

CONTRATO Nº 38/2022/TCE/PI

Ref.: Processo 101106/2022

CONTRATO DE AQUISIÇÃO DE SOLUÇÃO DE SEGURANÇA EM REDES DE COMPUTADORES, COM ALTA DISPONIBILIDADE HA (HIGH-AVAILABILITY) DO TIPO FIREWALL NGFW - APPLIANCE (NEXT-GENERATION FIREWALL) DA MARCA PALO ALTO, MODELO PA-3410 OU SUPERIOR. FAZ PARTE DA SOLUÇÃO A INSTALAÇÃO, CONFIGURAÇÃO E TESTES, ALÉM DA GARANTIA, SUBSCRIÇÕES “THREAT PREVENTION”, “ADVANCED URL FILTERING”, “GLOBALPROTECT”, “VIRTUAL SYSTEM” E SUPORTE TÉCNICO PELO PERÍODO DE 60(SESENTA) MESES, QUE FAZEM ENTRE SI O TRIBUNAL DE CONTAS DO ESTADO DO PIAUÍ E A EMPRESA

O TRIBUNAL DE CONTAS DO ESTADO DO PIAUÍ, com sede na Av. Pedro Freitas, nº 2100, bairro São Pedro, CEP 64.018-900, na cidade de Teresina/PI, inscrito no CNPJ sob o nº 05.818.935/0001-01, neste ato representado por sua Presidente Conselheira LILIAN DE ALMEIDA VELOSO NUNES MARTINS, inscrita no CPF sob o nº 077.565.183-49, portadora da Carteira de Identidade nº 171.133 – SSP/PI, doravante denominado CONTRATANTE, e a empresa APPROACH TECNOLOGIA LTDA. , inscrita no CNPJ/MF sob o nº 24.736.542.542/0001-21, I.E: 25.792.687-9, sediada na Av. Prefeito Osmar Cunha nº 416, SL 303, Centro, Florianópolis – Santa Catarina, CEP 88015-100, Telefones: (48) 4009-2160 , E-mail: contato@approachtec.com.br, doravante designada CONTRATADA, neste ato, representada por Kent Johann Modes, portador da Carteira de Identidade nº 4.826.448, expedida pela SSP/SC e CPF nº 047.478.629-35, tendo em vista o que consta no Processo SEI nº 101106/2022-TCE/PI e em observância às disposições da Lei nº 8.666/93, da Lei nº 10.520/02, Decreto nº 10.024/2019, Lei Estadual 7.482, de 18 de janeiro de 2021 e das demais normas aplicáveis, resolvem celebrar o presente Contrato, decorrente do Pregão Eletrônico nº 19/2022 - TCE /PI, mediante as cláusulas e condições a seguir:

CLÁUSULA PRIMEIRA – OBJETO

1.1 Contratação para aquisição de solução de segurança em redes de computadores, com alta disponibilidade HA (High-Availability) do tipo Firewall NGFW - Appliance (Next-Generation Firewall) da marca Palo Alto, modelo PA-3410 ou superior. Faz parte da solução a instalação, configuração e testes, além da garantia, subscrições “Threat Prevention”, “Advanced URL Filtering”, “GlobalProtect”, “Virtual System” e suporte técnico pelo período de 60(sessenta) meses, de acordo com as condições, quantidades e exigências estabelecidas no edital e anexo do Pregão identificado no preâmbulo e na proposta vencedora, os quais integram este instrumento, independente de transcrição.

1.2 Discriminação do objeto:

ESPECIFICAÇÃO	ITEM	QTD	VALOR UNITÁRIO R\$	VALOR TOTAL R\$
FIREWALL DO TIPO NEXT GENERATION, INCLUINDO INSTALAÇÃO, CONFIGURAÇÃO, SUBSCRIÇÕES E SUPORTE TÉCNICO. 1. FIREWALL DO TIPO NEXT GENERATION;				

1.1. A solução consiste em appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW) tais como reconhecimento e controle de aplicações, identificação de usuários, prevenção contra ameaças de vírus, spywares e malwares desconhecidos (Zero Day), IPS, filtro de URL e recursos de VPN; 1.2. O hardware e software que executem as funcionalidades de proteção de rede são do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico; 1.3. O equipamento fornecido é próprio para montagem em rack 19", incluindo kit tipo trilho para adaptação, se necessário, e cabos de alimentação; 1.4. Possui throughput de, no mínimo, 11 (onze) Gbps com a funcionalidade de controle de aplicação para todas as assinaturas que o fabricante possuir; 1.5. Possui throughput de, no mínimo, 5 (cinco) Gbps com as funcionalidades de controle de aplicação, IPS, Antivírus e Anti-Spyware habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real; 1.6. Suporta, no mínimo, 1.200.000 (um milhão e duzentas mil) conexões simultâneas; 1.7. Suporta, no mínimo, 140.000 (cento e quarenta mil) novas conexões por segundo; 1.8. Possui, no mínimo, 04 (quatro) interfaces físicas de rede de 1 Gbps do tipo RJ-45; 1.9. Possui, no mínimo, 10 (dez) interfaces físicas de rede de 10 Gbps do tipo SFP/SFP+, sendo fornecidos os respectivos transceivers na quantidade de interfaces físicas solicitada; 1.10. Possui, no mínimo, 4 (quatro) interfaces físicas de rede de 25 Gbps do tipo SFP28, sendo fornecidos os respectivos transceivers na quantidade de interfaces físicas solicitada; 1.11. São fornecidos 4(quatro) transceivers de 10 Gbps do tipo SFP+, homologados pela fabricante Cisco, a serem instalados nos dois roteadores Cisco ASR1001-X, existentes no datacenter do TCE-PI, a fim de possibilitar a interconexão dos firewalls aos referidos equipamentos; 1.12. Possui, no mínimo, 1 (uma) interface física de rede de 1 Gbps dedicada para gerenciamento; 1.13. Possui, no mínimo, 1 (uma) interface física dedicada para o recurso de alta disponibilidade; 1.14. Possui, no mínimo, 1 (uma) interface física do tipo console ou similar; 1.15. Possui disco do tipo Solid State Drive (SSD) de, no mínimo, 480 (quatrocentos e oitenta) GB de armazenamento do sistema operacional e registro de logs; 1.16. Possui fonte de alimentação elétrica redundante capaz de operar entre 120 e 240 VAC permitindo, em caso de problema com uma das fontes, a substituição da fonte defeituosa com o equipamento em funcionamento (hotswappable); 1.17. Suporta, no mínimo, 1.000 (um mil) clientes de VPN SSL simultaneamente estando, caso necessário devidamente licenciado para este fim; 1.18. Suporta, no mínimo, 2.000 (dois mil) túneis de VPN IPSEC simultaneamente estando, caso necessário, devidamente licenciado para este fim; 1.19. Possui suporte a criação de rede virtuais (VLAN), conforme o padrão IEEE 802.1Q, de, no mínimo, 1.000 (um mil) VLANs; 1.20. Implementa o protocolo LLDP – Link Layer Discovery Protocol; 1.21. Possui o recurso de agregação de links conforme padrão IEEE 802.3ad (LACP) permitindo o agrupamento de interfaces físicas de rede em um link agrupado virtualmente (LAG – Link Aggregation Group); 1.22. Possui o recurso de NAT – Network Address Translation nas modalidades de NAT estático 1 para 1, NAT dinâmico 1 para vários e NAT dinâmico vários para vários. Este recurso é aplicado tanto para o endereço de origem quanto para endereço de destino. Deve possuir também NAT64 para tradução entre endereços IPv6 e IPv4 e NPTv6 (Network Prefix Translation) para tradução de um prefixo IPv6 para outro prefixo IPv6 prevenindo problemas de roteamento assimétrico;	01	02	1.049.500,00	2.099.000,00
---	----	----	--------------	--------------

1.23. Suporta a criação de rotas estáticas e os protocolos de roteamento estático e dinâmico RIPv2, OSPFv2 e OSPFv3 incluindo OSPF graceful restart e BGP; 1.24. Implementa o protocolo ECMP – Equal Cost Multiple Path para balanceamento de carga entre links baseados no hash do endereço IP de origem, no hash do endereço IP de origem e de destino, pela técnica conhecida como roundrobin e com base no peso ou prioridade atribuídos a cada link. Suporta o balanceamento entre, no mínimo 4 (quatro) links; 1.25. Permite o envio de logs para sistemas de monitoração externos utilizando o padrão syslog, bem como o envio de forma segura através do protocolo SSL/TLS; 1.26. Possui o recurso de alta disponibilidade e permitir a configuração nos modos ativo/passivo e ativo/ativo; 1.27. Implementa controle por políticas/regras de firewall capaz de permitir ou bloquear o tráfego de rede por porta e protocolo, por aplicações, por grupos estáticos de aplicações, por grupos dinâmicos de aplicações baseados em características e comportamento das aplicações, por usuários e grupos de usuários, por endereços IP e faixas de endereços IP e por país de origem e destino do tráfego; 1.28. A identificação do país é através do código do país, por exemplo, BR, USA, UK, RUS, etc e também através de geolocalização possibilitando a criação de regiões geográficas; 1.29. Permite configurar o agendamento das políticas/regras de firewall para habilitar ou desabilitar tais políticas/regras em horários pré-definidos; 1.30. Possui a capacidade para realizar a descriptografia do tráfego SSL e SSH permitindo o controle e inspeção tanto do tráfego de entrada quanto de saída. A descriptografia é realizada com base em políticas/regras de acordo com a origem e destino do tráfego; 1.31. Possui recurso de QoS – Quality of Service com suporte a DSCP – Differentiated Services Code Point. Permite também definir, baseado em políticas/regras, a prioridade e o limite máximo de largura de banda de um determinado tipo de tráfego. As definições de prioridade e limite de largura de banda são baseadas no endereço IP de origem e destino, no usuário e na aplicação; 1.32. Possui a capacidade de reconhecer, no mínimo, 3.000 (três mil) aplicações diferentes tais como redes sociais, compartilhamento de arquivos, email, atualização de softwares, acesso remoto, VoIP, áudio e vídeo, peer-to-peer, sistemas de mensagem instantânea etc., sendo esta uma lista não exaustiva; 1.33. O reconhecimento da aplicação se dá, independentemente de porta e protocolo, através de, no mínimo, os seguintes métodos: baseado na assinatura da aplicação conhecida pelo fabricante da solução de firewall, através da decodificação de protocolos para detectar aplicações encapsuladas dentro do protocolo e identificação através de análise heurística a fim de detectar aplicações através de análise comportamental do tráfego analisado; 1.34. Permite a criação de assinaturas personalizadas para o reconhecimento de aplicações proprietárias na própria interface gráfica do equipamento sem a necessidade de intervenção do fabricante; 1.35. Permite a diferenciação e controle de partes da aplicação como, por exemplo, em uma aplicação de mensagem instantânea permite a troca de mensagens de texto e bloqueia a transferência de arquivos por dentro da aplicação; 1.36. Permite bloquear sessões TCP que utilizarem variações do three-way handshake como four-way e o five-way split handshake, prevenindo assim possíveis tráfegos maliciosos; 1.37. Permite bloquear conexões que contenham dados no payload dos pacotes TCP SYN e TCP SYN-ACK durante o three-way handshake; 1.38. A solução de firewall possui funcionalidades de IPS, antivírus e antispymware que permita o bloqueio de vulnerabilidades e exploits conhecidos e proteção contra vírus e spywares baseado em assinaturas de ameaças conhecidas; 1.39. É possível a criação de assinaturas customizadas de ameaças; 1.40. Permite realizar o bloqueio de vírus realizando a inspeção em, no mínimo, os protocolos HTTP, FTP, SMB, SMTP e POP3; 1.41. Possui a capacidade de detectar e prevenir ameaças em tráfego HTTP/2; 1.42. Possui proteção contra ataques de negação de serviço (DoS) capaz de impedir ataques de SYN Flood, ICMP Flood, UDP Flood, etc e				
---	--	--	--	--

também bloqueia port scans, bloqueia ataques de buffer overflow e identifica e bloqueia comunicação com botnets; 1.43. Para cada ameaça detectada pela solução é realizado o registro nos logs do sistema das informações de data e hora, tipo da ameaça, origem e destino da comunicação e a ação tomada (se permitiu ou bloqueou o tráfego); 1.44. A solução de firewall possui funcionalidade de filtro URL que permite a criação de políticas/regras para controle do acesso a websites baseado em categorias de URL e o fabricante da solução disponibiliza a base de dados de URL categorizadas para consulta por parte da solução. As políticas/regras que permitem ou bloqueiam o acesso a determinada categoria de URL são com base no usuário e grupos de usuários e por endereços IP e faixas de endereços IP; 1.45. A funcionalidade de filtro URL possui categoria específica para classificar domínios recém registrados com menos de 30 dias; 1.46. Permite a criação de categoria de URL customizada permitindo inserir uma lista de URLs específicas; 1.47. Permite a customização da página de bloqueio exibida ao usuário quando este tentar realizar um acesso a um website pertencente a uma categoria de URLs bloqueada; 1.48. Possui recurso para proteger contra o roubo de credenciais de usuário e senha, identificadas através da integração com o Active Directory, submetidas em sites não corporativos. É possível definir em quais websites é permitido ou bloqueado o envio das credenciais baseado na categoria de URL a qual o website pertencer. Caso o usuário tente submeter suas credenciais de usuário e senhas pertencentes ao Active Directory em um website não autorizado é exibida uma página de bloqueio informando que o uso de tais credenciais no website específico não está autorizado; 1.49. A solução de firewall possui recurso que permita bloquear a transferência de arquivos baseado na extensão dos mesmos e definir por qual aplicação a transferência do arquivo está bloqueada, por exemplo, bloquear a transferência de arquivos .exe através de web browser. Permite bloquear, no mínimo, arquivo com as extensões .exe, .bat, .dll, .pif e .torrent; 1.50. A solução de firewall possui integração com LDAP, MS Active Directory e RADIUS para identificação dos usuários e grupos da rede para uso nas políticas/regras baseadas por usuários e grupo de usuários; 1.51. A integração com MS Active Directory para identificação dos usuários da rede é realizada sem a necessidade de instalação de um agente no Controlador de Domínio e nem nas estações dos usuários; 1.52. A solução de firewall possui recurso de portal de autenticação prévia (Captive Portal) para identificação dos usuários que realizam o acesso à internet, sem a necessidade de instalação de software cliente ou agente no computador. O portal de autenticação é exibido antes de o usuário iniciar a navegação pela internet; 1.53. A solução de firewall possui o recurso de VPN – Virtual Private Network dos tipos site-to-site e client-to-site e suportar IPsec – Internet Protocol Security e SSL – Secure Sockets Layer; 1.54. O recurso de VPN IPsec suporta os algoritmos de criptografia 3DES, AES 128, AES 192 e AES 256, os algoritmos de autenticação MD5 e SHA 1, o algoritmo IKEv1 e IKEv2 e os algoritmos de troca de chaves DiffieHellman Grupo 1, Grupo 2, Grupo 5 e Grupo 14 e suporta também a autenticação através de certificados IKE PKI; 1.55. O recurso de VPN SSL permite que o usuário remoto se conecte através de um software cliente de VPN instalado no sistema operacional do equipamento do usuário sendo possível a atribuição de endereços IP fixos e atribuição de DNS ao mesmo; 1.56. Suporta a autenticação dos usuários remotos que se conectam à VPN via LDAP, MS Active Directory, TACACS+, RADIUS, SAML e através de base de usuários local no equipamento da solução de firewall. Suporta também a autenticação via certificado e OTP – One Time Password; 1.57. É disponibilizado o software cliente de VPN do mesmo fabricante da solução de firewall ofertada compatível para instalação em computadores com sistema operacional MS Windows 8, MS Windows 10, MacOS e Linux e para instalação em dispositivos móveis Android e IOS; 1.58. O recurso de VPN SSL possui mecanismo de checagem da conformidade do computador do usuário remoto e a checagem permite				
---	--	--	--	--

verificar, no mínimo, as informações de qual sistema operacional e patches estão instalados, se o antivírus está instalado e ativo no computador, se o firewall está instalado e ativo no computador, se o disco está criptografado, se o agente de DLP – Data Loss Prevention está instalado e ativo, informações de chaves de registro e processos ativos no computador; 1.59. É possível criar perfis customizados de conformidade com, no mínimo, as mesmas informações obtidas pelo mecanismo de checagem da conformidade do computador do usuário remoto. Tais perfis são utilizados para assegurar que apenas computadores de usuários remotos que atendem aos requisitos solicitados nos perfis customizados possam ter acesso através da VPN aos dados e sistemas hospedados na rede interna do órgão; 1.60. A solução de firewall possui console de gerenciamento do equipamento acessada através de interface gráfica web permitindo realizar as configurações da solução como criar e administrar as políticas/regras de firewall e controle de aplicações, criar e administrar as políticas de IPS, antivírus e anti-spyware, criar e administrar as políticas de filtro URL, monitorar e investigar os registros de logs de eventos e demais configurações; 1.61. Suporta a autenticação dos usuários administradores que se conectam à interface de gerenciamento do equipamento via LDAP, MS Active Directory, RADIUS e através de base de usuários local no equipamento da solução de firewall; 1.62. É possível criar perfis de acesso à interface de gerenciamento com permissões granulares como acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações entre outros; 1.63. Permite realizar o backup das configurações do equipamento e a restauração da configuração salva através de interface de gerenciamento; 1.64. A interface de gerenciamento do equipamento possui recurso para análise das políticas indicando, quando houver, regras que ofusquem, conflitem ou sobreponham outras regras (shadowing) e quais objetos não estão sendo utilizados, para avaliação de elementos dispensáveis, permitindo assim, a higienização gradual das regras e seus respectivos elementos. Possui também recurso para análise das políticas indicando, quando houver, regras baseadas em porta e protocolo, permitindo a conversão para uma regra baseada em aplicação, melhorando assim o controle do tráfego e a segurança do ambiente; 1.65. É possível, através de interface de gerenciamento do equipamento, a geração de relatórios tais como um resumo gráfico das aplicações utilizadas e ameaças vistas, principais aplicações por utilização de largura de banda, atividades de um usuário ou grupo de usuários específicos, incluindo aplicações e URLs acessadas e permite a criação de relatórios personalizados; 1.66. É possível gerar relatório de visibilidade e uso das aplicações do tipo SaaS – Software as a Service, mostrando os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso à aplicação e o consumo da aplicação SaaS pelo usuário; 1.67. É exibida na interface gráfica de gerenciamento do equipamento informações em tempo real, atualizadas de forma automática a cada 1 (um) minuto, as principais aplicações acessadas, o risco das principais aplicações, número de sessões simultâneas, status das interfaces de rede e uso de CPU; 1.68. É possível configurar o envio de alertas do sistema via e-mail; 1.69. Suporta o monitoramento via SNMPv3; 1.70. O sistema operacional que é instalado no equipamento que compõe a solução é fornecido em sua versão mais atualizada, não sendo aceito sistema operacional de uso genérico; 1.71. Por cada equipamento que compõe a solução de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento; 1.72. Na data do certame, nenhum dos equipamentos ofertados estão listados no site do fabricante em listas de end-of-life e end-of-sale; 1.73. Pelo período de, no mínimo, 60 (sessenta) meses, todos os componentes da solução de firewall, incluindo o equipamento, o sistema operacional, as licenças necessárias para atender as funcionalidades e recursos solicitados, os softwares clientes de VPN e demais itens necessários para				
---	--	--	--	--

o perfeito funcionamento estão cobertos por garantia e suporte técnico do fabricante da solução em caso de problema;				
1.74. A solução de firewall possui garantia pelo período de, no mínimo, 60 (sessenta) meses, compreendendo a reposição de peças/equipamentos, atualizações do sistema operacional do equipamento, softwares e das assinaturas de proteção da solução.				
2. SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO				
2.1. A contratada presta serviços de instalação e configuração da solução, que compreendem, entre outros, os seguintes procedimentos:				
2.1.1. Reunião de alinhamento para criação do escopo do projeto previamente a instalação;				
2.1.2. Instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos no local determinado pela equipe responsável pelo projeto por parte da contratante. Considera também a instalação em modo Alta Disponibilidade (ativo/passivo);				
2.1.3. Análise da topologia e arquitetura da rede, considerando todos os equipamentos já existentes e instalados;				
2.1.4. Análise do acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;				
2.1.5. Migração das regras de firewall existentes e aplicáveis à solução ofertada, considerando a adequação às políticas de aplicações em camada 7;				
2.1.6. Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;				
2.1.7. Configuração do sistema de firewall, VPN, IPS, Filtro URL, Antivírus e Antimalware de acordo com as exigências levantadas;				
2.2. Toda configuração do sistema é realizada de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada. O fabricante disponibiliza ferramenta gratuita para acompanhamento da evolução da parametrização de proteção dos firewalls afim de garantir a melhor eficiência da solução durante o período de vigência das licenças;				
2.3. Repasse de informação das configurações realizadas no formato hands-on de 20 horas para a equipe responsável pelo projeto por parte da contratante após validação da migração;				
Todos os modelos ofertados acompanham as garantias, cabos e acessórios exigidos nos respectivos itens e estão de acordo com as especificações, termo de referência, edital e seus anexos.				
Declaramos que atendemos todos os itens do edital e termo de referência e seus anexos.				
Garantia: 60 meses				
Procedência: Estados Unidos				
Fabricante: Palo Alto Networks				
Modelo: PA-3410				
Part Numbers:				
1 x PAN-PA-3410 (NGFW Palo Alto PA-3410 com fonte de alimentação redundante)				
1 x PAN-PA-3400-RACK4 (Kit para fixação em rack 19")				
1 x PAN-SVC-PREM-3410-5YR (Garantia e suporte do fabricante para o NGFW Palo Alto PA-3410 pelo período de 5 anos)				
1 x PAN-PA-3410-ATP-5YR-HA2 (Licença de Advanced Threat Prevention com subscrição pelo período de 5 anos)				
1 x PAN-PA-3410-ADVURL-5YR-HA2 (Licença de Advanced URL Filtering com subscrição pelo período de 5 anos)				
1 x PAN-PA-3410-GP-5YR-HA2 (Licença de GlobalProtect com subscrição pelo período de 5 anos)				
1 x PAN-SFP-PLUS-CU-5M (Cabo DAC de 5 metros de comprimento)				
10 x FTLX8574D3BCL (Transceiver SFP+ 10GBASE-SR)				
4 x FTLF8536P5BCL (Transceiver SFP28 25GBASE-SR)				
4 x SFP-10G-SR-S (Cisco Transceiver SFP+ 10GBASE-SR)				
Links de comprovação:				
Palo Alto Next Generation Firewalls Website				
https://www.paloaltonetworks.com/networksecurity/next-generation-firewall-hardware				

Palo Alto PA-3400 Series Datasheet				
https://www.paloaltonetworks.com/resources/datasheets/pa-3400-series				
Palo Alto PA-3410 Features List				
https://www.paloaltonetworks.com/products/product-comparison?chosen=pa-3410				
Palo Alto PA-3400 Series Hardware Reference				
https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/hardware/pa-3400-series/pa-3400-hardware-reference.pdf				
Palo Alto Networks Compatibility Matrix				
https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/compatibilitymatrix/compatibility-matrix.pdf				
Advanced Threat Prevention Datasheet				
https://www.paloaltonetworks.com/resources/datasheets/advanced-threat-prevention				
Advanced Threat Prevention Administration				
https://docs.paloaltonetworks.com/advanced-threat-prevention/administration				
Advanced URL Filtering Datasheet				
https://www.paloaltonetworks.com/resources/datasheets/advanced-url-filtering				
Advanced URL Filtering Administration				
https://docs.paloaltonetworks.com/advanced-url-filtering/administration				
GlobalProtect Datasheet				
https://www.paloaltonetworks.com/resources/datasheets/globalprotect-datasheet				
GlobalProtect TechDocs Website				
https://docs.paloaltonetworks.com/globalprotect				
GlobalProtect Administrator's Guide				
https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/globalprotect/10-1/globalprotect-admin/globalprotectadmin.pdf				
PAN-OS Administrator's Guide				
https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/11-0/panos-admin/pan-os-admin.pdf				
PAN-OS Networking Administrator's Guide				
https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/11-0/panos-networking-admin/pan-os-networkingadmin.pdf				
PAN-OS Web Interface Help				
https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/11-0/panos-web-interface-help/pan-os-web-interfacehelp.pdf				
PAN-OS New Features Guide Version 11.0				
https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/11-0/panos-new-features/pan-os-new-features.pdf				
PAN-OS Upgrade Guide				
https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/11-0/panos-upgrade/pan-os-upgrade.pdf				
PAN-OS and Panorama API Usage Guide				
https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/11-0/panos-panorama-api/pan-os-panorama-api.pdf				
Agentless User-ID Configuration				
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIGGC				
A0				
Complete List of PAN-DB URL Filtering Categories				
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm5h				
CAC				
How to Configure a Security Policy to Use a Region				
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIJWC				
A0				
Palo Alto Networks Product Summary				

Specsheet https://www.paloaltonetworks.com/resources/datasheets/product-summary-specsheet Application Research Center https://applipedia.paloaltonetworks.com/App-ID Tech Brief https://www.paloaltonetworks.com/resources/techbriefs/app-id-tech-brief.html Getting Started with the BPA https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/best-practices/10-2/bpa-getting-started/bpa-getting-started.pdf 10GBASE-SR/SW 400m Multimode Datacom SFP+ Optical Transceiver Website https://ii-vi.com/product/10gbase-sr-sw-400m-multimode-datacom-sfp-opticaltransceiver/ 10GBASE-SR/SW 400m Multimode Datacom SFP+ Optical Transceiver Datasheet https://app.boxcn.net/shared/static/u2v6v4cg56v636bsq8mlb59w9nz36zt5.pdf 25GE SR/10GE SR Lite/eCPRI 100m SFP28 Optical Transceiver Website https://ii-vi.com/product/25ge-sr-10ge-sr-liteecpri-100m-sfp28-optical-transceiver/ 25GE SR/10GE SR Lite/eCPRI 100m SFP28 Optical Transceiver Datasheet https://iiviincorporated1.box.com/shared/static/1kgao mgvez09kxkso50bbsxj10q6awk3.pdf Cisco 10GBASE SFP+ Modules Datasheet https://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceivermodules/data_sheet_c78-455693.html				
VALOR TOTAL DO CONTRATO				R\$ 2.099.000,00

CLÁUSULA SEGUNDA – PREÇO

2.1 O valor do presente Contrato é de R\$ 2.099.000,00 (dois milhões e noventa e nove mil reais), a ser pago por meio de ordem de crédito na Conta da Contratada nº 33207-0; Agência 7197; Banco Itaú.

2.2 No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução contratual, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outras necessárias ao cumprimento integral da execução do objeto contratado.

3. CLÁUSULA TERCEIRA – DOTAÇÃO ORÇAMENTÁRIA

3.1 OS RECURSOS FINANCEIROS destinados para custear as despesas dessa contratação serão oriundos do Tesouro Estadual, na Unidade Orçamentária: 02101 – TRIBUNAL DE CONTAS DO ESTADO; Programa de Trabalho: 01.032.0017.4121 – Gestão Estratégica e Manutenção Operacional; Fonte: 100 – Recursos do Tesouro Estadual; Natureza: 449040 – Serviços de Tecnologia da Informação e Comunicação – Pessoa Jurídica, conforme Nota de Empenho 2022NE01413, emitida em 14 de dezembro de 2022.

CLÁUSULA QUARTA – VIGÊNCIA CONTRATUAL

4.1 A vigência do contrato será de **12 (doze) meses**, contados da data de sua assinatura.

CLÁUSULA QUINTA – ESPECIFICAÇÕES TÉCNICAS DO OBJETO

5.1 FIREWALL DO TIPO NEXT GENERATION

5.1.1 A solução deve consistir em appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW) tais como reconhecimento e controle de aplicações, identificação de usuários, prevenção contra ameaças de vírus, spywares e malwares desconhecidos (Zero Day), IPS, filtro de URL e recursos de VPN;

5.1.2 O hardware e software que executem as funcionalidades de proteção de rede devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

5.1.3 O equipamento fornecido deve ser próprio para montagem em rack 19", incluindo kit tipo trilho para adaptação, se necessário, e cabos de alimentação;

5.1.4 Deve possuir throughput de, no mínimo, 11 (onze) Gbps com a funcionalidade de controle de aplicação para todas as assinaturas que o fabricante possuir;

5.1.5 Deve possuir throughput de, no mínimo, 5 (cinco) Gbps com as funcionalidades de controle de aplicação, IPS, Antivírus e Anti-Spyware habilitadas simultaneamente na solução. A comprovação se dará através de documentação técnica do fabricante de acesso público informando os throughput aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real;

5.1.6 Deve suportar, no mínimo, 1.200.000 (um milhão e duzentas mil) conexões simultâneas;

5.1.7 Deve suportar, no mínimo, 140.000 (cento e quarenta mil) novas conexões por segundo;

5.1.8 Deve possuir, no mínimo, 04 (quatro) interfaces físicas de rede de 1 Gbps do tipo RJ-45;

5.1.9 Deve possuir, no mínimo, 10 (dez) interfaces físicas de rede de 10 Gbps do tipo SFP/SFP+, devendo ser fornecidos os respectivos transceivers na quantidade de interfaces físicas solicitada;

5.1.10 Deve possuir, no mínimo, 4 (quatro) interfaces físicas de rede de 25 Gbps do tipo SFP28, devendo ser fornecidos os respectivos transceivers na quantidade de interfaces físicas solicitada;

5.1.11 Devem ser fornecidos 4(quatro) transceivers de 10 Gbps do tipo SFP+, homologados pela fabricante Cisco, a serem instalados nos dois roteadores Cisco ASR1001-X, existentes no datacenter do TCE-PI, a fim de possibilitar a interconexão dos firewalls aos referidos equipamentos;

5.1.12 Deve possuir, no mínimo, 1 (uma) interface física de rede de 1 Gbps dedicada para gerenciamento;

5.1.13 Deve possuir, no mínimo, 1 (uma) interface física dedicada para o recurso de alta disponibilidade;

5.1.14 Deve possuir, no mínimo, 1 (uma) interface física do tipo console ou similar;

5.1.15 Deve possuir disco do tipo Solid State Drive (SSD) de, no mínimo, 480 (quatrocentos e oitenta) GB de armazenamento do sistema operacional e registro de logs;

5.1.16 Deve possuir fonte de alimentação elétrica redundante capaz de operar entre 120 e 240 VAC devendo, em caso de problema com uma das fontes, permitir a substituição da fonte defeituosa com o equipamento em funcionamento (hot-swappable);

5.1.17 Deve suportar, no mínimo, 1.000 (um mil) clientes de VPN SSL simultaneamente estando, caso necessário, devidamente licenciado para este fim;

5.1.18 Deve suportar, no mínimo, 2.000 (dois mil) túneis de VPN IPSEC simultaneamente estando, caso necessário, devidamente licenciado para este fim;

5.1.19 Deve possuir suporte a criação de rede virtuais (VLAN), conforme o padrão IEEE 802.1Q, de, no mínimo, 1.000 (um mil) VLANs;

5.1.20 Deve implementar o protocolo LLDP – Link Layer Discovery Protocol;

5.1.21 Deve possuir o recurso de agregação de links conforme padrão IEEE 802.3ad (LACP) permitindo o agrupamento de interfaces físicas de rede em um link agrupado virtualmente (LAG – Link Aggregation Group);

5.1.22 Deve possuir o recurso de NAT – Network Address Translation nas modalidades de NAT estático 1 para 1, NAT dinâmico 1 para vários e NAT dinâmico vários para vários. Este recurso deve ser aplicado tanto para o endereço de origem quanto para endereço de destino. Deve possuir também NAT64 para tradução entre endereços IPv6 e IPv4 e NPTv6 (Network Prefix Translation) para tradução de um prefixo IPv6 para outro prefixo IPv6 prevenindo problemas de roteamento assimétrico;

5.1.23 Deve suportar a criação de rotas estáticas e os protocolos de roteamento estático e dinâmico RIPv2, OSPFv2 e OSPFv3 incluindo OSPF graceful restart e BGP;

5.1.24 Deve implementar o protocolo ECMP – Equal Cost Multiple Path para balanceamento de carga entre links baseados no hash do endereço IP de origem, no hash do endereço IP de origem e de destino, pela técnica conhecida como round-robin e com base no peso ou prioridade atribuídos a cada link. Deve suportar o balanceamento entre, no mínimo 4 (quatro) links;

5.1.25 Deve permitir o envio de logs para sistemas de monitoração externos utilizando o padrão syslog, bem como o envio de forma segura através do protocolo SSL/TLS;

5.1.26 Deve possuir o recurso de alta disponibilidade e permitir a configuração nos modos ativo/passivo e ativo/ativo;

5.1.27 Deve implementar controle por políticas/regras de firewall capaz de permitir ou bloquear o tráfego de rede por porta e protocolo, por aplicações, por grupos estáticos de aplicações, por grupos dinâmicos de aplicações baseados em características e comportamento das aplicações, por usuários e grupos de usuários, por endereços IP e faixas de endereços IP e por país de origem e destino do tráfego;

5.1.28 A identificação do país deve ser através do código do país, por exemplo, BR, USA, UK, RUS, etc e também através de geolocalização possibilitando a criação de regiões geográficas;

5.1.29 Deve permitir configurar o agendamento das políticas/regras de firewall para habilitar ou desabilitar tais políticas/regras em horários pré-definidos;

5.1.30 Deve possuir a capacidade para realizar a descriptografia do tráfego SSL e SSH permitindo o controle e inspeção tanto do tráfego de entrada quanto de saída. A descriptografia deve ser realizada com base em políticas/regras de acordo com a origem e destino do tráfego;

5.1.31 Deve possuir recurso de QoS – Quality of Service com suporte a DSCP – Differentiated Services Code Point. Deve permitir também definir, baseado em políticas/regras, a prioridade e o limite máximo de largura de banda de um determinado tipo de tráfego. As definições de prioridade e limite de largura de banda devem ser baseadas no endereço IP de origem e destino, no usuário e na aplicação;

5.1.32 Deve possuir a capacidade de reconhecer, no mínimo, 3.000 (três mil) aplicações diferentes tais como redes sociais, compartilhamento de arquivos, e-mail, atualização de softwares, acesso remoto, VoIP, áudio e vídeo, peer-to-peer, sistemas de mensagem instantânea etc., sendo esta uma lista não exaustiva;

- 5.1.33** O reconhecimento da aplicação se dará, independentemente de porta e protocolo, através de, no mínimo, os seguintes métodos: baseado na assinatura da aplicação conhecida pelo fabricante da solução de firewall, através da decodificação de protocolos para detectar aplicações encapsuladas dentro do protocolo e identificação através de análise heurística a fim de detectar aplicações através de análise comportamental do tráfego analisado;
- 5.1.34** Deve permitir a criação de assinaturas personalizadas para o reconhecimento de aplicações proprietárias na própria interface gráfica do equipamento sem a necessidade de intervenção do fabricante;
- 5.1.35** Deve permitir a diferenciação e controle de partes da aplicação como, por exemplo, em uma aplicação de mensagem instantânea permitir a troca de mensagens de texto e bloquear a transferência de arquivos por dentro da aplicação;
- 5.1.36** Deve permitir bloquear sessões TCP que utilizarem variações do three-way handshake como four-way e o five-way split handshake, prevenindo assim possíveis tráfegos maliciosos;
- 5.1.37** Deve permitir bloquear conexões que contenham dados no payload dos pacotes TCP SYN e TCP SYN-ACK durante o three-way handshake;
- 5.1.38** A solução de firewall deve possuir funcionalidades de IPS, antivírus e anti-spyware que permita o bloqueio de vulnerabilidades e exploits conhecidos e proteção contra vírus e spywares baseado em assinaturas de ameaças conhecidas;
- 5.1.39** Deve ser possível a criação de assinaturas customizadas de ameaças;
- 5.1.40** Deve permitir realizar o bloqueio de vírus realizando a inspeção em, no mínimo, os protocolos HTTP, FTP, SMB, SMTP e POP3. Será permitido o uso de appliance externo para o bloqueio de vírus caso a solução de firewall ofertada não realize nativamente a inspeção em algum dos protocolos solicitados;
- 5.1.41** Deve possuir a capacidade de detectar e prevenir ameaças em tráfego HTTP/2;
- 5.1.42** Deve possuir proteção contra ataques de negação de serviço (DoS) capaz de impedir ataques de SYN Flood, ICMP Flood, UDP Flood, etc e deve também bloquear port scans, bloquear ataques de buffer overflow e identificar e bloquear comunicação com botnets;
- 5.1.43** Para cada ameaça detectada pela solução deve ser realizado o registro nos logs do sistema das informações de data e hora, tipo da ameaça, origem e destino da comunicação e a ação tomada (se permitiu ou bloqueou o tráfego);
- 5.1.44** A solução de firewall deve possuir funcionalidade de filtro URL que permita a criação de políticas/regras para controle do acesso a websites baseado em categorias de URL devendo o fabricante da solução disponibilizar a base de dados de URL categorizadas para consulta por parte da solução. As políticas/regras que permitem ou bloqueiam o acesso a determinada categoria de URL devem ser com base no usuário e grupos de usuários e por endereços IP e faixas de endereços IP;
- 5.1.45** A funcionalidade de filtro URL deve possuir categoria específica para classificar domínios recém registrados com menos de 30 dias;
- 5.1.46** Deve permitir a criação de categoria de URL customizada permitindo inserir uma lista de URLs específicas;
- 5.1.47** Deve permitir a customização da página de bloqueio exibida ao usuário quando este tentar realizar um acesso a um website pertencente a uma categoria de URLs bloqueada;
- 5.1.48** Deve possuir recurso para proteger contra o roubo de credenciais de usuário e senha, identificadas através da integração com o Active Directory, submetidas em sites não corporativos. Deve ser possível definir em quais websites é permitido ou bloqueado o envio das credenciais baseado na categoria de URL a qual o website pertencer. Caso o usuário tente submeter suas credenciais de usuário e senhas pertencentes ao Active Directory em um website não autorizado deve ser exibida uma página de bloqueio informando que o uso de tais credenciais no website específico não está autorizado;
- 5.1.49** A solução de firewall deve possuir recurso que permita bloquear a transferência de arquivos baseado na extensão dos mesmos e definir por qual aplicação a transferência do arquivo está bloqueada, por exemplo, bloquear a transferência de arquivos .exe através de web browser. Deve permitir bloquear, no mínimo, arquivo com as extensões .exe, .bat, .dll, .pif e .torrent;
- 5.1.50** A solução de firewall deve possuir integração com LDAP, MS Active Directory e RADIUS para identificação dos usuários e grupos da rede para uso nas políticas/regras baseadas por usuários e grupo de usuários;
- 5.1.51** A integração com MS Active Directory para identificação dos usuários da rede deve ser realizada sem a necessidade de instalação de um agente no Controlador de Domínio e nem nas estações dos usuários;
- 5.1.52** A solução de firewall deve possuir recurso de portal de autenticação prévia (Captive Portal) para identificação dos usuários que realizam o acesso à internet, sem a necessidade de instalação de software cliente ou agente no computador. O portal de autenticação deve ser exibido antes de o usuário iniciar a navegação pela internet;
- 5.1.53** A solução de firewall deve possuir o recurso de VPN – Virtual Private Network dos tipos site-to-site e client-to-site e suportar IPsec – Internet Protocol Security e SSL – Secure Sockets Layer;
- 5.1.54** O recurso de VPN IPsec deve suportar os algoritmos de criptografia 3DES, AES 128, AES 192 e AES 256, os algoritmos de autenticação MD5 e SHA 1, o algoritmo IKEv1 e IKEv2 e os algoritmos de troca de chaves Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 e Grupo 14 e suportar também a autenticação através de certificados IKE PKI;
- 5.1.55** O recurso de VPN SSL deve permitir que o usuário remoto se conecte através de um software cliente de VPN instalado no sistema operacional do equipamento do usuário sendo possível a atribuição de endereços IP fixos e atribuição de DNS ao mesmo;
- 5.1.56** Deve suportar a autenticação dos usuários remotos que se conectam à VPN via LDAP, MS Active Directory, TACACS+, RADIUS, SAML e através de base de usuários local no equipamento da solução de firewall. Deve suportar também a autenticação via certificado e OTP – One Time Password;

5.1.57 Deve ser disponibilizado o software cliente de VPN do mesmo fabricante da solução de firewall ofertada compatível para instalação em computadores com sistema operacional MS Windows 8, MS Windows 10, MacOS e Linux e para instalação em dispositivos móveis Android e IOS;

5.1.58 O recurso de VPN SSL deve possuir mecanismo de checagem da conformidade do computador do usuário remoto e a checagem deve permitir verificar, no mínimo, as informações de qual sistema operacional e patches estão instalados, se o antivírus está instalado e ativo no computador, se o firewall está instalado e ativo no computador, se o disco está criptografado, se o agente de DLP – Data Loss Prevention está instalado e ativo, informações de chaves de registro e processos ativos no computador;

5.1.59 Deve ser possível criar perfis customizados de conformidade com, no mínimo, as mesmas informações obtidas pelo mecanismo de checagem da conformidade do computador do usuário remoto. Tais perfis devem ser utilizados para assegurar que apenas computadores de usuários remotos que atendem aos requisitos solicitados nos perfis customizados possam ter acesso através da VPN aos dados e sistemas hospedados na rede interna do órgão;

5.1.60 A solução de firewall deve possuir console de gerenciamento do equipamento acessada através de interface gráfica web permitindo realizar as configurações da solução como criar e administrar as políticas/regras de firewall e controle de aplicações, criar e administrar as políticas de IPS, antivírus e anti-spyware, criar e administrar as políticas de filtro URL, monitorar e investigar os registros de logs de eventos e demais configurações;

5.1.61 Deve suportar a autenticação dos usuários administradores que se conectam à interface de gerenciamento do equipamento via LDAP, MS Active Directory, RADIUS e através de base de usuários local no equipamento da solução de firewall;

5.1.62 Deve ser possível criar perfis de acesso à interface de gerenciamento com permissões granulares como acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações entre outros;

5.1.63 Deve permitir realizar o backup das configurações do equipamento e a restauração da configuração salva através de interface de gerenciamento;

5.1.64 A interface de gerenciamento do equipamento deve possuir recurso para análise das políticas indicando, quando houver, regras que ofusquem, conflitem ou sobreponham outras regras (shadowing) e quais objetos não estão sendo utilizados, para avaliação de elementos dispensáveis, permitindo assim, a higienização gradual das regras e seus respectivos elementos. Deve possuir também recurso para análise das políticas indicando, quando houver, regras baseadas em porta e protocolo, permitindo a conversão para uma regra baseada em aplicação, melhorando assim o controle do tráfego e a segurança do ambiente. É permitido o uso de appliance externo para realização da análise das políticas, devendo o mesmo ser fornecido em conjunto com a solução de firewall e estar devidamente licenciado;

5.1.65 Deve ser possível, através de interface de gerenciamento do equipamento, a geração de relatórios tais como um resumo gráfico das aplicações utilizadas e ameaças vistas, principais aplicações por utilização de largura de banda, atividades de um usuário ou grupo de usuários específicos, incluindo aplicações e URLs acessadas e permitir a criação de relatórios personalizados;

5.1.66 Deve ser possível gerar relatório de visibilidade e uso das aplicações do tipo SaaS – *Software as a Service*, mostrando os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso à aplicação e o consumo da aplicação SaaS pelo usuário;

5.1.67 Deve ser exibida na interface gráfica de gerenciamento do equipamento informações em tempo real, atualizadas de forma automática a cada 1 (um) minuto, as principais aplicações acessadas, o risco das principais aplicações, número de sessões simultâneas, status das interfaces de rede e uso de CPU;

5.1.68 Deve ser possível configurar o envio de alertas do sistema via e-mail;

5.1.69 Deve suportar o monitoramento via SNMPv3;

5.1.70 O sistema operacional a ser instalado no equipamento que compõe a solução deverá ser fornecido em sua versão mais atualizada, não sendo aceito sistema operacional de uso genérico;

5.1.71 Por cada equipamento que compõe a solução de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;

5.1.72 Na data do certame, nenhum dos equipamentos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

5.1.73 Durante o período de vigência do contrato de garantia todos os componentes da solução de firewall, incluindo o equipamento, o sistema operacional, as licenças necessárias para atender as funcionalidades e recursos solicitados, os softwares clientes de VPN e demais itens necessários para o perfeito funcionamento devem estar cobertos por garantia e suporte técnico do fabricante da solução em caso de problema;

5.1.74 A solução de firewall deve possuir garantia pelo período de, no mínimo, 60 (sessenta) meses, compreendendo a reposição de peças/equipamentos, atualizações do sistema operacional do equipamento, softwares e das assinaturas de proteção da solução.

5.2 SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO

5.2.1 A contratada deverá prestar serviços de instalação e configuração da solução, que compreendem, entre outros, os seguintes procedimentos:

5.2.1.1 Reunião de alinhamento para criação do escopo do projeto previamente a instalação;

5.2.1.2 Instalação física de todos os equipamentos (hardware) e licenças (softwares) adquiridos no local determinado pela equipe responsável pelo projeto por parte da contratante. Deve considerar também a instalação em modo Alta Disponibilidade (ativo/passivo);

5.2.1.3 Análise da topologia e arquitetura da rede, considerando todos os equipamentos já existentes e instalados;

- 5.2.1.4** Análise do acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;
- 5.2.1.5** Migração das regras de firewall existentes e aplicáveis à solução ofertada, considerando a adequação às políticas de aplicações em camada 7;
- 5.2.1.6** Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;
- 5.2.1.7** Configuração do sistema de firewall, VPN, IPS, Filtro URL, Antivírus e Anti-malware de acordo com as exigências levantadas;
- 5.2.2** Toda configuração do sistema deverá ser realizada de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada. O fabricante deverá disponibilizar ferramenta gratuita para acompanhamento da evolução da parametrização de proteção dos firewalls afim de garantir a melhor eficiência da solução durante o período de vigência das licenças;
- 5.2.3** Repasse de informação das configurações realizadas no formato hands-on de 20 horas para a equipe responsável pelo projeto por parte da contratante após validação da migração;

CLÁUSULA SEXTA – CONDIÇÕES DE PAGAMENTO

6.1. O pagamento do objeto contratado efetivamente executado será efetuado mediante ordem de crédito em conta corrente da CONTRATADA, indicada na sua proposta, e dar-se-á no prazo máximo de 30 (trinta) dias, contados após o requerimento de pagamento, que deverá ser efetuado pelo sistema SEI – Sistema Eletrônico de Informações, conforme Portaria nº 643, de 29 de julho de 2022, publicada no Diário Oficial Eletrônico do TCE/PI nº 142/2022, de 01/08/2022, que estabelece regras técnicas para utilização do sistema, acompanhado dos seguintes documentos:

- 6.1.1 Nota de Empenho (cópia);
- 6.1.2 Nota Fiscal, atestada pelo Fiscal do Contrato;
- 6.1.3 Comprovantes da entrega do material e/ou da prestação efetiva do serviço;
- 6.1.4 Certidões de Regularidade Fiscal e Trabalhista ou Declaração do Sistema de Cadastramento Unificado de Fornecedores (SICAF)
- 6.1.5 Comprovação da condição de optante do SIMPLES: apenas credores optantes;
- 6.1.6 Outros documentos contratualmente exigidos: o credor deve verificar particularidades estabelecidas no instrumento contratual como: relatórios, comprovantes de cumprimento de obrigações tributárias, previdenciárias, trabalhistas ou outros.

6.2 O prazo para pagamento somente começará a fluir a partir da data da solicitação de pagamento devidamente instruído.

6.3 Se a Nota Fiscal apresentar irregularidades, falhas ou omissões que comprometam a liquidação da despesa, o prazo supracitado será contado a partir da data em que tais impropriedades forem sanadas.

6.4 O desconto de qualquer valor no pagamento devido ao contratado será precedido de processo administrativo em que será garantido à empresa o contraditório e a ampla defesa, com os recursos e meios que lhes são inerentes.

6.5 Não haverá, em hipótese alguma, pagamento antecipado.

6.6 Os casos omissos obedecerão ao previsto no art. 73 e da Lei nº 8.666/93.

6.7 No caso de eventuais atrasos de pagamento, desde que a licitante vencedora não tenha concorrido de alguma forma para tanto, incidirão correção monetária e juros moratórios. Fica convencionado que a correção monetária e os encargos moratórios devidos pelo Tribunal de Contas do Estado do Piauí entre a data acima referida e a do efetivo pagamento da nota Fiscal/fatura será calculada por meio da aplicação da seguinte fórmula:

$EM = I \times N \times VP$, onde:

EM= Encargos moratórios;

N= Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP= valor da parcela em atraso

I = índice de compensação financeira = 0,00016438, assim apurado:

$I = i/365$ $I = 0,06/365$ $I = 0,00016438$

Sendo: I = taxa percentual no valor de 6% a.a.

CLÁUSULA SETIMA – PRAZO DE ENTREGA DO OBJETO.

7.1 O prazo para entrega e instalação dos equipamentos será de até 90 (noventa) dias corridos, contados da assinatura do contrato.

CLÁUSULA OITAVA – CONDIÇÕES DE RECEBIMENTO DO OBJETO

O objeto será recebido pela Divisão de Redes e Segurança, pertencente à Secretaria de Tecnologia da Informação, conforme a seguir:

8.1 O recebimento de quaisquer itens, necessariamente, será realizado dentro do expediente do TCE-PI, no intervalo das 7h às 14h, dias úteis;

8.2 O objeto será recebido da seguinte forma.

8.2.1 Provisoriamente, no dia da conclusão da instalação e configuração dos equipamentos, para verificação da conformidade com as especificações constantes deste Termo de Referência.

8.2.2 O Termo de Recebimento Definitivo será emitido em até 10 (dez) dias úteis contados da data de recebimento do Termo de Recebimento Provisório.

CLÁUSULA NONA – OBRIGAÇÕES DA CONTRATANTE

9.1 Designar os servidores que atuarão como fiscais do contrato/comissão, que deverão:

9.1.1 Informar ao gestor do contrato se os prazos foram cumpridos pela empresa CONTRATADA e demais fatos que achar relevante para a perfeita gestão do contrato;

9.1.2 Tanto a comissão de recebimento como os fiscais do contrato devem cumprir integralmente o que for determinado por meio de qualquer acordo, termo de compromisso ou qualquer outro documento expedido pelo TCE-PI, sem comprometimento das obrigações estabelecidas neste Termo de Referência.

9.1.3 Receber o objeto no prazo e condições estabelecidas no Edital e seus anexos;

9.1.4 Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;

9.2 Proporcionar todas as condições necessárias, para que a CONTRATADA possa cumprir seus deveres;

9.3 Fiscalizar, com o auxílio da área técnica, o cumprimento, por parte da CONTRATADA, das exigências legais e de eficiência, eficácia, efetividade e economicidade do contrato.

9.4 Efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto, após recebimento e atesto da Nota Fiscal/Fatura, comprovando o efetivo fornecimento, no prazo e forma estabelecidos no Edital e seus anexos;

9.5 Rejeitar, no todo ou em parte, os produtos fornecidos em desacordo com as obrigações assumidas;

9.6 Permitir acesso dos empregados da Contratada às suas dependências, equipamentos, softwares e sistemas de informação necessários à execução dos serviços;

9.7 Prestar as informações e os esclarecimentos pertinentes que venham a ser solicitados pelos empregados da Contratada ou por seus prepostos.

CLÁUSULA DÉCIMA - OBRIGAÇÕES DA CONTRATADA

10.1 Entregar os equipamentos adquiridos no Tribunal de Contas do Estado do Piauí, localizado na Av. Pedro Freitas, 2100, Centro Administrativo, CEP: 64018-900, Teresina-PI;

10.2 Fornecer suporte técnico, pelo período de 60 (sessenta) meses, contados do recebimento definitivo das licenças;

10.3 Disponibilizar central de atendimento via telefone (0800 ou com custo de ligação local) e meio eletrônico para realização de requisições de execução de serviço ou resolução de dúvidas durante 7 (sete) dias por semana, 24 (vinte e quatro) horas por dia, inclusive feriados, prevalecendo a especificação de cada item;

10.4 Conceder ao TCE-PI acesso ao sistema de controle de chamados, para acompanhamento dos chamados técnicos, ficando o encerramento destes condicionados ao aceite do Tribunal;

10.5 Para todo o objeto da licitação, apresentar, no ato da assinatura do contrato, declaração do fabricante dos softwares ou do distribuidor autorizado no Brasil, com menção ao edital ou ao Tribunal de Contas do Piauí, afirmando que a licitante está apta a comercializar e prestar garantia e assistência técnica em seus produtos.

10.6 Fornecer o licenciamento dos produtos acompanhado de chaves de ativação e demais itens necessários à sua perfeita instalação e funcionamento, contemplando as versões indicadas no Edital ou as versões mais recentes disponibilizadas pelo fabricante, observando todas as especificações técnicas consignadas em sua proposta comercial.

10.7 Fornecer credenciais de acesso ao(s) site(s) do fabricante, para a realização de “downloads” de correções, atualizações recentes, drivers, e quaisquer “softwares” de apoio ali disponibilizado, mantendo a conta corporativa já existente em nome do Tribunal de Contas do Estado do Piauí.

10.8 Validar, sempre que necessário, em razão de eventuais mudanças de nomenclatura dos produtos, os novos nomes e códigos referentes às versões mais atualizadas.

10.9 Fornecer a documentação técnica completa e atualizada dos produtos adquiridos, contendo manuais do fabricante, guias de instalação e outros documentos pertinentes, sempre em suas versões originais;

10.10 A documentação poderá ser disponibilizada em site do fabricante, com acesso liberado ao Contratante.

10.11 Disponibilizar ao Contratante, acesso, sem quaisquer ônus adicionais, ao site que contenha Base de Conhecimento do fabricante sobre os produtos contemplados no objeto do ajuste;

10.12 Manter, durante todo o período de vigência do contrato, todas as condições de habilitação que ensejaram sua contratação.

10.13 Não veicular publicidade acerca dos serviços contratados, sem prévia autorização, por escrito, do CONTRATANTE.

10.14 Manter sigilo, sob pena de responsabilidade civil e penal, sobre todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto deste Contrato, devendo orientar seus empregados nesse sentido.

10.15 Manter em caráter confidencial, mesmo após o término do prazo de vigência ou rescisão do contrato, as informações relativas:

10.15.1 À política de segurança adotada pela CONTRATANTE e as configurações de hardware e de softwares decorrentes;

10.15.2 Ao processo de instalação, configuração e customizações de produtos, ferramentas e equipamentos;

10.15.3 Ao processo de implementação, no ambiente da CONTRATANTE, dos mecanismos de criptografia e autenticação;

10.16 Comunicar ao Contratante, por escrito, qualquer anormalidade verificada na entrega dos produtos, fornecendo os devidos esclarecimentos, sempre que solicitados.

10.17 Cumprir, sem ônus adicionais ao Contratante, todas as cláusulas contratuais que definam suas obrigações.

10.18 Executar fielmente o objeto contratado, de acordo com as normas legais, em conformidade com a proposta apresentada e nas orientações da Contratante, observando sempre os critérios de qualidade aplicáveis.

10.19 Aceitar nas mesmas condições contratuais acréscimos ou supressões nos termos do artigo 65, § 1º, da Lei nº 8.666/92.

CLÁUSULA DÉCIMA PRIMEIRA – DINÂMICA DE EXECUÇÃO, INSTRUMENTO DE SOLICITAÇÃO DOS SERVIÇOS E NÍVEIS DE SERVIÇOS EXIGIDOS.

11.1 Dinâmica de Execução

11.1.1 No ato da entrega dos equipamentos, deverão ser fornecidos manuais técnicos do usuário e de referência contendo todas as informações sobre os produtos e instruções para instalação, configuração, operação e administração (quando aplicáveis), todos atualizados, em meio impresso e eletrônico, de preferência em idioma português, caso contrário em idioma inglês;

11.1.2 A empresa CONTRATADA deverá entregar, às suas expensas, todos os itens acessórios de hardware e software necessários à perfeita instalação e funcionamento dos equipamentos, incluindo conectores, licenças registradas em nome do TCE-PI, interfaces, suportes e demais equipamentos necessários para instalação e funcionamento da solução CONTRATADA, em plena compatibilidade com as especificações constantes neste Termo de Referência e recomendadas pelo fabricante;

11.1.3 O prazo para entrega e instalação dos equipamentos será de até 90 (noventa) dias corridos, contados da assinatura do contrato;

11.1.4 A instalação de qualquer software que faça parte das soluções contratadas, será de responsabilidade do fornecedor, cabendo a este inclusive fornecer suporte técnico, caso necessário;

11.1.5 A empresa CONTRATADA será responsável pela instalação física de todos os equipamentos que façam parte do objeto deste Termo de Referência.

11.2 Instrumentos de Solicitação do(s) Serviço(s)

11.2.1 Um canal de suporte técnico através de serviço telefônico será disponibilizado pela contratada através de um número de telefone gratuito (0800 ou ligação com custo de local) a um Centro de Atendimento por Voz, com atendimentos obrigatoriamente na língua portuguesa, devendo esse Centro operar de forma ininterrupta, 24x7(vinte e quatro horas por dia, sete dias por semana).

11.2.2 Um canal de suporte técnico através de Portal web e/ou correio eletrônico (e-mail), deverá ser disponibilizado pela contratada de forma ininterrupta 24x7(vinte e quatro horas por dia, sete dias por semana).

11.2.3 Os chamados técnicos deverão possuir identificador de ocorrência próprio, data e hora de abertura devidamente repassada ao CONTRATANTE, a fim de registro e acompanhamento das ocorrências;

11.2.4 A CONTRATADA deverá informar o número do chamado e disponibilizar um meio de acompanhamento das ocorrências;

11.2.5 Ao final de cada atendimento, a CONTRATADA deverá emitir relatório técnico contendo as seguintes informações:

A Nº do chamado;

B Categoria de prioridade;

C Descrição do problema e da solução;

D Procedimentos realizados;

E Data e hora da abertura e do fechamento do chamado;

F Data e hora do início e do término da execução dos serviços; e

G Identificação do técnico da empresa.

11.2.6 Os tempos de resposta e de solução para os chamados técnicos abertos serão contados a partir do registro através de contato telefônico ou por outro meio disponível.

11.2.7 Em caso de atraso na conclusão do atendimento, em qualquer nível de prioridade, será admitida a proposição, pela CONTRATADA, de justificativa técnica, a qual deverá conter os motivos do atraso, acompanhada da devida comprovação;

11.2.8 A justificativa eventualmente apresentada será analisada pela Administração a qual emitirá parecer, para fins de aceitação ou não da justificativa;

11.2.9 Em sendo aceita, ocorrerá tão somente a interrupção dos prazos contratuais, sem prejuízo da conclusão do chamado. Em não sendo aceita, impor-se-á as sanções previstas na forma da execução contratual, bem como no Item Penalidades deste Termo de Referência;

11.2.10 A justificativa deverá ser apresentada em até 03 (três) dias úteis após a conclusão do chamado. Uma vez apresentada fora deste prazo, caberá a Administração conhecer ou não o documento;

11.3 Níveis de Serviços Exigidos (NSE)

11.3.1 Os chamados técnicos serão classificados pelo Fiscal Técnico, por criticidade, de acordo com o impacto no ambiente computacional, conforme abaixo:

11.3.1.1 **Prioridade ALTA:** Sistema indisponível ou com severa degradação de desempenho;

11.3.1.2 **Prioridade MÉDIA:** Sistema disponível, com mau funcionamento, que implique em baixa degradação de desempenho ou comprometimento em um de seus elementos que implique em risco para a disponibilidade do sistema;

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

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

11.3.2.1 Os chamados de **Prioridade ALTA** deverão ser atendidos em até 4(quatro) horas, contado da validação do chamado, e solucionados em até 24 (vinte e quatro) horas do início do atendimento;

11.3.2.2 Os chamados de **Prioridade MÉDIA** deverão ser atendidos em até 1(um) dia e solucionados em até 48 (quarenta e oito) horas a contar do início do atendimento;

11.3.2.3 Os chamados de **Prioridade BAIXA** deverão ser atendidos em até 2 (dois) dias e solucionados em até 48 (quarenta e oito) horas a contar do início do atendimento, podendo ser realizados de forma remota, se for possível;

11.3.3 Os chamados poderão ser escalados pelo Fiscal Técnico para níveis mais altos ou mais baixos, de acordo com a criticidade do problema. Nesse caso, os prazos de solução serão automaticamente ajustados, a partir da notificação de mudança, para o novo nível de prioridade;

11.3.4 Chamados de **Prioridade ALTA** não serão escalonados para níveis mais baixos, salvo situação de manifesto engano por parte da CONTRATANTE.

CLÁUSULA DÉCIMA SEGUNDA – DIREITO DE PROPRIEDADE INTELECTUAL

12.1 Direitos de Propriedade Intelectual

12.1.1 Os conhecimentos técnicos repassados para a equipe técnica do TCE-PI serão utilizados em casos de interrupção, transição e encerramento contratual, de modo a minimizar impactos e permitir que as necessidades do Tribunal não sejam prejudicadas ou interrompidas;

12.1.2 A CONTRATADA cederá ao Tribunal de Contas do Estado do Piauí, nos termos do artigo 111 da Lei nº 8.666/93, concomitante com o art. 4º da Lei nº 9.609/1998, o direito patrimonial e a propriedade intelectual em caráter definitivo dos sistemas desenvolvidos e resultados produzidos em consequência do cumprimento deste contrato, entendendo-se por resultados quaisquer estudos, relatórios, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, fluxogramas e documentação didática, em papel ou mídia eletrônica.

CLÁUSULA DÉCIMA TERCEIRA – MONITORAMENTO DA EXECUÇÃO

13.1 Monitoramento da Execução

13.1.1 O acompanhamento e fiscalização da execução do contrato serão exercidos pelos fiscais do contrato, especialmente designados para este fim, que deverão informar a Seção de Gestão Contratual as ocorrências durante seu andamento;

13.1.2 Compete à Seção de Gestão Contratual e aos fiscais do contrato dirimir eventuais dúvidas que surgirem no curso da sua prestação e de tudo dar ciência à empresa CONTRATADA, para fiel execução contratual durante toda a vigência do contrato, de acordo com os termos do Art. 67 da Lei nº 8.666/93;

13.1.3 Sem prejuízo da plena responsabilidade da empresa CONTRATADA perante o TCE-PI ou a terceiros, os serviços estarão sujeitos à mais ampla e irrestrita fiscalização;

13.1.4 A presença dos servidores designados como fiscais do contrato não diminuirá a responsabilidade contratual da empresa CONTRATADA.

13.1.5 O Contrato oriundo do procedimento licitatório será acompanhado e fiscalizado por servidor (fiscal) integrante da Secretaria de Tecnologia da Informação - TCE/PI, designado especialmente para tal fim, o qual fiscalizará a execução do objeto, anotando em registro próprio todas as ocorrências relacionadas com a execução, observando-se o exato cumprimento de todas as cláusulas e condições contratuais, determinando quando necessário, a regularização das falhas observadas, cabendo ao referido servidor o "ATESTO" das respectivas Notas Fiscais, conforme prevê o art. 67 da lei 8.666/93 e Resolução TCE/PI nº 28 de 03/11/2016 – publicado do Diário Oficial Eletrônico nº 207/16 de 08/11/2016.

CLÁUSULA DÉCIMA QUARTA – QUALIFICAÇÃO TÉCNICA DOS PROFISSIONAIS

14.1 A CONTRATADA encaminhará a relação nominal dos técnicos capacitados para execução dos serviços, desde que prestados diretamente pela contratada, contendo a indicação dos perfis exigidos, acompanhada dos currículos individuais e credenciais e/ou certificados que comprovem sua qualificação técnica nos equipamentos e/ou serviços contratados. A lista deverá ser encaminhada ao fiscal do contrato no prazo máximo de 72 horas antes do início da execução dos serviços;

14.2 Tais documentos deverão ser encaminhados à Secretaria de Tecnologia da Informação – STIF;

14.3 Durante a execução do objeto da licitação, sempre que houver alteração da relação de técnicos, a CONTRATADA deverá remeter à STIF, em até 3 dias úteis antes do efetivo envio dos novos técnicos, lista atualizada, bem como currículos e cópias dos certificados e documentos relativos aos novos técnicos incluídos na lista;

14.4 O Tribunal analisará a documentação recebida, de acordo com as especificações técnicas deste Termo, podendo solicitar a substituição dos profissionais que não possuam as qualificações mínimas exigidas para o perfil;

14.5 Apenas os técnicos formalmente indicados pela CONTRATADA podem ser alocados para execução dos serviços, exceto em situações excepcionais mediante anuência prévia do Tribunal;

14.6 Para cumprir todas as atividades previstas, a CONTRATADA deverá empregar esforços de técnicos treinados e certificados pelo fabricante dos produtos, visando uma atuação mais eficiente e a perfeita execução dos serviços ora contratados;

14.7 A CONTRATADA deverá indicar um profissional para Gerenciamento do Projeto e que ficará sendo o ponto focal de comunicação entre a mesma e o TCE-PI.

14.8 Todas as atividades de implantação serão realizadas obrigatoriamente por profissionais devidamente capacitados pelos fabricantes e indicados pela CONTRATADA devendo esta condição ser devidamente comprovada;

14.9 A comprovação do vínculo profissional formal dos técnicos com a CONTRATADA deverá ser feita mediante apresentação de um dos seguintes documentos:

14.9.1 No caso de vínculo empregatício: cópia da Carteira de Trabalho e Previdência Social (CTPS), expedida pelo Ministério do Trabalho, contendo as folhas que demonstrem o número de registro e qualificação civil;

14.9.2 No caso de vínculo societário: ato constitutivo da empresa devidamente registrado no órgão de Registro de Comércio competente, do domicílio ou da sede do licitante;

14.9.3 No caso de profissional autônomo: contrato de prestação de serviços;

14.9.4 Outros documentos hábeis à comprovação do vínculo profissional.

CLÁUSULA DÉCIMA QUINTA – GARANTIA DO OBJETO

15.1 Garantia do objeto

15.1.1 As condições exigidas a seguir se aplicam a todos os equipamentos presente nesta aquisição;

15.1.2 A CONTRATADA deverá prestar serviços de atendimento técnico e garantia, dos itens do objeto, inclusive atualizações e correções, pelo período de **60 (sessenta) meses**, a contar da data do recebimento definitivo dos produtos e serviços, compreendendo, sem custos a CONTRATANTE, dentre outros:

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

15.1.2.2 Atualizações, corretivas e evolutivas, de drivers, firmwares, softwares e manuais, durante a vigência da garantia;

15.1.2.3 Ajustes e configurações conforme manuais e normas técnicas do fabricante;

15.1.2.4 Demais procedimentos destinados a recolocar os equipamentos em perfeito estado de funcionamento;

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

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

15.1.3 Caso o equipamento incorpore software de propriedade de outros fabricantes, todo suporte deve ser feito pelo fornecedor (ponto único de contato para suporte);

15.1.4 A garantia de 60 (sessenta) meses, para todos os componentes ofertados na proposta, deverá ser comprovada pelo fabricante do equipamento (por meio de site, portal ou documentação) no momento da contratação, mediante propositura de carta de garantia com aval do fabricante;

15.1.5 A CONTRATADA (ou o fabricante) deverá ainda:

15.1.5.1 Revisar, semestralmente, as atualizações de drivers, firmwares e patches para todos os equipamentos e softwares contratados. Os serviços de atualizações deverão ocorrer somente para os classificados como críticos, e serão executados de forma remota ou on-site, com prévia anuência da Contratante;

15.1.5.2 Fazer uma avaliação semestral da “saúde” dos equipamentos sob contrato, de forma remota ou on-site, para auxiliar a identificar problemas relacionados à segurança, desempenho, configuração e disponibilidade, antes que causem impactos ou paradas não programadas ao ambiente da CONTRATANTE;

15.1.5.3 Revisar os boletins de suporte disponibilizados pelo respectivo fabricante, analisar suas aplicabilidades ao ambiente da CONTRATANTE e fazer recomendações específicas as quais poderão reduzir riscos e melhorar a operação;

15.1.5.4 Fornecer assistência de instalação remota para as devidas atualizações recomendadas.

15.1.5.5 Serão disponibilizados serviços de suporte (incluindo manutenção de hardware) durante 7 (sete) dias da semana, 24 (vinte e quatro) horas por dia, executando-os sempre que acionados pelo CONTRATANTE, mediante a abertura de chamado técnico, prestados por técnicos devidamente habilitados e credenciados pelo fabricante, com nível de certificação compatível com as atividades a serem executadas, e sem qualquer ônus adicional;

15.1.6 Os serviços de atendimento da central de assistência técnica deverão ser providos das seguintes formas:

15.1.6.1 Um canal de suporte técnico através de serviço telefônico será disponibilizado através de um número de telefone gratuito (0800 ou ligação com custo de local) a um Centro de Atendimento por Voz, com atendimentos obrigatoriamente na língua portuguesa, devendo esse Centro operar de forma ininterrupta, no mínimo, das 8h às 18h em dias úteis (8x5);

15.1.6.2 Um canal de suporte técnico através de Portal web e/ou correio eletrônico (e-mail), deverá ser disponibilizado de forma ininterrupta 24x7(vinte e quatro horas por dia, sete dias por semana).

15.1.7 Deverá ser disponibilizada, para a equipe técnica da CONTRATANTE, uma conta de acesso (somente leitura) para acompanhamento de chamados de suporte e manutenção abertos;

15.1.8 Deverá ser disponibilizada, para a equipe técnica da CONTRATANTE, uma conta de acesso para consulta de documentação técnica do fabricante e atualizações de software;

15.1.9 Entende-se por término do atendimento técnico a hora em que a solução for disponibilizada para uso em perfeitas condições de funcionamento, estando condicionado à aprovação da CONTRATANTE.

15.1.10 Os serviços de reparo dos equipamentos defeituosos serão executados “on site” (TCE-PI), onde o equipamento estiver instalado, salvo em caso de impossibilidade técnica devidamente justificada pela CONTRATADA.

15.1.11 No caso de ser necessária a retirada do equipamento defeituoso das dependências da CONTRATANTE, a CONTRATADA deverá relatar por escrito a situação ao Gestor do Contrato ou seu substituto, que autorizará por escrito a saída do referido equipamento, após constatar tal necessidade;

15.1.12 No caso de dispositivo de armazenamento que contenham informações de interesse da CONTRATANTE, tais como discos rígidos, a peça substituída ficará sob o poder da CONTRATANTE;

15.1.13 Substituir, temporária ou definitivamente, o equipamento defeituoso por outro de mesma marca e modelo e com as mesmas características técnicas, novo e de primeiro uso, quando então, a partir de seu efetivo funcionamento, ficará suspensa a contagem do prazo de reparo, nos casos em que não seja possível o reparo dentro dos prazos máximos estipulados acima;

15.1.14 Devolver, em perfeito estado de funcionamento, no prazo máximo de 30 (trinta) dias corridos, a contar da data de retirada dos equipamentos, aqueles que necessitem ser temporariamente retirados para conserto, ficando a remoção, o transporte e a substituição sob inteira responsabilidade da CONTRATADA;

15.1.15 Dentro do período de garantia, deverá ser substituída qualquer parte ou peça defeituosa, sem ônus para a CONTRATANTE.

15.1.16 No caso de troca de equipamento e/ou perda de configuração, a CONTRATADA será responsável por prestar o auxílio necessário ao técnico da CONTRATANTE, independentemente de onde o equipamento estiver;

15.1.17 Todos os custos relativos ao deslocamento de técnicos, eventual transporte de componentes e equipamentos, dentre outros, correrão exclusivamente por conta da CONTRATADA, independentemente do local do atendimento;

15.1.18 Caberá aos técnicos da fabricante ou da empresa autorizada pelo fabricante identificar os componentes, peças e materiais responsáveis pelo mau funcionamento dos produtos fornecidos e solucionar o problema;

15.1.19 O encerramento do chamado será dado por técnico da CONTRATANTE na conclusão dos serviços;

15.1.20 Relativamente à manutenção corretiva de hardware e software:

15.1.20.1 Efetuar, sem que isso implique acréscimo aos preços contratados, a substituição de qualquer equipamento, componente ou periférico por outro novo, de primeiro uso, com características idênticas ou superiores, no prazo de 10(dez) dias úteis, independente do fato de ser ou não fabricante dos equipamentos fornecidos, nos seguintes casos:

15.1.20.1.1 Se apresentar divergência com as especificações descritas na proposta apresentada;

15.1.20.1.2 Se no período de 15 (quinze) dias corridos, contados após a abertura do chamado técnico, ocorrerem defeitos recorrentes que não permitam seu correto funcionamento, mesmo tendo havido substituição de peças e componentes mecânicos ou eletrônicos.

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

15.1.20.3 Concluída a manutenção, a CONTRATADA fornecerá ao CONTRATANTE, documento em que conste a identificação do chamado técnico, data e hora de início e término da assistência técnica, descrição dos serviços executados, indicação da peça e/ou componente eventualmente substituído, assim como relato referente às

condições inadequadas ao funcionamento do equipamento ou sua má utilização, fazendo constar a causa e as medidas para a sua correção.

15.1.20.4 **Será admitida a subcontratação apenas dos serviços de assistência técnica da garantia**, desde que previamente autorizada por escrito pelo CONTRATANTE, por empresas comprovadamente autorizadas pelo fabricante dos equipamentos, observadas as mesmas condições de habilitação e qualificação no ato convocatório.

15.1.20.5 Dentro do período de garantia, em casos de falhas de hardware irreversíveis ou não solucionadas pelo suporte da CONTRATADA e do fabricante, este último ou seu distribuidor autorizado deverá providenciar troca por componente, módulo ou equipamento idêntico;

15.1.20.6 As peças quebradas, com defeito ou gastas pelo uso normal dos equipamentos, serão substituídas por outras de configuração idêntica ou superior, originais e novas, sem que isso implique acréscimo aos preços contratados;

CLÁUSULA DÉCIMA SEXTA – SANÇÕES ADMINISTRATIVAS

16.1 Comete infração administrativa nos termos da Lei nº 10.520, de 2002, a Contratada que:

16.1.1. inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

16.1.2 ensejar o retardamento da execução do objeto;

16.1.3 falhar ou fraudar na execução do contrato;

16.1.4 comportar-se de modo inidôneos

16.1.5 cometer fraude fiscal;

16.2 Pela inexecução do objeto deste contrato, a Administração pode aplicar à CONTRATADA as seguintes sanções:

16.2.1 advertência, por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante;

16.2.2 multas

16.2.2.1 Na hipótese de atraso na entrega do objeto, fica estabelecido o percentual de 0,2% sobre o valor dos itens em atraso, a título de multa, por dia de atraso;

16.2.2.2 Na hipótese de atraso no atendimento dos chamados de suporte, para cada ocorrência fica estabelecido o percentual de 0,02%, por hora de atraso, a ser calculado sobre o valor total adjudicado;

16.2.2.3 Multa compensatória diária de 0,03% (três centésimos por cento), sobre o valor contratado, caso haja a interrupção/suspensão dos serviços de garantia e/ou suporte técnico;

16.2.3 suspensão temporária de participação em licitação e impedimento de contratar com o Tribunal de Contas do Estado do Piauí, por prazo não superior a 2 (dois) anos;

16.2.4 impedimento de licitar e contratar com órgãos e entidades do Estado do Piauí com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;

16.2.5 declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;

16.3 A sanção de impedimento de licitar e contratar prevista no item anterior também é aplicável em quaisquer das hipóteses previstas como infração administrativa no subitem

16.4 As sanções previstas nos subitens 16.2.1, 16.2.3, 16.2.4 e 16.2.5 poderão ser aplicadas à CONTRATADA juntamente com as de multa.

16.5 Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

16.5.2 tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

16.5.3 tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

16.5.4 demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

16.6 O valor da multa poderá ser descontado das faturas devidas à CONTRATADA.

16.6.2 Se o valor a ser pago à CONTRATADA não for suficiente para cobrir o valor da multa a diferença será descontada da garantia contratual.

16.6.3 Se os valores das faturas e da garantia forem insuficientes, fica a CONTRATADA obrigada a recolher a importância devida no prazo de 15 (quinze) dias, contados da comunicação oficial.

16.6.4 Esgotados os meios administrativos para cobrança do valor devido pela CONTRATADA à CONTRATANTE, o débito será encaminhado para inscrição em dívida ativa.

16.6.5 Caso o valor da garantia seja utilizado no todo ou em parte para o pagamento da multa, esta deve ser complementada no prazo de até 10 (dez) dias úteis, contado da solicitação da CONTRATANTE.

17.7 A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

16.8 A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

16.9 As penalidades serão obrigatoriamente registradas e publicadas no SICAF.

CLÁUSULA DÉCIMA SÉTIMA – SUBCONTRATAÇÃO

17.1 Não será admitida a subcontratação do objeto desta licitação, com exceção dos casos especificados no Termo de Referência.

CLÁUSULA DECIMA OITAVA – REAJUSTE

18.1 Os preços inicialmente contratados são fixos e irrevogáveis no prazo de um ano contado da data limite para a apresentação das propostas.

18.2 Após o interregno de um ano, os preços iniciais poderão ser reajustados, mediante a aplicação do Índice de Custo da Tecnologia da Informação (ICTI), em conformidade com a legislação em vigor.

18.3 Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

CLÁUSULA DÉCIMA NONA – SUSTENTABILIDADE

19.1 A contratada deverá adotar critérios e práticas de sustentabilidade, observando, em especial, no que couber, a Portaria nº 170, de 10 de abril de 2012, do Instituto Nacional de Metrologia, Qualidade e Tecnologia (Inmetro) e a Lei nº 12.305, de 2 de agosto de 2010, que institui a Política Nacional de Resíduos Sólidos.

CLAUSULA VIGÉSIMA - RESCISÃO

20.1. A rescisão desta contratação se dará nos termos dos arts. 79 e 80 da Lei nº 8.666/93.

20.2. No caso de rescisão provocada por inadimplemento da CONTRATADA, o TCE/PI poderá reter, cautelarmente, os créditos decorrentes do contrato até o valor dos prejuízos causados, já calculados ou estimados.

20.3. A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

20.4. No procedimento que visa à rescisão do contrato, será assegurado o contraditório e a ampla defesa, sendo que, depois de encerrada a instrução inicial, a CONTRATADA terá o prazo de 5 (cinco) dias úteis para se manifestar e produzir provas, sem prejuízo da possibilidade de o TCE/PI adotar, motivadamente, providências acauteladoras.

20.5 O termo de rescisão será precedido de Relatório indicativo dos seguintes aspectos, conforme o caso:

20.5.1 Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

20.5.2 Relação dos pagamentos já efetuados e ainda devidos;

20.5.3 Indenizações e multas

CLÁUSULA VIGÉSIMA PRIMEIRA - CASOS OMISSOS.

21.1 Os casos omissos serão decididos pela CONTRATANTE, segundo as disposições contidas na Lei nº 8.666, de 1993, na Lei nº 10.520, de 2002 e nas e demais normas de licitações e contratos administrativos e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 “Código de Defesa do Consumidor” e normas e princípios gerais dos contratos.

CLÁUSULA VIGÉSIMA SEGUNDA – PUBLICAÇÃO

22.1 Incumbirá à CONTRATANTE providenciar a publicação deste instrumento, por extrato, no Diário Oficial Eletrônico do TCE/PI, no prazo previsto na Lei nº 8.666, de 1993.

CLÁUSULA VIGÉSIMA TERCEIRA – FORO

23.1 É eleito o Foro da Comarca de Teresina para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não possam ser compostos pela conciliação, conforme art. 55, §2º da Lei nº 8.666/93.

Para firmeza e validade do pactuado, o presente Termo de Contrato foi lavrado em duas (duas) vias de igual teor, que, depois de lido e achado em ordem, vai assinado pelos contraentes.

Conselheira Lilian de Almeida Veloso Nunes Martins
Presidente do Tribunal de Contas do Estado do Piauí

CONTRATANTE

Kent Johann Modes
Responsável legal da CONTRATADA

Teresina, Piauí, 15 de dezembro de 2022.



Documento assinado eletronicamente por **LILIAN DE ALMEIDA VELOSO NUNES MARTINS, Presidente**, em 15/12/2022, às 11:25, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **KENT JOHANN MODES, Usuário Externo**, em 15/12/2022, às 15:29, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site http://sei.tce.pi.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0029815** e o código CRC **01E7C2A7**.

Referência: Processo nº 101106/2022

SEI nº 0029815

Av. Pedro Freitas 2100 | Centro Administrativo | Teresina-PI | CEP: 64018-900

3215-3800 | CNPJ: 05.818.935/0001-01

tce@tce.pi.gov.br

Criado por [lucas.colares](#), versão 4 por [lucas.colares](#) em 15/12/2022 10:52:36.