam ao dever de confidencialidade e sigilo relativamente a toda a informação e/ou dados pessoais a que tenha acesso por virtude ou em consequência das relações profissionais, devendo assegurar-se de que os seus colaboradores, consultores e/ou prestadores deverá serviços que, no exercício das suas funções, tenham acesso e/ou conhecimento da informação e/ou dos dados pessoais tratados, se encontram eles próprios contratualmente obrigados ao sigilo profissional.

15.3. As partes de obrigam a realizar o tratamento de dados pessoais de acordo com as disposições legais vigentes, bem como nos moldes da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), visando dar efetiva proteção aos dados coletados de pessoas naturais que possam identificá-las ou torná-las identificáveis, utilizando-os de tais dados tão somente para os fins necessários à consecução do objeto do Contrato, ou nos limites do consentimento expressamente manifestado por escrito por seus respectivos titulares.

15.4. A CONTRATANTE e a CONTRATADA se responsabilizam, única e exclusivamente, acerca da utilização dos dados obtidos por meio do contrato, sendo terminantemente vedada a utilização de tais informações para fins diversos daqueles relativos ao objeto do contrato, bem como outros fins ilícitos, ou que, de qualquer forma, atendem contra a moral e os bons costumes.

15.5. A OVG não será, em qualquer hipótese, responsabilizada pelo uso indevido por parte da CONTRATADA e/ou terceiros, com relação a dados armazenados em seus softwares e bancos de dados.

15.6. A CONTRATADA não poderá utilizar a informação e/ou os dados pessoais a que tenha acesso para fins distintos do seu fornecimento/prestação deverá serviços à OVG, não podendo, nomeadamente, transmiti-los a terceiros

15.7. A OVG NÃO IRÁ COMPARTILHAR NENHUM DADO DAS PESSOAS NATURAIS, SALVO AS HIPÓTESES EXPRESSAS DA LEI Nº 13.709/2018, QUE PERMITEM O COMPARTILHAMENTO SEM CONSENTIMENTO DO TITULAR.

15.8. O dever de sigilo e de confidencialidade e as restantes obrigações previstas no presente item, deverão permanecer em vigor mesmo após o término de vigência do contrato.

15.9. Eventuais violações externas que atinjam o sistema de proteção da OVG, serão comunicadas aos titulares, bem como a Autoridade Nacional de Proteção de Dados - ANPD.

15.10. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

15.10.1. Cumprimento de obrigação legal ou regulatória pelo controlador;

15.10.2. Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

15.10.3. Transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na Lei; ou

15.10.4. Uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

16. **DISPOSIÇÕES FINAIS**

16.1. 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.

16.2. O fornecedor/prestador deverá 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/serviços, sem prejuízo das demais sanções cabíveis.

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

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

16.5. 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.

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

16.7. Caso de rescisão contratual por descumprimento das obrigações pactuadas, a OVG poderá convocar o segundo colocado na ordem de classificação da cotação, caso o valor esteja dentro do “preço de referência” e entendendo ser vantajoso para a organização.

16.8. A Contratada fica obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem nos serviços, até 25% (vinte e cinco por cento) do valor inicial do contrato e, no caso particular de obra, reforma de edifício ou de equipamento, até o limite de 50% (cinquenta por cento) para os seus acréscimos.

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

16.10. A OVG poderá adotar por analogia, quando necessário, normas gerais de contratações disciplinadas por legislação pertinente.

16.11. O vencedor da cotação só será declarado após Despacho favorável da Gerência de Controle Interno e Parecer favorável da Assessoria Jurídica e assinatura na Ordem de compras/serviços ou Contrato.

16.12. PARA ASSINATURA DO CONTRATO E/OU ORDEM DE COMPRAS, A EMPRESA (REPRESENTANTE LEGAL RESPONSÁVEL) DEVERÁ POSSUIR ASSINATURA DIGITAL/ELETRÔNICA, PREFERENCIALMENTE, CADASTRO NO SEI GOIÁS – SISTEMA ELETRÔNICO DE INFORMAÇÕES DO ESTADO DE GOIÁS.

16.12.1. O CADASTRO NO SEI (GOIÁS) PODERÁ SER REALIZADO ATRAVÉS DO LINK - https://sei.goias.gov.br/como_se_cadastrar-externo.php

16.13. Gerência de Aquisição de Bens, Produtos e Serviços – GAPS atenderá aos interessados no horário comercial, de segunda a sexta feira, exceto feriados, na sala da Gerência de Aquisição de Bens, Produtos e Serviços – GAPS, Fone: 3201-9496 – CEP: 74.230-130, Goiânia–GO.

Documento assinado eletronicamente por **ROBERTO CARLOS GONZAGA JAIME**, **Gerente**, em 06/03/2025, às 11:15, 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 **71392346** e o código CRC **C663FFE4**.
