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

TERMO DE REFERÊNCIA

PROCESSO Nº. 202200058004244/2021
TERMO DE REFERÊNCIA Nº 18/2022-GTI

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. 005 de 15 de janeiro de 2021 disponível no site da OVG http://www.ovg.org.br e demais condições estabelecidas neste Termo.

1. DO OBJETO

1.1 O presente termo de referência, tem por objetivo a contratação de empresa especializada no fornecimento de licenciamento de funcionalidades dos equipamentos firewalls da marca Sophos adquiridos no processo SEI nº 201900058002499, CF/CPS nº 022/2020, conforme especificações e quantidades descritas no termo em questão.

Lote 1			
ITEM	DESCRIÇÃO E CARACTERÍSTICAS	Unidade	Quantidade
01	Licenciamento Firewall Sophos XG135	Unid.	08
02	Licenciamento Firewall Sophos XG230	Unid.	01

1.2. Não serão admitidos licenças que não atendam os requisitos descritos no termo de referência por objeto.

2. DA JUSTIFICATIVA

2.1 Os pilares de segurança da informação sofreram alterações na era da informação, sendo eles caracterizados pelos seguintes atributos: disponibilidade, integridade, confidencialidade. Segurança são processos contínuos, precisam ser revistos e não se concluem, sendo salvaguardados por diversos equipamentos, incluindo a ferramenta que receberá o objeto desta solicitação.

2.2 O Firewall é utilizado para controlar acesso indevido, e compor uma das camadas de segurança desta organização para proteger informações e dados sensíveis e mitigar ataques cibernéticos. Além de executar um controle a nível de aplicação e programas, bloqueando acessos a sites e plataformas inseguras.

2.3 Informamos que a OVG adquiriu através do processo 201900058002499, CF/CPS nº 022/2020, adquiriu os Firewalls da marca Sophos modelo XG135 e XG230, desta forma, para continuar o devido uso dos equipamentos, deve ser adquirido licenciamento desta mesma marca de equipamento supracitada, por conseguinte, este processo tem por objetivo central executar o licenciamento de funcionalidades em todos os firewalls da Organização, visando manter o nível de segurança e estabilidade experimentado durante os últimos 02 (dois) anos na OVG de vigência do contrato.

2.4 Faz-se necessária o licenciamento das atualizações da base de ameaças, e das proteções WEB e de Aplicações, sendo assim, sem esta contratação torna-se impossível permanecer com um bom nível de segurança do nosso ambiente computacional, deixando-o mais vulnerável e suscetível a ataques e ações de cyber criminosos.

3. DA ESPECIFICAÇÃO E DO QUANTITATIVO DO OBJETO

3.1 Licenciamento Firewall Sophos XG135.

3.1.1 Deverá ser ofertada a licença Standard Protection (EnterpriseGuard), não obstante em ser fornecido licenciamento completo Xtream Protection (FullGuard).

3.1.2 A solução deverá licenciar todos os firewalls listados no lote 01, item 01 por no mínimo 24 (vinte e quatro) meses.

3.1.2.1 A CONTRATADA deverá fornecer garantia legal e de compatibilidade com o equipamento apresentado no item 3.1 deste Termo.

3.1.3 A solução ofertada deverá habilitar e manter no mínimo as seguintes funções:

3.1.3.1 A proteção Base existente não pode sofrer alterações, ou ser desabilitada;

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

3.1.3.1.2 Deverá permitir o controle e monitoramento das seguintes políticas

3.1.3.1.2.1 Políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.

3.1.3.1.2.2 Políticas de controle por países via localização por IP.

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

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

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

3.1.3.1.6 Deverá suportar monitoramento através de SNMP v2 e v3;

3.1.3.1.7 Deverá o permitir 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.

3.1.3.1.8 Deverá permitir subdivizão de zonas em pelo menos em WAN, LAN e DMZ.

3.1.3.1.9 Deverá permitir que as políticas de NAT possam ser customizáveis para cada regra.

3.1.3.1.10 Deverá permitir DHCP Server interno;

3.1.3.1.11 Deverá suportar protocolos de roteamento;

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

3.1.3.1.11.2 Deverá suportar IPv6, com roteamento estático e dinâmico (OSPFv3, RIPng);

3.1.3.2 Proteção Rede;

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

3.1.3.2.2 Deverá permitir proteção contra anti-spoofing.

3.1.3.2.3 Deverá permitir proteção do ambiente contra-ataques, dispositivos de proteção devem possuir módulo de IPS integrados no próprio appliance de firewall, onde sua console de gerência deverá residir na mesma console centralizada dos appliances de segurança, com suporte a pelo menos 3.000 assinaturas;

3.1.3.2.4 Deverá permitir os seguintes mecanismos de detecção na função IPS: assinaturas e trabalhar em conjunto com o controle de aplicações;

3.1.3.2.5 Deverá permitir a solução de IPS fazer a inspeção de todo o pacote, independentemente do tamanho;

3.1.3.2.7 Deverá permitir capacidade de remontagem de pacotes para identificação de ataques;

3.1.3.2.8 Deverá permitir o mecanismo de inspeção receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;

3.1.3.2.9 Deverá permitir as regras de exceção contendo: origem, destino e serviço;

3.1.3.2.10Deverá permitir a solução ser capaz de inspecionar tráfego HTTPS.

3.1.3.2.11 Deverá permitir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;

3.1.3.2.12 Deverá permitir a solução de política ser capaz de definir o modo de operação (bloqueio ou detecção);

3.1.3.3 Proteção Web;

3.1.3.3.1 Deverá permitir o reconhecimento de 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.

3.1.3.3.2 Deverá pemitir a realização de 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)*

3.1.3.3.3 Deverá permitir a análise do tráfego criptografado SSL a fim de possibilitar a leitura de *payload* para checagem de assinaturas de aplicações conhecidas pelo fabricante.

3.1.3.3.4 Deverá permitir a atualização da base de assinaturas de aplicações automaticamente.

3.1.3.3.5 Deverá permitir o reconhecimento de aplicações em IPv6.

3.1.3.3.6 Deverá permitir a limitação da banda usada por aplicações (*traffic shaping*).

3.1.3.3.7 Deverá permitir a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como :

3.1.3.3.7.1 Nível de risco da aplicação.

3.1.3.3.7.2 Categoria de aplicações.

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

3.1.3.3.9 Deverá permitir o controle de software FreeProxy tais como ToR, Ultrasurf, Freegate,etc.

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

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

3.1.3.3.12 Deverá permitir a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

3.1.3.3.13 Deverá permitir a categorização das URLs a partir de base ou cache de URLs locais ou através de consultas dinâmicas na nuvem do fabricante

3.1.3.3.14 Deverá permitir a criação categorias de URLs customizadas;

3.1.3.4 Conexões VPN

3.1.3.4.1 Deverá permitir Criptografia 3DES, AES 128 e AES 256;

3.1.3.4.2 Deverá permitir 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).

3.1.3.4.3 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;

3.1.3.4.4 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;

3.1.3.4.5 Deverá permitir o acesso via o portal de usuário para o download e configuração do cliente SSL para Windows3.1.3.4.6 Deverá suportar autenticação via AD/LDAP, *Token* e base de usuários local;

3.1.5 Modelo de referência: Sophos XG 135 Standard Protection - 24 MOS

3.2 Licenciamento Firewall Sophos XG230

3.2.1 Deverá ser ofertada a licença Standard Protection (EnterpriseGuard), não osbtante em ser fornecido licenciamento completo Xtream Protection (FullGuard).

3.2.2 A solução deverá licenciar todos os firewalls listados no lote 01, item 02 por no mínimo 24 meses

3.2.2.1 A CONTRATADA deverá fornecer garantia legal e de compatibilidade com o equipamento apresentado no item 3.2 deste Termo.

3.2.3 A solução ofertada deverá habilitar e manter no mínimo as seguintes funções

3.2.3.1 A proteção Base existente não pode sofrer alterações, ou ser desabilitada;

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

3.2.3.1.2 Deverá permitir o controle e monitoramento das seguintes políticas

3.2.3.1.2.1 Políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.

3.2.3.1.2.2 Políticas de controle por países via localização por IP.

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

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

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

3.2.3.1.6 Deverá suportar monitoramento através de SNMP v2 e v3;

3.2.3.1.7 Deverá o permitir 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.

3.2.3.1.8 Deverá permitir subdivizão de zonas em pelo menos em WAN, LAN e DMZ.

3.2.3.1.9 Deverá permitir que as políticas de NAT possam ser customizáveis para cada regra.

3.2.3.1.10 Deverá permitir DHCP Server interno;

3.2.3.1.11 Deverá suportar protocolos de roteamento;

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

3.2.3.1.11.2 Deverá suportar IPv6, com roteamento estático e dinâmico (OSPFv3, RIPng);2

3.2.3.2 Proteção Rede;

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

3.2.3.2.2 Deverá permitir proteção contra anti-spoofing.

3.2.3.2.3 Deverá permitir proteção do ambiente contra-ataques, dispositivos de proteção devem possuir módulo de IPS integrados no próprio appliance de firewall, onde sua console de gerência deverá residir na mesma console centralizada dos appliances de segurança, com suporte a pelo menos 3.000 assinaturas;

3.2.3.2.4 Deverá permitir os seguintes mecanismos de detecção na função IPS: assinaturas e trabalhar em conjunto com o controle de aplicações;

3.2.3.2.5 Deverá permitir a solução de IPS fazer a inspeção de todo o pacote, independentemente do tamanho;

3.2.3.2.7 Deverá permitir capacidade de remontagem de pacotes para identificação de ataques;

3.2.3.2.8 Deverá permitir o mecanismo de inspeção receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;

3.2.3.2.9 Deverá permitir as regras de exceção contendo: origem, destino e serviço;

3.2.3.2.10Deverá permitir a solução ser capaz de inspecionar tráfego HTTPS.

3.2.3.2.11 Deverá permitir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;

3.2.3.2.12 Deverá permitir a solução de política ser capaz de definir o modo de operação (bloqueio ou detecção);

3.2.3.3 Proteção Web;

3.2.3.3.1 Deverá permitir o reconhecimento de 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.

3.2.3.3.2 Deverá pemitir a realização de 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)*

3.2.3.3.3 Deverá permitir a análise do tráfego criptografado SSL a fim de possibilitar a leitura de *payload* para checagem de assinaturas de aplicações conhecidas pelo fabricante.

3.2.3.3.4 Deverá permitir a atualização da base de assinaturas de aplicações automaticamente.

3.2.3.3.5 Deverá permitir o reconhecimento de aplicações em IPv6.

3.2.3.3.6 Deverá permitir a limitação da banda usada por aplicações (*traffic shaping*).

3.2.3.3.7 Deverá permitir a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como :

3.2.3.3.7.1 Nível de risco da aplicação.

3.2.3.3.7.2 Categoria de aplicações.

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

3.2.3.3.9 Deverá permitir o controle de software FreeProxy tais como ToR, Ultrasurf, Freegate,etc.

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

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

3.2.3.3.12 Deverá permitir a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

3.2.3.3.13 Deverá permitir a categorização das URLs a partir de base ou cache de URLs locais ou através de consultas dinâmicas na nuvem do fabricante

3.2.3.3.14 Deverá permitir a criação categorias de URLs customizadas;

3.2.3.4 Conexões VPN

3.2.3.4.1 Deverá permitir Criptografia 3DES, AES 128 e AES 256;

3.2.3.4.2 Deverá permitir 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).

3.2.3.4.3 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;

3.2.3.4.4 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;

3.2.3.4.5 Deverá permitir o acesso via o portal de usuário para o download e configuração do cliente SSL para Windows3.2.3.4.6 Deverá suportar autenticação via AD/LDAP, *Token* e base de usuários local;

3.2.5 Modelo de referência: Sophos XG 230 Standard Protection - 24 MOS

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 de 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. Admitir-se-á como válida a certidão positiva com efeito de negativa.

4.3. 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.

4.4. 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.

4.5. 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.

4.6. Não será admitido neste processo a participação de fornecedor/prestador de 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.

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 por lote.

7. DO PRAZO DE ENTREGA E FORMA DE RECEBIMENTO

7.1. Os produtos deverão ser disponibilizados de forma única, com um prazo de entrega de até 15 (quinze) dias após pagamento das licenças do software, por meio de plataforma web ou informações/orientações via E-mail, possibilitando acesso da contratante as licenças adquiridas.

7.2. Os produtos deverão ser entregues na modalidade online, devendo ser fornecido o acesso no portal da CONTRATADA ou do fabricante ou através do envio por e-mail, sendo enviado para informatica@ovg.org.br.

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

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

7.5. 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.

8. DO PAGAMENTO

8.1 O pagamento será efetuado em até 30 (trinta) dias após a emissão válida do documento fiscal e boleto correspondente a prestação do serviço (nota fiscal, recibo ou equivalente), devidamente preenchido, atestado e acompanhado das Certidões que comprovem a sua devida Regularidade Fiscal.

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

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

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

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

8.4. Caso o recurso financeiro seja do Contrato de Gestão, deverá constar nas notas fiscais a seguinte anotação: CONTRATO DE GESTÃO Nº. 001/2011-SEAD.

8.5. As notas fiscais deverão destacar as retenções de impostos conforme legislação, sendo a OVG substituta tributária.

8.6. As empresas optantes do Simples Nacional deverão apresentar declaração informando em qual Anexo está enquadrado.

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.

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 VIGÊNCIA DO CONTRATO OU EMISSÃO DE ORDEM DE COMPRAS

11.1 Será emitido Contrato, com prazo de execução de 24 (vinte e quatro) meses.

12. DA GARANTIA

12.1. A contratada deverá fornecer garantia detalhada no item 3. DA ESPECIFICAÇÃO E DO QUANTITATIVO DO OBJETO.

13. DAS PENALIDADES

13.1. O fornecedor que descumprir com suas obrigações, injustificadamente, ficará sujeito às penalidades previstas no subitem 9.7 do Regulamento para Aquisição da OVG.

14. DO PRAZO PARA INTERPOSIÇÃO DE RECURSO ADMINISTRATIVO

14.1. Nas contratações com valor superior a R$ 300.000,00 (trezentos mil reais), o fornecedor ou prestador de serviço que não concordar com o resultado da inabilitação no processo no qual seja participante, terá o prazo de 02 (dois) dias úteis, contados a partir da comunicação da decisão de inabilitação para a propositura do recurso.

14.1.1. Nos demais casos, o prazo recursal de 05 (cinco) dias úteis se dará a partir da publicação do contrato.

14.1.2. Caso o recurso seja em desfavor de outrem, fica a outra parte intimada, a partir da comunicação do recurso, para apresentar contrarrazões em igual número de dias, sendo-lhe assegurada vista imediata dos autos.

14.2. O recurso será proposto por escrito devidamente protocolizado no Núcleo de Protocolo e Arquivo – NPA da OVG e encaminhado à Gerência de Aquisição de Bens, Produtos e Serviços para proferir decisão, e, se necessário, será encaminhado à Gerência Estratégica Jurídica para emissão de parecer, sujeito à anuência da Diretoria Geral e Diretoria Administrativa e Financeira.

14.3. Os recursos deverão ser acompanhados, sob pena de não conhecimento, do contrato social da empresa participante ou documentos pessoais (RG e CPF) em se tratando de pessoa física, e, no caso de procurador, procuração com poderes específicos.

14.4. Os recursos serão recebidos sem efeito suspensivo, salvo quando, por sua relevância, a Diretoria Geral entender conveniente a suspensão do Processo.

15. DISPOSIÇÕES FINAIS

15.1 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.

15.2. 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/serviços, sem prejuízo das demais sanções cabíveis.

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

15.4. Os fornecedores/prestadores de 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.

15.5. 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.

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

15.7. 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.

15.8. 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.

15.9. 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.

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

15.11. O vencedor da cotação será declarado após Despacho favorável da Gerência Estratégica de Controladoria e *Compliance* da OVG, Parecer favorável da Gerência Estratégica Jurídica e assinatura da ordem de compras ou contrato.

15.12. 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 **FLAVIANA DIAMANTE DA MOTA RIBEIRO**, **Colaborador (a)**, em 13/09/2022, às 15:19, 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 **000033625507** e o código CRC **BA6A7CCC**.
