Defensoria Pública
BAHIA

EDITAL

(**X**) Sistema de Registro de Preços

PREÂMBULO

1. Regência legal:

Esta licitação obedecerá as disposições da Lei estadual nº 9.433/05, da Lei Complementar nº 123/06, das normas gerais da Lei nº 8.666/93, e ainda, do Decreto estadual nº 19.896/20 (na modalidade pregão eletrônico), do Decreto estadual nº 19.252/19 (no Sistema de Registro de Preços), e respectivas alterações, além dos da legislação específica aplicável.

2. Requisito de participação:

(**X**) Ampla Participação
(X) Serviços – Sem reserva de cota
(X) Aquisição – Sem reserva de cota

3. Processo administrativo:
01.0485.2023.000003249-0

4. Órgão/entidade e setor:
DPE/COPEL/CMO

5. Modalidade/número de ordem:
(**X**) Pregão eletrônico nº 17/2023

5.1 Modo de disputa
(**X**) Aberto

5.2 Intervalo mínimo de diferença entre lances (degrau de valor ou percentual)
(X) Sim (conforme orçamento estimado em planilha - termo de referência)

6. Tipo de Licitação:
(**X**) Menor Preço (**X**) Global

7. Objeto da licitação:

Registro de preço, para eventual aquisição de soluções de Segurança da Informação com o propósito de ampliar a segurança da rede da DPE/BA, incluindo repasse de conhecimento, manutenção e suporte técnico por 60 (sessenta) meses de acordo com as condições, características e especificações constantes da Seção II -Termo de Referência objeto da licitação.

8. Regime de execução/fornecimento:

(X) **Serviço** com empreitada por preço (X) Unitário

9. Dotação orçamentária:

(**X**) Sistema de Registro de Preços
As despesas decorrentes da contratação correrão à conta da dotação orçamentária concernente aos órgãos ou entidades solicitantes, devendo cada contratação ser precedida da emissão da declaração de compatibilidade com a LRF.

10. Prazos:

(**X**) Sistema de Registro de Preços

10.1 O prazo de validade do registro será de 01 (um) ano, improrrogável.

10.2 O(s) fornecedor(es) será(ão) convocado(s) para assinar a Ata de Registro de Preços no prazo de até 10 (dez) dias, prorrogável por igual período.

11. Local, dia e hora para recebimento das propostas e documentos e início da sessão pública da licitação:

Site: www.licitacoes-e.com.br

Recebimento das propostas: das 09:00 horas do dia 20/06/2023 às 09:00 horas do dia 07/07/2023.

Início da sessão pública: às 11:00 horas do dia 07/07/2023.

12. Exame prévio da minuta e aprovação da assessoria jurídica:

(**x**) Declaro que a fase interna deste procedimento foi examinada pelo órgão legal de assessoramento jurídico, conforme o Parecer nº 259445/2023.

13. Interstício mínimo para o recebimento das propostas:

(**x**) 08 dias úteis **[pregão]**

14. Índice:

PARTE I – PROPOSTAS

(✓) SEÇÃO I. Especificações para elaboração da proposta de preços
(✓) SEÇÃO II. Termo de Referência do objeto da licitação
(✓) SEÇÃO III. Orçamento estimado em planilha
(✓) SEÇÃO IV. Modelo de Descrição da Proposta
(✓) 1 - Modelo de descrição da proposta de preços

(✓) SEÇÃO V. Modelo de declaração de elaboração independente de proposta e de inexistência de impedimento à participação no certame
(✓) SEÇÃO VI. Modelo de procuração
(✓) SEÇÃO VII. Modelo de declaração de enquadramento (Lei Complementar nº 123/06) **[NOTA: exclusiva para microempresa e empresa de pequeno porte]**
(✓) SEÇÃO VIII. Modelo de declaração de pleno conhecimento e de veracidade dos documentos **[NOTA: assinalar apenas na modalidade pregão]**

PARTE II – HABILITAÇÃO

(✓) SEÇÃO I. Documentos de Habilitação
(✓) SEÇÃO II. Certificado de Registro Cadastral CRC/CRS
(✓) SEÇÃO III. Modelos de Prova de Qualificação Técnica
(✓) Comprovação de Aptidão para o Desempenho

(✓) Indicação das Instalações, do Aparelhamento e do Pessoal Técnico

(✓) Declaração de Ciência dos Requisitos Técnicos (Visita técnica)

(✓) SEÇÃO IV. Modelo de Declaração de Proteção ao Trabalho do Menor
(✓) SEÇÃO V. Modelo de declaração quanto à regularidade fiscal e trabalhista (Lei Complementar nº 123/06) **[NOTA: exclusiva para microempresa e empresa de pequeno porte]**

PARTE III – CRITÉRIOS ESPECÍFICOS

(✓) SEÇÃO I. Amostras/demonstração de compatibilidade
(✓) Não

(✓) SEÇÃO II. Participação de empresas reunidas em consórcio
(✓) Não

(✓) SEÇÃO III. Participação de cooperativas
(✓) Não

(✓) SEÇÃO IV. Avaliação das propostas técnicas
(✓) Não se aplica

(✓) SEÇÃO V. Reserva de cota para microempresas e empresas de pequeno porte
(✓) Não se aplica

(✓) SEÇÃO VI. Adesão posterior à ata de registro de preços (carona)
(✓) Sim

(✓) SEÇÃO VII. Da Lei Geral de Proteção de Dados- LGPD
(✓) Informações da LGPD.

PARTE IV – CONTRATO

(✓) Minuta do contrato

PARTE V – ATA DE REGISTRO DE PREÇOS

(✓) Minuta da Ata de Registro de Preços

PARTE FIXA- RITO DO PROCEDIMENTO LICITATÓRIO E CONTRATAÇÃO

(✓) Título I – Dos Princípios
(✓) Título II – Dos Impedimentos
(✓) Título III- Das Propostas e dos Documentos de Habilitação
(✓) Título IV – Do Procedimento na Licitação
(✓) Título V – Das Impugnações
(✓) Título VI – Das Disposições Finais
(✓) Título VII – Da Revogação e Anulação
(✓) Título VIII - Da Contratação
(✓) Título IX – Das Penalidades
(✓) Título X – Do Foro

15. Informações e esclarecimentos adicionais

As informações e esclarecimentos necessários ao perfeito conhecimento do objeto desta licitação poderão ser obtidos no portal www.defensoria.ba.def.br, www.licitacoes-e.com.br ou solicitados ao responsável pela expedição do instrumento convocatório.

16. Responsável pela expedição do convocatório e meio de contato:

Servidor responsável e portaria de designação: Laurindo Grilo Matos (Portaria DPE/BA n° 596/2021)

Endereço: Avenida. Ulisses Guimarães, 3386, Sussuarana, Edf. MultiCab Empresarial, 3° andar, Salvador-Bahia. CEP 41.219-400.

Horário: 08:00 às 17:00 hs (segunda quinta-feira) e sexta-feira (08:00 às 14:00)

Tel.: (71) 3117-9075

E-mail: copel@defensoria.ba.def.br

Salvador (BA), em 16 de junho de 2023.

Laurindo Grilo Matos/86955456655

Defensoria Pública
BAHIA

PARTE I – PROPOSTAS

SEÇÃO I
ESPECIFICAÇÕES PARA ELABORAÇÃO DA PROPOSTA DE PREÇOS

1. A proposta de preços terá validade mínima de 60 (sessenta) dias a contar da data fixada neste instrumento para início da sessão pública, ainda que a licitante estipule prazo menor ou que não a consigne.

1.1 Será considerada não escrita a fixação de prazo de validade inferior ao mínimo, ficando facultado às licitantes ampliá-lo.

2. O prazo de entrega ou de execução do objeto será o fixado no Termo de Referência, ainda que a licitante, em sua proposta, consigne prazo maior ou que não o estipule.

2.1 Será considerada não escrita a fixação de prazo de entrega ou de execução superior ao estabelecido no Termo de Referência, ficando facultado às licitantes reduzi-lo.

3. O prazo de garantia técnica será o fixado no Termo de Referência, ainda que a licitante, em sua proposta, consigne prazo menor ou que não o estipule.

3.1 Será considerada não escrita a fixação de prazo de garantia técnica inferior ao estabelecido no Termo de Referência, ficando facultado às licitantes ampliá-lo.

4. O proponente deverá elaborar a sua proposta escrita de preços de acordo com as exigências constantes do Termo de Referência, em consonância com o modelo proposto neste convocatório, expressando os valores em moeda nacional – reais e centavos, em 02 (duas) casas decimais, ficando esclarecido que não serão admitidas propostas alternativas.

5. No valor da proposta deverão estar contempladas todas e quaisquer despesas necessárias ao fiel cumprimento do objeto desta licitação, inclusive todos os custos com material de consumo, salários, encargos sociais, previdenciários e trabalhistas de todo o pessoal da Contratada, como também fardamento, transporte de qualquer natureza, materiais empregados, inclusive ferramentas, utensílios e equipamentos utilizados, depreciação, aluguéis, administração, tributos, impostos, taxas, emolumentos e quaisquer outros custos que, direta ou indiretamente, se relacionem com o fiel cumprimento pela Contratada das obrigações.

5.1. Quaisquer tributos, custos e despesas diretos e indiretos omitidos da proposta ou incorretamente cotados, serão considerados como inclusos nos preços, não sendo considerados pleitos de acréscimos ou pedido de revisões, em nenhuma hipótese.

6. Precedentemente à elaboração da proposta, a licitante deverá observar as cláusulas e disposições deste edital, de seus apensos e anexos, especialmente as constantes do instrumento de contrato e as informações e condições locais para o cumprimento das obrigações objeto da licitação, não podendo alegar desconhecimento supervenientemente.

[NOTA: Pregão eletrônico]

7. As microempresas e empresas de pequeno porte que desejarem os benefícios da Lei Complementar nº 123/06 deverão obter esta qualificação junto ao sistema *licitacoes-e* do Banco do Brasil, comprometendo-se a remeter ao órgão licitante, por ocasião da habilitação, a Declaração de Enquadramento (PARTE I – PROPOSTAS/SEÇÃO VII), sob pena de não obter a concessão do tratamento diferenciado.

SEÇÃO II
TERMO DE REFERÊNCIA DO OBJETO DA LICITAÇÃO

1. OBJETO

Registro de preço, para eventual aquisição de soluções de Segurança da Informação com o propósito de ampliar a segurança da rede da DPE/BA, incluindo repasse de conhecimento, manutenção e suporte técnico por 60 (sessenta) meses de acordo com as condições e especificações constantes neste Termo de Referência.

2. MOTIVAÇÃO

A realidade na qual a Defensoria Pública está inserida traz consigo a absoluta necessidade do uso daqueles recursos que a tecnologia da informação e comunicação (TIC) tornou disponíveis ao longo dos anos. Nessa conjuntura, a informação é um dos principais ativos das instituições públicas, tratando-se de um elemento fundamental para a tomada de decisões em todos os níveis, sendo determinante para a gestão.

Os constantes ataques cibernéticos, a necessidade de continuidade do negócio e a evolução de ameaças das mais variadas espécies criam a necessidade de contratação de uma solução que proteja as informações da instituição e diminua os riscos de acesso indevido às mesmas.

Assim, o firewall representa um quesito de segurança fundamental, uma vez que regula o tráfego de dados entre redes distintas e impede a transmissão e recepção de informações a partir de acessos nocivos ou não autorizados na rede. Além disso, um firewall de rede pode ajudar a garantir o cumprimento das regulamentações de segurança cibernética, como a Lei Geral de Proteção de Dados (LGPD), que exige que as organizações protejam os dados pessoais dos usuários.

Portanto, a contratação em tela visa expandir para as unidades da Defensoria Pública da capital e regionais, a segurança já existente na sede administrativa do CAB, garantindo a proteção de acessos à rede LAN (interna) e WAN (externa), no intuito de prover a confidencialidade, integridade e disponibilidade dos dados transmitidos ou armazenados na infraestrutura de rede da Defensoria Pública, bem como gerenciar os riscos e ameaças aos ativos de tecnologia da informação dessa instituição.

Além disto, por meio desta aquisição, será possível gerenciar e proteger todo tráfego de rede da DPE/BA, nos fornecendo visibilidade sobre as demandas transacionais e nos permitindo aplicar políticas a partir de um local central, diminuindo o tempo investido em tarefas administrativas e operacionais; ampliar e aperfeiçoar o acesso à internet sem fio (wireless), provendo conectividade de rede segura para dispositivos móveis, como notebooks e smartphones, cujo uso é extremamente generalizado na sociedade contemporânea e por consequência, na comunidade de usuários da Defensoria Pública; e proteger as aplicações web, a exemplo do SIGAD, contra ameaças cibernéticas, como ataques de injeção SQL, cross-site scripting (XSS) e outros ataques de aplicativos da web.

3. RESUMO DO OBJETO DA CONTRATAÇÃO

LOTE ÚNICO – (EQUIPAMENTOS PARA SEGURANÇA DA INFORMAÇÃO)		
ITEM	**DESCRIÇÃO**	**QUANTIDADE**
1	SOLUÇÃO DE SEGURANÇA E GERENCIA DE REDES NGFW EM CLUSTER – TIPO 1	01
2	SOLUÇÃO DE SEGURANÇA E GERENCIA DE REDES NGFW – TIPO 2	03
3	SOLUÇÃO DE SEGURANÇA E GERENCIA DE REDES NGFW – TIPO 3	13

4	UNIDADE CENTRALIZADA DE ARMAZENAMENTO DE LOGS E RELATORIA	01
5	UNIDADE DE GERÊNCIA CENTRALIZADA DE EQUIPAMENTOS	01
6	ATIVOS DE REDE WIRELESS INDOOR	80
7	SOLUÇÃO DE SEGURANÇA, FIREWALL DE APLICAÇÕES WEB, DORAVANTE DENOMINADO SOLUÇÃO WAF, COM SUPORTE, GARANTIA E ATUALIZAÇÕES	01
8	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO PARA SOLUÇÃO DE SEGURANÇA E GERÊNCIA DE REDES NGFW EM CLUSTER DE ALTA DISPONIBILIDADE	01
9	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO PARA SOLUÇÃO DE SEGURANÇA E GERENCIA DE REDES NGFW TIPOS "2" E "3"	16
10	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO DE UNIDADE CENTRALIZADA DE ARMAZENAMENTO DE LOGS E RELATORIA	01
11	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO DE UNIDADE DE GERENCIA CENTRALIZADA DE EQUIPAMENTOS.	01
12	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO DOS ATIVOS DE REDE WIRELESS INDOOR	80
13	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO DE SEGURANÇA WAF	01

4. ESPECIFICAÇÕES TÉCNICAS

4.1. SOLUÇÃO DE SEGURANÇA E GERÊNCIA DE REDES NGFW EM CLUSTER – TIPO 1

- CARACTERÍSTICAS E FUNCIONALIDADES GERAIS -

4.1.1. Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.

4.1.2. Poderá ser entregue em equipamento único ou com composição de equipamentos.

4.1.3. A Solução de Segurança e Gerência de Redes NGFW em Cluster de Alta Disponibilidade, deve ser composto por no mínimo 02(dois) equipamento ambos licenciados para operar em modo ATIVO-ATIVO.

4.1.4. Deverá possuir e estar licenciados com as funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, DLP – Data Leak Prevention, Controladora Wireless e Virtualização, pelo período de 60 (sessenta) meses.

4.1.5. Deverá possuir fonte de alimentação redundante com chaveamento automático com capacidade para operar em tensões de 110V e 220V.

4.1.6. Firewall com capacidade mínima de processamento de 9 (nove) Gbps.

4.1.7. IPS com capacidade mínima de processamento de 2 (dois) Gbps.

4.1.8. Proteção contra Ameaças Avançadas (Threat Protection) com capacidade mínima de processamento de 900 (novecentos) Mbps. Proteção contra Ameaças Avançadas contempla as funções de Firewall, IPS, Controle de Aplicação e Proteção contra Malware/Vírus ativadas em conjunto.

4.1.9. Inspeção SSL Throughput com capacidade mínima de processamento de 1 (um) Gbps.

4.1.10 VPN com capacidade de, pelo menos, 10 (dez) Gbps de tráfego IPSec.

4.1.13 Deverá suportar, pelo menos, 50.000 (cinquenta mil) novas conexões por segundo.

4.1.14 Deverão ser licenciados para suportar, pelo menos, 400 (quatrocentos) usuários de VPN SSL.

4.1.15 Deverá suportar, pelo menos, 1.000 (um mil) túneis de VPN Site-Site.

4.1.16 Deverá suportar, pelo menos, 10.000 (dez mil) túneis de VPN Client-Site.

4.1.17 Deverá possuir pelo menos 16 (dezesseis) interfaces RJ 45 01 GE.

4.1.18 Deverá possuir pelo menos 6 (seis) interfaces SFP 01GE.

4.1.19 Deverá possuir pelo menos 2 (duas) interfaces SFP+ 10GE.

4.1.20 Deverá ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 60 (sessenta) Pontos de Acesso sem fio.

4.1.21 Deverá ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 30 (trinta) equipamentos.

4.1.22 Deverá ser compatível e integrável com o ITEM 4 deste Termo de Referência.

4.1.23 Deverá ser compatível e integrável com o ITEM 5 deste Termo de Referência.

4.1.24 Deverá ser fornecida toda documentação técnica, bem como manual de utilização, em português do Brasil ou em inglês.

- FUNCIONALIDADES DE FIREWALL

4.1.25 Deverá possuir controle de acesso à internet por endereço IP de origem e destino;

4.1.26 Deverá possuir controle de acesso à internet por subrede;

4.1.27 Deverá suportar tags de VLAN (802.1q);

4.1.28 Deverá possuir ferramenta de diagnóstico do tipo tcpdump;

4.1.29 Deverá possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;

4.1.30 Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;

4.1.31 Deverá suportar single-sign-on para Active Directory, Novell eDirectory, Citrix e RADIUS;

4.1.32 Deverá possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

4.1.33 Deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, vários para um, NAT64, NAT46, PAT, STUN e Full Cone NAT;

4.1.34 Deverá permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;

4.1.34 Deverá permitir controle de acesso à internet por domínio, por exemplo: gov.br, org.br, edu.br;

4.1.35 Deverá possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;

4.1.36 Deverá suportar roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGPv4;

4.1.37 Deverá suportar roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGPv4;

4.1.38 Deverá possuir funcionalidades de DHCP Cliente, Servidor e Relay;

4.1.39 Deverá suportar aplicações multimídia, como: H.323 e SIP;

4.1.40 Deverá possuir tecnologia de firewall do tipo Statefull;

4.1.41 Deverá suportar alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;

4.1.42 Deverá permitir o funcionamento em modo transparente tipo "bridge" sem alterar o endereço MAC do tráfego;

4.1.43 Deverá suportar PBR – Policy Based Routing;

4.1.44 Deverá permitir a criação de VLANS no padrão IEEE 802.1q;

4.1.45 Deverá possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);

4.1.46 Deverá permitir filtro de pacotes sem controle de estado (stateless) para verificação em camada 2;

4.1.47 Deverá permitir forwarding de camada 2 para protocolos não IP;

4.1.48 Deverá suportar forwarding multicast;

4.1.49 Deverá suportar roteamento multicast PIM Sparse Mode e Dense Mode;

4.1.50 Deverá permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos: TCP, UDP, ICMP e IP;

4.1.51 Deverá permitir o agrupamento de serviços;

4.1.52 Deverá permitir o filtro de pacotes sem a utilização de NAT;

4.1.53 Deverá permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;

4.1.54 Deverá possuir mecanismo de anti-spoofing;

4.1.55 Deverá permitir criação de regras definidas pelo usuário;

4.1.56 Deverá permitir o serviço de autenticação para tráfego HTTP e FTP;

4.1.57 Deverá permitir IP/MAC binding, permitindo que cada endereço IP possa ser associado a um endereço MAC, gerando maior controle dos endereços internos e impedindo o IP spoofing;

4.1.58 Deverá possuir a funcionalidade de balanceamento e contingência de links;

4.1.59 Deverá suportar sFlow;

4.1.60 O dispositivo deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas;

4.1.61 Deverá ter a capacidade de criar e aplicar políticas de reputação de cliente para registrar e pontuar as seguintes atividades: tentativas de conexões más, pacotes bloqueados por política, detecção de ataques de intrusão, detecção de ataques de malware, atividades Web em categorias de risco, proteção de aplicação, locais geográficos que os clientes estão tentando se comunicar;

4.1.62 Deverá permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;

4.1.63 Deverá permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, horário, protocolo e aplicação;

4.1.64 Deverá suportar certificados X.509, SCEP, Certificate Signing Request (CSR) e OCSP;

4.1.65 Deverá permitir funcionamento em modo bridge, router, proxy explícito, sniffer e/ou VLAN-tagged;

4.1.66 Deverá possuir mecanismo de tratamento (session-helpers ou ALGs) para os protocolos ou aplicações dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS;

4.1.67 Deverá suportar SIP, H.323 e SCCP NAT Traversal;

4.1.68 Deverá permitir a criação de objetos e agrupamento de objetos de usuários, redes, FQDN, protocolos e serviços para facilitar a criação de regras;

4.1.69 Deverá possuir porta de comunicação serial ou USB para testes e configuração do equipamento, com acesso protegido por usuário e senha;

- FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO -

4.1.70 Deverá permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;

4.1.71 Deverá permitir modificação de valores DSCP para o DiffServ;

4.1.72 Deverá permitir priorização de tráfego e suportar ToS;

4.1.73 Deverá limitar individualmente a banda utilizada por programas, tais como: peer- to-peer, streaming, chat, VoIP e Web;

4.1.74 Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

4.1.75 Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;

4.1.76 Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;

4.1.77 Deverá permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação;

4.1.78 Deverá controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino;

4.1.79 Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

- FUNCIONALIDADE DE ANTI-SPAM DE GATEWAY -

4.1.80 Deverá permitir, na funcionalidade de anti-spam, verificação do cabeçalho SMTP do tipo MIME;

4.1.81 Deverá possuir filtragem de e-mail por palavras chaves;

4.1.82 Deverá permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM;

4.1.83 Deverá possuir, para a funcionalidade de anti-spam, o recurso de RBL;

4.1.84 Deverá permitir a checagem de reputação da URL no corpo mensagem de correio eletrônico;

- FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB -

4.1.85 Deverá possuir solução de filtro de conteúdo Web integrado à solução de segurança;

4.1.86 Deverá possuir, pelo menos, 70 (setenta) categorias para classificação de sites Web;

4.1.87 Deverá possuir base mínima contendo 40.000.000 (quarenta milhões) de sites internet Web já registrados e classificados;

4.1.88 Deverá possuir a funcionalidade de cota de tempo de utilização por categoria;

4.1.89 Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como:

4.1.89.1 Proxy anônimo;

4.1.89.2 Webmail;

4.1.89.3 Instituições de saúde;

4.1.89.4 Notícias;

4.1.89.5 Phishing;
4.1.89.6 Hackers;
4.1.89.7 Pornografia;
4.1.89.8 Racismo;
4.1.89.9 Websites pessoais;
4.1.89.10 Compras;

4.1.90 Deverá permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;
4.1.91 Deverá permitir a criação de, pelo menos, 05 (cinco) categorias personalizadas;
4.1.92 Deverá permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP;
4.1.93 Deverá prover Termo de Responsabilidade on-line para aceite pelo usuário, a ser apresentado toda vez que houver tentativa de acesso a determinado serviço permitido ou bloqueado;
4.1.94 Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;
4.1.95 Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
4.1.96 Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;
4.1.97 Deverá exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança;
4.1.98 Deverá permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies e activeX, através de base de URL própria atualizável;
4.1.99 Deverá permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual;
4.1.100 Deverá permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra);
4.1.101 Deverá permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido;
4.1.102 Deverá filtrar o conteúdo baseado em categorias em tempo real;
4.1.103 Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web;
4.1.104 Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;
4.1.105 Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
4.1.106 Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem;
4.1.107 Deverá ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP;
4.1.108 Deverá permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams;
4.1.109 Deverá possuir Proxy Explícito e Transparente;
4.1.110 Deverá implementar roteamento WCCP e ICAP;

- FUNCIONALIDADE DE DETECÇÃO DE INTRUSÃO -

4.1.111 Deverá permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;
4.1.112 Deverá possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas;
4.1.113 Deverá estar orientado à proteção de redes;
4.1.114 Deverá permitir funcionar em modo transparente, sniffer e router;
4.1.115 Deverá possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;
4.1.116 Deverá permitir a criação de padrões de ataque manualmente;
4.1.117 Deverá possuir integração à plataforma de segurança;
4.1.118 Deverá possuir capacidade de remontagem de pacotes para identificação de ataques;
4.1.119 Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web;
4.1.120 Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
4.1.121 Deverá possuir mecanismos de detecção/proteção de ataques;

4.1.122 Deverá possuir reconhecimento de padrões;

4.1.123 Deverá possuir análise de protocolos;

4.1.124 Deverá possuir detecção de anomalias;

4.1.125 Deverá possuir detecção de ataques de RPC (Remote Procedure Call);

4.1.126 Deverá possuir proteção contra-ataques de Windows ou NetBios;

4.1.127 Deverá possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol);

4.1.128 Deverá possuir proteção contra-ataques DNS (Domain Name System);

4.1.129 Deverá possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin;

4.1.130 Deverá possuir proteção contra-ataques de ICMP (Internet Control Message Protocol);

4.1.131 Deverá possuir métodos de notificação de detecção de ataques;

4.1.132 Deverá possuir alarmes na console de administração;

4.1.133 Deverá possuir alertas via correio eletrônico;

4.1.134 Deverá possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;

4.1.135 Deverá ter a capacidade de resposta/logs ativa a ataques;

4.1.136 Deverá prover a terminação de sessões via TCP resets;

4.1.137 Deverá armazenar os logs de sessões;

4.1.138 Deverá atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;

4.1.139 Deverá mitigar os efeitos dos ataques de negação de serviços;

4.1.140 Deverá permitir a criação de assinaturas personalizadas;

4.1.141 Deverá possuir filtros de ataques por anomalias;

4.1.142 Deverá permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destinationsessionlimit;

4.1.143 Deverá permitir filtros de anomalias de protocolos;

4.1.144 Deverá suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;

4.1.145 Deverá suportar verificação de ataque na camada de aplicação;

4.1.146 Deverá suportar verificação de tráfego em tempo real, via aceleração de hardware;

4.1.147 Deverá possuir as seguintes estratégias de bloqueio: pass, drop e reset.

- FUNCIONALIDADE DE VPN -

4.1.148 Deverá possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;

4.1.149 Deverá possuir suporte a certificados PKI X.509 para construção de VPNs;

4.1.150 Deverá possuir suporte a VPNs IPSeC Site-to-Site e VPNs IPSec Client-to-Site;

4.1.151 Deverá possuir suporte a VPN SSL;

4.1.152 Deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais;

4.1.153 A VPN SSL deverá possibilitar o acesso à rede, de acordo com a política de segurança, através do acesso via navegador WEB;

4.1.154 Deverá possuir hardware acelerador criptográfico para incrementar o desempenho da VPN;

4.1.155 A VPN SSL deverá suportar cliente para plataforma Windows, Linux e Mac OS X;

4.1.156 Deverá permitir a arquitetura de VPN hub and spoke;

4.1.157 Deverá possuir suporte à inclusão em autoridades certificadoras (enrollment), mediante SCEP (Simple Certificate Enrollment Protocol) e mediante arquivos.

- FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES -

4.1.158 Deverá reconhecer, no mínimo, 2.000 (duas mil) aplicações;

4.1.159 Deverá possuir, pelo menos, 10 (dez) categorias para classificação de aplicações;

4.1.160 Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como:

- **4.1.160.1** P2P;
- **4.1.160.2** Instant Messaging;
- **4.1.160.3** Web-Client;
- **4.1.160.4** Transferência de arquivos;

4.1.160.5 VoIP;

4.1.161 Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;

4.1.162 Deverá ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma;

4.1.163 Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

4.1.164 Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

4.1.165 Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;

4.1.166 Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;

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

4.1.168 Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;

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

4.1.170 Deverá permitir a inspeção/bloqueio de códigos maliciosos para, no mínimo, as seguintes categorias: Instant Messaging e transferência de arquivos;

4.1.171 Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações;

4.1.172 Deverá permitir criação de padrões de aplicação manualmente;

- FUNCIONALIDADE DE DLP (DATA LEAK PREVENTION) -

4.1.173 O sistema de DLP (Data Leak Prevention – Proteção contra Vazamento de Informações) de gateway deverá funcionar de maneira que se consiga que os dados sensíveis não saiam da rede e também deverá funcionar de modo que se previna que dados não requisitados entrem na sua rede;

4.1.174 Deverá inspecionar, no mínimo, os tráfegos de e-mail e HTTP;

4.1.175 Sobre o tráfego de e-mail, deverá inspecionar, no mínimo, os protocolos SMTP, POP3 e IMAP;

4.1.176 Deverá realizar buscas para a aplicação de regras de DLP em arquivos do tipo PDF e MS-Word;

4.1.177 Deverá aplicar regras baseadas em usuários autenticados, isto é, fazendo buscas pelo tráfego de um específico usuário;

4.1.178 Deverá verificar para aplicações do tipo e-mail, se o anexo das mensagens de correio entrantes/saintes possui um tamanho máximo especificado pelo administrador;

4.1.179 Deverá utilizar expressões regulares para composição das regras de verificação dos tráfegos;

4.1.180 Deverá tomar minimamente as ações de bloquear ou colocar o IP em quarentena;

4.1.181 Deverá permitir o armazenamento em solução específica de armazenamento de logs, o conteúdo do tráfego que coincidir com o tráfego esperado pela regra de DLP para minimamente os protocolos de e-mail e HTTP;

4.1.182 Deverá permitir a composição de múltiplas regras de DLP, formando uma regra única mais específica que usa lógica booleana para fazer a comparação com o tráfego que atravessa o sistema.

- FUNCIONALIDADE DE BALANCEAMENTO DE CARGA -

4.1.183 Deverá permitir a criação de endereços IPs virtuais;

4.1.184 Deverá permitir balanceamento de carga entre, pelo menos, 04 (quatro) servidores reais;

4.1.185 Deverá suportar balanceamento, ao menos, para os seguintes serviços: HTTP, HTTPS, TCP e UDP;

4.1.186 Deverá permitir balanceamento, ao menos, com os seguintes métodos: Hash do endereço IP de origem, Round Robin, Weighted, First Alive e HTTP host;

4.1.187 Deverá permitir persistência de sessão por cookie HTTP ou SSL session ID;

4.1.188 Deverá permitir que seja mantido o IP de origem;

4.1.189 Deverá suportar SSL offloading nos equipamentos que suportem, pelo menos, 200 (duzentos) usuários;

4.1.190 Deverá ter a capacidade de identificar, através de health checks, quais os servidores que estejam ativos, removendo automaticamente o tráfego dos servidores que não estejam;

4.1.191 Deverá permitir que o health check seja feito, ao menos, via ICMP, TCP em porta configurável e HTTP.

- FUNCIONALIDADE DE VIRTUALIZAÇÃO -

4.1.192 Deverá suportar a criação de, ao menos, 10 (dez) instâncias virtuais no mesmo hardware;

4.1.193 Deverá permitir a criação de administradores independentes para cada uma das instâncias virtuais;

4.1.194 Deverá permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas

- FUNCIONALIDADE DE CONTROLADORA WIRELESS -

4.1.195 Deverá ser capaz de gerenciar, de forma centralizada, outros Pontos de Acesso do mesmo fabricante;

4.1.196 Deverá suportar o serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless;

4.1.197 Deverá suportar monitoração e supressão de Ponto de Acesso indevido;

4.1.198 Deverá prover autenticação para a rede wireless através de bases externas, como: LDAP, RADIUS ou TACACS+;

4.1.199 Deverá permitir a visualização dos clientes conectados;

4.1.200 Deverá prover suporte a Fast Roaming;

4.1.201 Deverá ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF;

4.1.202 A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;

4.1.203 Deverá possuir Captive Portal por SSID;

4.1.204 Deverá permitir configurar o bloqueio de tráfego entre SSIDs;

4.1.205 Deverá suportar Wi-Fi Protected Access (WPA), WPA2 ou WPA3 por SSID, utilizando-se de AES e/ou TKIP;

4.1.206 Deverá suportar os seguintes métodos de autenticação EAP:

- **4.1.206.1** EAP-TLS
- **4.1.206.2** EAP-TTLS;
- **4.1.206.3** EAP-PEAP;
- **4.1.206.4** EAP-SIM
- **4.1.206.5** EAP-AKA;

4.1.207 Deverá suportar 802.1x através de RADIUS;

4.1.208 Deverá suportar filtro baseado em endereço MAC por SSID;

4.1.209 Deverá permitir configurar parâmetros de rádio, como: banda e canal;

4.1.210 Deverá possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast;

4.1.211 Deverá possuir mecanismo de identificação e controle de Rogue APs, suportando supressão automática e bloqueio por endereço MAC de Aps;

4.1.212 Deverá possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue)

4.1.213 Deverá possuir WIDS com, ao menos, os seguintes perfis:

- **4.1.213.1.** Rogue/Interfering AP Detection;
- **4.1.213.2.** Ad-hoc Network Detection;
- **4.1.213.3.** Wireless Bridge Detection;
- **4.1.213.4.** Weak WEP Detection;
- **4.1.213.5.** MAC OUI Checking;

4.1.214 A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;

4.1.215 A controladora deverá oferecer Firewall integrado, baseado em identidade do usuário;

4.1.216 Deverá possuir controle baseado em política de firewall para acesso entre as WLANs;

4.1.217 Deverá permitir a criação de políticas de traffic shaping;

4.1.218 Deverá permitir a criação de políticas de firewall baseadas em horário;

4.1.219 Deverá permitir NAT nas políticas de firewall;

4.1.220 Deverá possibilitar definir número de clientes por SSID;

4.1.221 Deverá permitir e/ou bloquear o tráfego entre SSIDs;

4.1.222 Deverá possuir mecanismo de criação automática de usuários visitantes e senhas auto-geradas e/ou manual, que possam ser enviadas por e-mail ou SMS aos usuários, e com capacidade de definição de horário da expiração da senha;

4.1.223 A comunicação entre o Access Point e a Controladora Wireless deverá poder ser efetuada de forma criptografada;

4.1.224 Deverá possuir mecanismo de ajuste de potência do sinal, de forma a reduzir interferência entre canais entre 02 (dois) Access Points gerenciados;

4.1.225 Deverá possuir mecanismo de balanceamento de tráfego/usuários entre Access Point

4.1.226 Deverá possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou rádios

4.1.227 Toda a configuração do Ponto de Acesso deverá ser executada através da Controladora Wireless;

4.1.228 Deverá permitir a identificação de APs com firmware desatualizado e efetuar o upgrade via interface gráfica;

4.1.229 Deverá possuir console de monitoramento dos usuários conectados, indicando em que Access Point, em que rádio, em que canal, endereço IP do usuário, tipo de dispositivo e sistema operacional, uso de banda, potência do sinal e relação sinal/ruído;

4.1.230 O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser encaminhados dentro do túnel até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional do próprio fabricante para suportar a conexão dos túneis originados dos pontos de acesso;

4.1.231 A Controladora deverá oferecer Firewall integrado, baseado em identidade do usuário, entre todas as redes cujo tráfego seja tunelado até a Controladora;

4.1.232 Deverá possuir controle baseado em política de firewall para acesso entre as WLANs cujo tráfego seja tunelado até a Controladora;

4.1.233 Deverá permitir a criação de políticas de traffic shaping entre todas as redes cujo tráfego seja tunelado até a Controladora;

4.1.234 Deverá permitir aplicar políticas de filtro de conteúdo Web, que seja baseado em categorias de sites automaticamente atualizadas, para todas as redes cujo tráfego seja tunelado até a Controladora;

4.1.235 Deverá permitir aplicar políticas de antivírus, com detecção e bloqueio de malwares e redes botnet, entre todas as redes cujo tráfego seja tunelado até a Controladora;

4.1.236 Deverá permitir aplicar políticas de IPS, bloqueando e/ou monitorando tentativas de ataques, com base de assinatura de ataques atualizada automaticamente, entre todas as redes cujo tráfego seja tunelado até a Controladora;

4.1.237 Deverá permitir aplicar políticas de controle antispam para todas as redes cujo tráfego seja tunelado até a Controladora;

4.1.238 Deverá permitir controlar, identificar e bloquear tráfego de aplicações do tipo P2P, IM, Chat, Redes Sociais, Skype, Proxies Anônimos, streamings de áudio e vídeo, jogos entre outros, e que seja baseado no padrão de comunicação de tais aplicações, entre todas as redes cujo tráfego seja tunelado até a Controladora;

4.1.239 Deverá possuir as seguintes certificações:

4.1.239.1 Certificação Wi-Fi Alliance;
4.1.239.2. Certificação ICSA para Firewall;
4.1.239.3. Certificação ICSA para Antivírus;
4.1.239.4. Certificação ICSA para VPN SSL;
4.1.239.5. Certificação ICSA para VPN IPSec;
4.1.239.6. Certificação ICSA para IPS;

- FUNCIONALIDADE DE SD-WAN

4.1.240 A solução SD-WAN deve ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.

4.1.241 A solução SD-WAN deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos.

4.1.242 A solução SD-WAN deve suportar segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN.

4.1.243 A solução SD-WAN deve prover capacidade de inspeção SSL para a inspeção de tráfego https nas filiais, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações.

4.1.244 Solução deve ser capaz de prover Zero Touch provisioning.

4.1.245 A solução de Zero Touch provisioning deve ser capaz de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN.

4.1.246 Solução deve ser capaz de prover uma arquitetura onde em uma comunicação Matriz x Filiais, em que a comunicação de uma Filial A para a Matriz esteja comprometida, possa ser utilizada a comunicação entre Filial B e Matriz, em que através deste circuito, a Filial A alcance a Matriz.

4.1.247 A solução deve ser capaz de criar VPN "Full-Mesh", de forma automática, e sem que o administrador precise configurar site por site.

4.1.248 Reconhecimento em camada 7 totalmente segregado da camada 4.

4.1.249 Deve de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação à

um determinado IP/ range de IPs de destino.

4.1.250 O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;

4.1.251 Ainda sobre o reconhecimento de Aplicações, a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook, etc);

4.1.252 A solução de SD-WAN deve suportar Roteamento dinâmico BGP com suporte a IPv6 ;

4.1.253 A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições onde a largura de banda é modificada.

4.1.254 A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN.

4.1.255 A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link principal recuperado seja X% (com X variando de 10 à 50) do seu valor de Saúde melhor que o link atual.

4.1.256 A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema.

4.1.257 A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN.

4.2. SOLUÇÃO DE SEGURANÇA E GERÊNCIA DE REDES NGFW TIPO 2

4.2.1. Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.

4.2.2. Poderá ser entregue em equipamento único ou com composição de equipamentos.

4.2.3. Deverá possuir e estar licenciados com as funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, DLP – Data Leak Prevention, Controladora Wireless e Virtualização, pelo período de 60 (sessenta) meses.

4.2.4. Deverá possuir fonte de alimentação redundante com chaveamento automático com capacidade para operar em tensões de 110V e 220V.

4.2.5. Firewall com capacidade mínima de processamento de 6 (seis) Gbps.

4.2.6. IPS com capacidade mínima de processamento de 1 (um) Gbps.

4.2.7. Proteção contra Ameaças Avançadas (Threat Protection) com capacidade mínima de processamento de 800 (oitocentos) Mbps. Proteção contra Ameaças Avançadas contempla as funções de Firewall, IPS, Controle de Aplicação e Proteção contra Malware/Vírus ativadas em conjunto

4.2.8. Inspeção SSL Throughput com capacidade mínima de processamento de 700 (setecentos) Mbps.

4.2.9. VPN com capacidade de, pelo menos, 6 (seis) Gbps de tráfego IPSec.

4.2.10 VPN SSL com capacidade de, pelo menos, 900 (novecentos) Mbps de tráfego.

4.2.11 Deverá suportar 1 (um) Milhão conexões simultâneas

4.2.12 Deverá suportar, pelo menos, 40.000 (quarenta mil) novas conexões por segundo.

4.2.13 Deverão ser licenciados para suportar, pelo menos, 100 (cem) usuários de VPN SSL.

4.2.14 Deverá suportar, pelo menos, 100 (cem) túneis de VPN Site-Site.

4.2.15 Deverá suportar, pelo menos, 1.000 (mil) túneis de VPN Client-Site.

4.2.16 Deverá possuir pelo menos 6 (seis) interfaces RJ45 01GE.

4.2.17 Deverá possuir pelo menos 2 (duas) interfaces SFP 01GE.

4.2.18 Deverá ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 40 (quarenta) Pontos de Acesso sem fio.

4.2.19 Deverá ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 15 (quinze) equipamentos.

4.2.20 Deverá ser compatível e integrável com o ITEM 4 deste Termo de Referência.

4.2.21 Deverá ser compatível e integrável com o ITEM 5 deste Termo de Referência.

4.2.22 Deverá ser fornecida toda documentação técnica, bem como manual de utilização, em português do Brasil ou em inglês.

- FUNCIONALIDADES DE FIREWALL -

4.2.23 Deverá possuir controle de acesso à internet por endereço IP de origem e destino;

4.2.24 Deverá possuir controle de acesso à internet por subrede;

4.2.25 Deverá suportar tags de VLAN (802.1q);

4.2.26 Deverá possuir ferramenta de diagnóstico do tipo tcpdump;

4.2.27 Deverá possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;

4.2.28 Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;

4.2.29 Deverá suportar single-sign-on para Active Directory, Novell eDirectory, Citrix e RADIUS;

4.2.30 Deverá possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

4.2.31 Deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, vários para um, NAT64, NAT46, PAT, STUN e Full Cone NAT;

4.2.32 Deverá permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;

4.2.33 Deverá permitir controle de acesso à internet por domínio, por exemplo: gov.br, org.br, edu.br;

4.2.34 Deverá possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;

4.2.35 Deverá suportar roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGPv4;

4.2.36 Deverá possuir funcionalidades de DHCP Cliente, Servidor e Relay;

4.2.37 Deverá suportar aplicações multimídia, como: H.323 e SIP;

4.2.38 Deverá possuir tecnologia de firewall do tipo Statefull;

4.2.39 Deverá suportar alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;

4.2.40 Deverá permitir o funcionamento em modo transparente tipo "bridge" sem alterar o endereço MAC do tráfego;

4.2.41 Deverá suportar PBR – Policy Based Routing;

4.2.42 Deverá permitir a criação de VLANS no padrão IEEE 802.1q;

4.2.43 Deverá possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);

4.2.44 Deverá permitir filtro de pacotes sem controle de estado (stateless) para verificação em camada 2;

4.2.45 Deverá permitir forwarding de camada 2 para protocolos não IP;

4.2.46 Deverá suportar forwarding multicast;

4.2.47 Deverá suportar roteamento multicast PIM Sparse Mode e Dense Mode;

4.2.48 Deverá permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos: TCP, UDP, ICMP e IP;

4.2.49 Deverá permitir o agrupamento de serviços;

4.2.50 Deverá permitir o filtro de pacotes sem a utilização de NAT;

4.2.51 Deverá permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;

4.2.52 Deverá possuir mecanismo de anti-spoofing;

4.2.53 Deverá permitir criação de regras definidas pelo usuário;

4.2.54 Deverá permitir o serviço de autenticação para tráfego HTTP e FTP;

4.2.55 Deverá permitir IP/MAC binding, permitindo que cada endereço IP possa ser associado a um endereço MAC, gerando maior controle dos endereços internos e impedindo o IP spoofing;

4.2.56 Deverá possuir a funcionalidade de balanceamento e contingência de links;

4.2.57 Deverá suportar sFlow;

4.2.58 O dispositivo deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas;

4.2.59 Deverá ter a capacidade de criar e aplicar políticas de reputação de cliente para registrar e pontuar as seguintes atividades: tentativas de conexões más, pacotes bloqueados por política, detecção de ataques de intrusão, detecção de ataques de malware, atividades Web em categorias de risco, proteção de aplicação, locais geográficos que os clientes estão tentando se comunicar;

4.2.60 Deverá permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;

4.2.61 Deverá permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, horário, protocolo e aplicação;

4.2.62 Deverá suportar certificados X.509, SCEP, Certificate Signing Request (CSR) e OCSP;

4.263 Deverá permitir funcionamento em modo bridge, router, proxy explícito, sniffer e/ou VLAN-tagged;

4.2.64 Deverá possuir mecanismo de tratamento (session-helpers ou ALGs) para os protocolos ou aplicações dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS;

4.2.65 Deverá suportar SIP, H.323 e SCCP NAT Traversal;

4.2.66 Deverá permitir a criação de objetos e agrupamento de objetos de usuários, redes, FQDN, protocolos e serviços para facilitar a criação de regras;

4.2.67 Deverá possuir porta de comunicação serial ou USB para testes e configuração do equipamento, com acesso protegido por usuário e senha.

- FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO -

4.2.68 Deverá permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;

4.2.69 Deverá permitir modificação de valores DSCP para o DiffServ;

4.2.70 Deverá permitir priorização de tráfego e suportar ToS;

4.2.71 Deverá limitar individualmente a banda utilizada por programas, tais como: peer- to-peer, streaming, chat, VoIP e Web;

4.2.72 Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

4.2.73 Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;

4.2.74 Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;

4.2.75 Deverá permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação;

4.2.76 Deverá controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino;

4.2.77 Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

- FUNCIONALIDADE DE ANTI-SPAM DE GATEWAY -

4.2.78 Deverá permitir, na funcionalidade de anti-spam, verificação do cabeçalho SMTP do tipo MIME;

4.2.79 Deverá possuir filtragem de e-mail por palavras chaves;

4.2.80 Deverá permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM;

4.2.81 Deverá possuir, para a funcionalidade de anti-spam, o recurso de RBL;

4.2.82 Deverá permitir a checagem de reputação da URL no corpo mensagem de correio eletrônico

- FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB -

4.2.83 Deverá possuir solução de filtro de conteúdo Web integrado à solução de segurança;

4.2.84 Deverá possuir, pelo menos, 70 (setenta) categorias para classificação de sites Web;

4.2.85 Deverá possuir base mínima contendo 40.000.000 (quarenta milhões) de sites internet Web já registrados e classificados;

4.2.86 Deverá possuir a funcionalidade de cota de tempo de utilização por categoria;

4.2.87 Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como:

- **4.2.87.1.** Proxy anônimo;
- **4.2.87.2.** Webmail;
- **4.2.87.3.** Instituições de saúde;
- **4.2.87.4.** Notícias;
- **4.2.87.5.** Phishing;
- **4.2.87.6.** Hackers;
- **4.2.87.7.** Pornografia;
- **4.2.87.8.** Racismo;
- **4.2.87.9.** Websites pessoais;
- **4.2.87.10** Compras;

4.2.88 Deverá permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

4.2.89 Deverá permitir a criação de, pelo menos, 05 (cinco) categorias personalizadas;

4.2.90 Deverá permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP;

4.2.91 Deverá prover Termo de Responsabilidade on-line para aceite pelo usuário, a ser apresentado toda vez que

houver tentativa de acesso a determinado serviço permitido ou bloqueado;

4.2.92 Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;

4.2.93 Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

4.2.94 Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;

4.2.95 Deverá exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança;

4.2.96 Deverá permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies e activeX, através de base de URL própria atualizável;

4.2.97 Deverá permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual;

4.2.98 Deverá permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra);

4.2.99 Deverá permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido;

4.2.100 Deverá filtrar o conteúdo baseado em categorias em tempo real;

4.2.101 Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web;

4.2.102 Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;

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

4.2.104 Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem;

4.2.105 Deverá ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP;

4.2.106 Deverá permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams;

4.2.107 Deverá possuir Proxy Explícito e Transparente;

4.2.108 Deverá implementar roteamento WCCP e ICAP;

- FUNCIONALIDADE DE DETECÇÃO DE INTRUSÃO -

4.2.109 Deverá permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;

4.2.110 Deverá possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas;

4.2.111 Deverá estar orientado à proteção de redes;

4.2.112 Deverá permitir funcionar em modo transparente, sniffer e router;

4.2.113 Deverá possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;

4.2.114 Deverá permitir a criação de padrões de ataque manualmente;

4.2.115 Deverá possuir integração à plataforma de segurança;

4.2.116 Deverá possuir capacidade de remontagem de pacotes para identificação de ataques;

4.2.117 Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web;

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

4.2.119 Deverá possuir mecanismos de detecção/proteção de ataques;

4.2.118 Deverá possuir reconhecimento de padrões;

4.2.121 Deverá possuir análise de protocolos;

4.2.122 Deverá possuir detecção de anomalias;

4.2.123 Deverá possuir detecção de ataques de RPC (Remote Procedure Call);

4.2.124 Deverá possuir proteção contra-ataques de Windows ou NetBios;

4.2.125 Deverá possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol);

4.2.126 Deverá possuir proteção contra-ataques DNS (Domain Name System);

4.2.127 Deverá possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin;

4.2.128 Deverá possuir proteção contra-ataques de ICMP (Internet Control Message Protocol);

4.2.129 Deverá possuir métodos de notificação de detecção de ataques;

4.2.130 Deverá possuir alarmes na console de administração;

4.2.131 Deverá possuir alertas via correio eletrônico;

4.2.132 Deverá possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;

4.2.133 Deverá ter a capacidade de resposta/logs ativa a ataques;

4.2.134 Deverá prover a terminação de sessões via TCP resets;

4.2.135 Deverá armazenar os logs de sessões;

4.2.136 Deverá atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;

4.2.137 Deverá mitigar os efeitos dos ataques de negação de serviços;

4.2.138 Deverá permitir a criação de assinaturas personalizadas;

4.2.139 Deverá possuir filtros de ataques por anomalias;

4.2.140 Deverá permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destinationsessionlimit;

4.2.141 Deverá permitir filtros de anomalias de protocolos;

4.2.142 Deverá suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;

4.2.143 Deverá suportar verificação de ataque na camada de aplicação;

4.2.144 Deverá suportar verificação de tráfego em tempo real, via aceleração de hardware;

4.2.145 Deverá possuir as seguintes estratégias de bloqueio: pass, drop e reset.

FUNCIONALIDADES DE VPN

4.2.146 Deverá possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;

4.2.147 Deverá possuir suporte a certificados PKI X.509 para construção de VPNs;

4.2.148 Deverá possuir suporte a VPNs IPSeC Site-to-Site e VPNs IPSec Client-to-Site;

4.2.149 Deverá possuir suporte a VPN SSL;

4.2.150 Deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais;

4.2.151 A VPN SSL deverá possibilitar o acesso à rede, de acordo com a política de segurança, através do acesso via navegador WEB;

4.2.152 Deverá possuir hardware acelerador criptográfico para incrementar o desempenho da VPN;

4.2.153 A VPN SSL deverá suportar cliente para plataforma Windows, Linux e Mac OS X;

4.2.154 Deverá permitir a arquitetura de VPN hub and spoke;

4.2.155 Deverá possuir suporte à inclusão em autoridades certificadoras (enrollment), mediante SCEP (Simple Certificate Enrollment Protocol) e mediante arquivos.

- FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES -

4.2.156 Deverá reconhecer, no mínimo, 2.000 (duas mil) aplicações;

4.2.157 Deverá possuir, pelo menos, 10 (dez) categorias para classificação de aplicações

4.2.158 Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como:

- **4.2.1.158.1** P2P;
- **4.2.1.158.2** Instant Messaging;
- **4.2.1.158.3** Web-Client;
- **4.2.1.158.4** Transferência de arquivos;
- **4.2.1.158.5** VoIP;

4.2.159 Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;

4.2.160 Deverá ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma;

4.2.161 Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

4.2.162 Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

4.2.163 Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;

4.2.164 Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;

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

4.2.166 Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;

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

4.2.168 Deverá permitir a inspeção/bloqueio de códigos maliciosos para, no mínimo, as seguintes categorias: Instant Messaging e transferência de arquivos;

4.2.169 Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações;

4.2.170 Deverá permitir criação de padrões de aplicação manualmente;

- FUNCIONALIDADE DE DLP (DATA LEAK PREVENTION)

4.2.171 O sistema de DLP (Data Leak Prevention – Proteção contra Vazamento de Informações) de gateway deverá funcionar de maneira que se consiga que os dados sensíveis não saiam da rede e também deverá funcionar de modo que se previna que dados não requisitados entrem na sua rede;

4.2.172 Deverá inspecionar, no mínimo, os tráfegos de e-mail e HTTP;

4.2.173 Sobre o tráfego de e-mail, deverá inspecionar, no mínimo, os protocolos SMTP, POP3 e IMAP;

4.2.174 Deverá realizar buscas para a aplicação de regras de DLP em arquivos do tipo PDF e MS-Word;

4.2.175 Deverá aplicar regras baseadas em usuários autenticados, isto é, fazendo buscas pelo tráfego de um específico usuário;

4.2.176 Deverá verificar para aplicações do tipo e-mail, se o anexo das mensagens de correio entrantes/saintes possui um tamanho máximo especificado pelo administrador;

4.2.177 Deverá utilizar expressões regulares para composição das regras de verificação dos tráfegos;

4.2.178 Deverá tomar minimamente as ações de bloquear ou colocar o IP em quarentena;

4.2.179 Deverá permitir o armazenamento em solução específica de armazenamento de logs, o conteúdo do tráfego que coincidir com o tráfego esperado pela regra de DLP para minimamente os protocolos de e-mail e HTTP;

4.2.180 Deverá permitir a composição de múltiplas regras de DLP, formando uma regra única mais específica que usa lógica booleana para fazer a comparação com o tráfego que atravessa o sistema.

- FUNCIONALIDADE DE BALANCEAMENTO DE CARGA -

4.2.181 Deverá permitir a criação de endereços IPs virtuais;

4.2.182 Deverá permitir balanceamento de carga entre, pelo menos, 04 (quatro) servidores reais;

4.2.183 Deverá suportar balanceamento, ao menos, para os seguintes serviços: HTTP, HTTPS, TCP e UDP;

4.2.184 Deverá permitir balanceamento, ao menos, com os seguintes métodos: Hash do endereço IP de origem, Round Robin, Weighted, First Alive e HTTP host;

4.2.185 Deverá permitir persistência de sessão por cookie HTTP ou SSL session ID;

4.2.186 Deverá permitir que seja mantido o IP de origem;

4.2.187 Deverá suportar SSL offloading nos equipamentos que suportem, pelo menos, 200 (duzentos) usuários;

4.2.188 Deverá ter a capacidade de identificar, através de health checks, quais os servidores que estejam ativos, removendo automaticamente o tráfego dos servidores que não estejam;

4.2.189 Deverá permitir que o health check seja feito, ao menos, via ICMP, TCP em porta configurável e HTTP.

- FUNCIONALIDADE DE VIRTUALIZAÇÃO -

4.2.190 Deverá suportar a criação de, ao menos, 10 (dez) instâncias virtuais no mesmo hardware;

4.2.191 Deverá permitir a criação de administradores independentes para cada uma das instâncias virtuais;

4.2.192 Deverá permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.

- FUNCIONALIDADE DE CONTROLADORA WIRELESS -

4.2.193 Deverá ser capaz de gerenciar, de forma centralizada, outros Pontos de Acesso do mesmo fabricante;

4.2.194 Deverá suportar o serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless;

4.2.195 Deverá suportar monitoração e supressão de Ponto de Acesso indevido;

4.2.196 Deverá prover autenticação para a rede wireless através de bases externas, como: LDAP, RADIUS ou TACACS+;

4.2.197 Deverá permitir a visualização dos clientes conectados;

4.2.198 Deverá prover suporte a Fast Roaming;

4.2.199 Deverá ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF;

4.2.200 A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;

4.2.201 Deverá possuir Captive Portal por SSID;

4.2.202 Deverá permitir configurar o bloqueio de tráfego entre SSIDs;

4.2.203 Deverá suportar Wi-Fi Protected Access (WPA), WPA2 ou WPA3 por SSID, utilizando-se de AES e/ou TKIP;

4.2.204 Deverá suportar os seguintes métodos de autenticação EAP:

- **4.2.204.1.** EAP-TLS
- **4.2.204.2.** EAP-TTLS;
- **4.2.204.3.** EAP-PEAP;
- **4.2.204.4.** EAP-SIM
- **4.2.204.5.** EAP-AKA;

4.2.205 Deverá suportar 802.1x através de RADIUS;

4.2.206 Deverá suportar filtro baseado em endereço MAC por SSID;

4.2.207 Deverá permitir configurar parâmetros de rádio, como: banda e canal;

4.2.208 Deverá possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast;

4.2.209 Deverá possuir mecanismo de identificação e controle de Rogue APs, suportando supressão automática e bloqueio por endereço MAC de APs;

4.2.210 Deverá possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue);

4.2.211 Deverá possuir WIDS com, ao menos, os seguintes perfis:

- **4.2.211.1.** Rogue/Interfering AP Detection;
- **4.2.211.2.** Ad-hoc Network Detection;
- **4.2.211.3.** Wireless Bridge Detection;
- **4.2.211.4.** Weak WEP Detection;
- **4.2.211.5.** MAC OUI Checking;

4.2.212 A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;

4.2.213 A controladora deverá oferecer Firewall integrado, baseado em identidade do usuário;

4.2.214 Deverá possuir controle baseado em política de firewall para acesso entre as WLANs;

4.2.215 Deverá permitir a criação de políticas de traffic shaping;

4.2.216 Deverá permitir a criação de políticas de firewall baseadas em horário;

4.2.217 Deverá permitir NAT nas políticas de firewall;

4.2.218 Deverá possibilitar definir número de clientes por SSID;

4.2.219 Deverá permitir e/ou bloquear o tráfego entre SSIDs;

4.2.220 Deverá possuir mecanismo de criação automática de usuários visitantes e senhas auto-geradas e/ou manual, que possam ser enviadas por e-mail ou SMS aos usuários, e com capacidade de definição de horário da expiração da senha;

4.2.221 A comunicação entre o Access Point e a Controladora Wireless deverá poder ser efetuada de forma criptografada;

4.2.222 Deverá possuir mecanismo de ajuste de potência do sinal, de forma a reduzir interferência entre canais entre

02 (dois) Access Points gerenciados;

4.2.223 Deverá possuir mecanismo de balanceamento de tráfego/usuários entre Access Points;

4.2.224 Deverá possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou rádios;

4.2.225 Toda a configuração do Ponto de Acesso deverá ser executada através da Controladora Wireless;

4.2.226 Deverá permitir a identificação de APs com firmware desatualizado e efetuar o upgrade via interface gráfica;

4.2.227 Deverá possuir console de monitoramento dos usuários conectados, indicando em que Access Point, em que rádio, em que canal, endereço IP do usuário, tipo de dispositivo e sistema operacional, uso de banda, potência do sinal e relação sinal/ruído;

4.2.228 O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser encaminhados dentro do túnel até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional do próprio fabricante para suportar a conexão dos túneis originados dos pontos de acesso;

4.2.229 A Controladora deverá oferecer Firewall integrado, baseado em identidade do usuário, entre todas as redes cujo tráfego seja tunelado até a Controladora;

4.2.230 Deverá possuir controle baseado em política de firewall para acesso entre as WLANs cujo tráfego seja tunelado até a Controladora;

4.2.231 Deverá permitir a criação de políticas de traffic shaping entre todas as redes cujo tráfego seja tunelado até a Controladora;

4.2.232 Deverá permitir aplicar políticas de filtro de conteúdo Web, que seja baseado em categorias de sites. automaticamente atualizadas, para todas as redes cujo tráfego seja tunelado até a Controladora;

4.2.233 Deverá permitir aplicar políticas de antivírus, com detecção e bloqueio de malwares e redes botnet, entre todas as redes cujo tráfego seja tunelado até a Controladora;

4.2.234 Deverá permitir aplicar políticas de IPS, bloqueando e/ou monitorando tentativas de ataques, com base de assinatura de ataques atualizada automaticamente, entre todas as redes cujo tráfego seja tunelado até a Controladora;

4.2.235 Deverá permitir aplicar políticas de controle antispam para todas as redes cujo tráfego seja tunelado até a Controladora;

4.2.236 Deverá permitir controlar, identificar e bloquear tráfego de aplicações do tipo P2P, IM, Chat, Redes Sociais, Skype, Proxies Anônimos, streamings de áudio e vídeo, jogos entre outros, e que seja baseado no padrão de comunicação de tais aplicações, entre todas as redes cujo tráfego seja tunelado até a Controladora;

4.2.237 Deverá possuir as seguintes certificações:

4.237.1.- Certificação Wi-Fi Alliance;

4.2.237.2. Certificação ICSA para Firewall;

4.2.237.3. Certificação ICSA para Antivírus;

4.237.4. Certificação ICSA para VPN SSL;

4.2.237.5. Certificação ICSA para VPN IPSec;

4.2.237.6. Certificação ICSA para IPS;

- FUNCIONALIDADE DE SD-WAN -

4.2.238. A solução SD-WAN deve ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.

4.2.239. A solução SD-WAN deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos.

4.2.240. A solução SD-WAN deve suportar segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN.

4.2.241. A solução SD-WAN deve prover capacidade de inspeção SSL para a inspeção de tráfego https nas filiais, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações.

4.2.242. Solução deve ser capaz de prover Zero Touch provisioning.

4.2.243. A solução de Zero Touch provisioning deve ser capaz de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN.

4.2.244. Solução deve ser capaz de prover uma arquitetura onde em uma comunicação Matriz x Filiais, em que a comunicação de uma Filial A para a Matriz esteja comprometida, possa ser utilizada a comunicação entre Filial B e Matriz, em que através deste circuito, a Filial A alcance a Matriz.

4.2.245. A solução deve ser capaz de criar VPN "Full-Mesh", de forma automática, e sem que o administrador precise configurar site por site.

4.2.246. Reconhecimento em camada 7 totalmente segregado da camada 4.

4.2.247. Deve de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação à um determinado IP/ range de IPs de destino.

4.2.248. O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;

4.2.249. Ainda sobre o reconhecimento de Aplicações, a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook, etc);

4.2.250. A solução de SD-WAN deve suportar Roteamento dinâmico BGP com suporte a IPv6

4.2.251. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições onde a largura de banda é modificada.

4.2.252. A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN.

4.2.253. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link principal recuperado seja X% (com X variando de 10 à 50) do seu valor de Saúde melhor que o link atual.

4.2.254. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema.

4.2.255. A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN.

4.3. SOLUÇÃO DE SEGURANÇA E GERÊNCIA DE REDES NGFW TIPO 3

- CARACTERÍSTICAS E FUNCIONALIDADES GERAIS -

4.3.1. Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux.

4.3.2. Poderá ser entregue em equipamento único ou com composição de equipamentos.

4.3.3. Deverá possuir e estar licenciados com as funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, DLP – Data Leak Prevention, Controladora Wireless e Virtualização, pelo período de 60 (sessenta) meses.

4.3.4. Firewall com capacidade mínima de processamento de 4 (quatro) Gbps.

4.3.5. IPS com capacidade mínima de processamento de 900 (novecentos) Mbps.

4.3.6. Proteção contra Ameaças Avançadas (Threat Protection) com capacidade mínima de processamento de 500 (quinhentos) Mbps. Proteção contra Ameaças Avançadas contempla as funções de Firewall, IPS, Controle de Aplicação e Proteção contra Malware/Vírus ativadas em conjunto.

4.3.7. Inspeção SSL Throughput com capacidade mínima de processamento de 300 (trezentos) Mbps.

4.3.8. VPN com capacidade de, pelo menos, 4 (quatro) Gbps de tráfego IPSec.

4.3.9. VPN SSL com capacidade de, pelo menos, 450 (novecentos) Mbps de tráfego.

4.3.10. Deverá suportar 600 (seiscentos mil) conexões simultâneas.

4.3.11. Deverá suportar, pelo menos, 30.000 (quarenta mil) novas conexões por segundo.

4.3.12. Deverão ser licenciados para suportar, pelo menos, 100 (cem) usuários de VPN SSL.

4.3.13. Deverá suportar, pelo menos, 100 (cem) túneis de VPN Site-Site.

4.3.14. Deverá suportar, pelo menos, 200 (duzentos) túneis de VPN Client-Site.

4.3.15. Deverá possuir pelo menos 4 (quatro) interfaces RJ 45 01 GE.

4.3.16. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 6 (seis) Pontos de Acesso sem fio.

4.3.17. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 6 (seis) equipamentos.

4.3.18. Deverá ser compatível e integrável com o ITEM 4 deste Termo de Referência.

4.3.19. Deverá ser compatível e integrável com o ITEM 5 deste Termo de Referência.

4.3.20. Deverá ser fornecida toda documentação técnica, bem como manual de utilização, em português do Brasil ou em inglês.

- FUNCIONALIDADES DE FIREWALL -

4.3.21. Deverá possuir controle de acesso à internet por endereço IP de origem e destino;

4.3.22. Deverá possuir controle de acesso à internet por subrede;

4.3.23. Deverá suportar tags de VLAN (802.1q);

4.3.24. Deverá possuir ferramenta de diagnóstico do tipo tcpdump;

4.3.25. Deverá possuir integração com servidores de autenticação RADIUS, LDAP e Microsoft Active Directory;
4.3.26. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;
4.3.27. Deverá suportar single-sign-on para Active Directory, Novell eDirectory, Citrix e RADIUS;
4.3.28. Deverá possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);
4.3.29. Deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, vários para um, NAT64, NAT46, PAT, STUN e Full Cone NAT;
4.3.30. Deverá permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;
4.3.31. Deverá permitir controle de acesso à internet por domínio, por exemplo: gov.br, org.br, edu.br;
4.3.32. Deverá possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT;
4.3.33. Deverá suportar roteamento estático e dinâmico RIP V1, V2, OSPF, ISIS e BGPv4;
4.3.34. Deverá possuir funcionalidades de DHCP Cliente, Servidor e Relay;
4.3.35. Deverá suportar aplicações multimídia, como: H.323 e SIP;
4.3.36. Deverá possuir tecnologia de firewall do tipo Statefull;
4.3.37. Deverá suportar alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;
4.3.38. Deverá permitir o funcionamento em modo transparente tipo "bridge" sem alterar o endereço MAC do tráfego;
4.3.39. Deverá suportar PBR – Policy Based Routing;
4.3.40. Deverá permitir a criação de VLANS no padrão IEEE 802.1q;
4.3.41. Deverá possuir conexão entre estação de gerência e appliance criptografada, tanto em interface gráfica, quanto em CLI (linha de comando);
4.3.42. Deverá permitir filtro de pacotes sem controle de estado (stateless) para verificação em camada 2;
4.3.43. Deverá permitir forwarding de camada 2 para protocolos não IP;
4.3.44. Deverá suportar forwarding multicast;
4.3.45. Deverá suportar roteamento multicast PIM Sparse Mode e Dense Mode;
4.3.46. Deverá permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos: TCP, UDP, ICMP e IP;
4.3.47. Deverá permitir o agrupamento de serviços;
4.3.48. Deverá permitir o filtro de pacotes sem a utilização de NAT;
4.3.49. Deverá permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;
4.3.50. Deverá possuir mecanismo de anti-spoofing;
4.3.51. Deverá permitir criação de regras definidas pelo usuário;
4.3.52. Deverá permitir o serviço de autenticação para tráfego HTTP e FTP;
4.3.53. Deverá permitir IP/MAC binding, permitindo que cada endereço IP possa ser associado a um endereço MAC, gerando maior controle dos endereços internos e impedindo o IP spoofing;

4.3.54. Deverá possuir a funcionalidade de balanceamento e contingência de links;
4.3.55. Deverá suportar sFlow;
4.3.56. O dispositivo deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas;
4.3.57. Deverá ter a capacidade de criar e aplicar políticas de reputação de cliente para registrar e pontuar as seguintes atividades: tentativas de conexões más, pacotes bloqueados por política, detecção de ataques de intrusão, detecção de ataques de malware, atividades Web em categorias de risco, proteção de aplicação, locais geográficos que os clientes estão tentando se comunicar;
4.3.58. Deverá permitir autenticação de usuários em base local, servidor LDAP, RADIUS e TACACS;
4.3.59. Deverá permitir a criação de regras baseada em usuário, grupo de usuários, endereço IP, FQDN, horário, protocolo e aplicação;
4.3.60. Deverá suportar certificados X.509, SCEP, Certificate Signing Request (CSR) e OCSP;
4.3.61. Deverá permitir funcionamento em modo bridge, router, proxy explícito, sniffer e/ou VLAN-tagged;
4.3.62. Deverá possuir mecanismo de tratamento (session-helpers ou ALGs) para os protocolos ou aplicações dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS;
4.3.63. Deverá suportar SIP, H.323 e SCCP NAT Traversal;
4.3.64. Deverá permitir a criação de objetos e agrupamento de objetos de usuários, redes, FQDN, protocolos e serviços para facilitar a criação de regras;
4.3.65. Deverá possuir porta de comunicação serial ou USB para testes e configuração do equipamento, com acesso protegido por usuário e senha.

- FUNCIONALIDADE DE TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO -

4.3.66. Deverá permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound), através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;
4.3.67. Deverá permitir modificação de valores DSCP para o DiffServ;
4.3.68. Deverá permitir priorização de tráfego e suportar ToS;
4.3.69. Deverá limitar individualmente a banda utilizada por programas, tais como: peer-to-peer, streaming, chat, VoIP e Web;
4.3.70. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
4.3.71. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;
4.3.72. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;
4.3.73. Deverá permitir definir banda máxima e banda garantida para um usuário, IP, grupo de IPs, protocolo e aplicação;
4.3.74. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por subrede de origem e destino;

4.3.75. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

- FUNCIONALIDADE DE ANTI-SPAM DE GATEWAY -

4.3.76. Deverá permitir, na funcionalidade de anti-spam, verificação do cabeçalho SMTP do tipo MIME;
4.3.77. Deverá possuir filtragem de e-mail por palavras chaves;
4.3.78. Deverá permitir adicionar rótulo ao assunto da mensagem quando classificado como SPAM;
4.3.79. Deverá possuir, para a funcionalidade de anti-spam, o recurso de RBL;
4.3.80. Deverá permitir a checagem de reputação da URL no corpo mensagem de correio eletrônico;

- FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB -

4.3.81. Deverá possuir solução de filtro de conteúdo Web integrado à solução de segurança;
4.3.82. Deverá possuir, pelo menos, 70 (setenta) categorias para classificação de sites Web;
4.3.83. Deverá possuir base mínima contendo 40.000.000 (quarenta milhões) de sites internet Web já registrados e classificados;
4.3.84. Deverá possuir a funcionalidade de cota de tempo de utilização por categoria;
4.3.85. Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites Web, como:
    4.3.85.1. Proxy anônimo;
    4.3.85.2. Webmail;
    4.3.85.3. Instituições de saúde;
    4.3.85.4. Notícias;
    4.3.85.5. Phishing;
    4.3.85.6. Hackers;
    4.3.85.7. Pornografia;
    4.3.85.8. Racismo;
    4.3.85.9. Websites pessoais;
    4.3.85.10. Compras;
4.3.86. Deverá permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;
4.3.87. Deverá permitir a criação de, pelo menos, 05 (cinco) categorias personalizadas;
4.3.88. Deverá permitir a reclassificação de sites Web, tanto por URL, quanto por endereço IP;
4.3.89. Deverá prover Termo de Responsabilidade on-line para aceite pelo usuário, a ser apresentado toda vez que houver tentativa de acesso a determinado serviço permitido ou bloqueado;
4.3.90. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;
4.3.91. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
4.3.92. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;

4.3.93. Deverá exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança;
4.3.94. Deverá permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies e activeX, através de base de URL própria atualizável;
4.3.95. Deverá permitir o bloqueio de páginas Web através da construção de filtros específicos com mecanismo de busca textual;
4.3.96. Deverá permitir a criação de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra);
4.3.97. Deverá permitir o bloqueio de URLs inválidas, cujo campo CN do certificado SSL não contenha um domínio válido;
4.3.98. Deverá filtrar o conteúdo baseado em categorias em tempo real;
4.3.99. Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo Web;
4.3.100. Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;
4.3.101. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
4.3.102. Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem;
4.3.103. Deverá ser capaz de categorizar a página Web, tanto pela sua URL, como pelo seu endereço IP;
4.3.104. Deverá permitir o bloqueio de páginas Web por classificação como páginas que facilitem a busca de áudio, vídeo e URLs originadas de spams;
4.3.105. Deverá possuir Proxy Explícito e Transparente;
4.3.106. Deverá implementar roteamento WCCP e ICAP;

- FUNCIONALIDADE DE DETECÇÃO DE INTRUSÃO -

4.3.107. Deverá permitir que seja definido, através de regra por IP origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão;
4.3.108. Deverá possuir base de assinaturas de IPS com, pelo menos, 3.500 (três mil e quinhentas) ameaças conhecidas;
4.3.109. Deverá estar orientado à proteção de redes;
4.3.110. Deverá permitir funcionar em modo transparente, sniffer e router;
4.3.111. Deverá possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente;
4.3.112. Deverá permitir a criação de padrões de ataque manualmente;
4.3.113. Deverá possuir integração à plataforma de segurança;
4.3.114. Deverá possuir capacidade de remontagem de pacotes para identificação de ataques;
4.3.115. Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas a web-server, para que seja usado para proteção específica de Servidores Web;

4.3.116. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
4.3.117. Deverá possuir mecanismos de detecção/proteção de ataques;
4.3.118. Deverá possuir reconhecimento de padrões;
4.3.119. Deverá possuir análise de protocolos;
4.3.120. Deverá possuir detecção de anomalias;
4.3.121. Deverá possuir detecção de ataques de RPC (Remote Procedure Call);
4.3.122. Deverá possuir proteção contra-ataques de Windows ou NetBios;
4.3.123. Deverá possuir proteção contra-ataques de SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Office Protocol);
4.3.124. Deverá possuir proteção contra-ataques DNS (Domain Name System);
4.3.125. Deverá possuir proteção contra-ataques a FTP, SSH, Telnet e rlogin;
4.3.126. Deverá possuir proteção contra-ataques de ICMP (Internet Control Message Protocol);
4.3.127. Deverá possuir métodos de notificação de detecção de ataques;
4.3.128. Deverá possuir alarmes na console de administração;
4.3.129. Deverá possuir alertas via correio eletrônico;
4.3.130. Deverá possuir monitoração do comportamento do appliance, mediante SNMP. O dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;
4.3.131. Deverá ter a capacidade de resposta/logs ativa a ataques;
4.3.132. Deverá prover a terminação de sessões via TCP resets;
4.3.133. Deverá armazenar os logs de sessões;
4.3.134. Deverá atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
4.3.135. Deverá mitigar os efeitos dos ataques de negação de serviços;
4.3.136. Deverá permitir a criação de assinaturas personalizadas;
4.3.137. Deverá possuir filtros de ataques por anomalias;
4.3.138. Deverá permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destinationsessionlimit;
4.3.139. Deverá permitir filtros de anomalias de protocolos;
4.3.140. Deverá suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;
4.3.141. Deverá suportar verificação de ataque na camada de aplicação;
4.3.142. Deverá suportar verificação de tráfego em tempo real, via aceleração de hardware;
4.3.143. Deverá possuir as seguintes estratégias de bloqueio: pass, drop e reset.

- FUNCIONALIDADE DE VPN -

4.3.144. Deverá possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
4.3.145. Deverá possuir suporte a certificados PKI X.509 para construção de VPNs;
4.3.146. Deverá possuir suporte a VPNs IPSeC Site-to-Site e VPNs IPSec Client-to-Site;
4.3.147. Deverá possuir suporte a VPN SSL;
4.3.148. Deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais;

4.3.149. A VPN SSL deverá possibilitar o acesso à rede, de acordo com a política de segurança, através do acesso via navegador WEB;
4.3.150. Deverá possuir hardware acelerador criptográfico para incrementar o desempenho da VPN;
4.3.151. A VPN SSL deverá suportar cliente para plataforma Windows, Linux e Mac OS X;
4.3.152. Deverá permitir a arquitetura de VPN hub and spoke;
4.3.153. Deverá possuir suporte à inclusão em autoridades certificadoras (enrollment), mediante SCEP (Simple Certificate Enrollment Protocol) e mediante arquivos.

- FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES -

4.3.154. Deverá reconhecer, no mínimo, 2.000 (duas mil) aplicações;
4.3.155. Deverá possuir, pelo menos, 10 (dez) categorias para classificação de aplicações;
4.3.156. Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações, como:
  4.3.156.1. P2P;
  4.3.156.2. Instant Messaging;
  4.3.156.3. Web-Client;
  4.3.156.4. Transferência de arquivos;
  4.3.156.5. VoIP;
4.3.157. Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;
4.3.158. Deverá ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma;
4.3.159. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
4.3.160. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
4.3.161. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;
4.3.162. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;
4.3.163. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
4.3.164. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;
4.3.165. Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;
4.3.166. Deverá permitir a inspeção/bloqueio de códigos maliciosos para, no mínimo, as seguintes categorias: Instant Messaging e transferência de arquivos;
4.3.167. Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações;
4.3.168. Deverá permitir criação de padrões de aplicação manualmente;

- FUNCIONALIDADE DE DLP (DATA LEAK PREVENTION) -

4.3.169. O sistema de DLP (Data Leak Prevention – Proteção contra Vazamento de Informações) de gateway deverá funcionar de maneira que se consiga que os

dados sensíveis não saiam da rede e também deverá funcionar de modo que se previna que dados não requisitados entrem na sua rede;

4.3.170. Deverá inspecionar, no mínimo, os tráfegos de e-mail e HTTP;

4.3.171. Sobre o tráfego de e-mail, deverá inspecionar, no mínimo, os protocolos SMTP, POP3 e IMAP;

4.3.172. Deverá realizar buscas para a aplicação de regras de DLP em arquivos do tipo PDF e MS-Word;

4.3.173. Deverá aplicar regras baseadas em usuários autenticados, isto é, fazendo buscas pelo tráfego de um específico usuário;

4.3.174. Deverá verificar para aplicações do tipo e-mail, se o anexo das mensagens de correio entrantes/saintes possui um tamanho máximo especificado pelo administrador;

4.3.175. Deverá utilizar expressões regulares para composição das regras de verificação dos tráfegos;

4.3.176. Deverá tomar minimamente as ações de bloquear ou colocar o IP em quarentena;

4.3.177. Deverá permitir o armazenamento em solução específica de armazenamento de logs, o conteúdo do tráfego que coincidir com o tráfego esperado pela regra de DLP para minimamente os protocolos de e-mail e HTTP;

4.3.178. Deverá permitir a composição de múltiplas regras de DLP, formando uma regra única mais específica que usa lógica booleana para fazer a comparação com o tráfego que atravessa o sistema.

- FUNCIONALIDADE DE BALANCEAMENTO DE CARGA -

4.3.179. Deverá permitir a criação de endereços IPs virtuais;

4.3.180. Deverá permitir balanceamento de carga entre, pelo menos, 04 (quatro) servidores reais;

4.3.181. Deverá suportar balanceamento, ao menos, para os seguintes serviços: HTTP, HTTPS, TCP e UDP;

4.3.182. Deverá permitir balanceamento, ao menos, com os seguintes métodos: Hash do endereço IP de origem, Round Robin, Weighted, First Alive e HTTP host;

4.3.183. Deverá permitir persistência de sessão por cookie HTTP ou SSL session ID;

4.3.184. Deverá permitir que seja mantido o IP de origem;

4.3.185. Deverá suportar SSL offloading nos equipamentos que suportem, pelo menos, 200 (duzentos) usuários;

4.3.186. Deverá ter a capacidade de identificar, através de health checks, quais os servidores que estejam ativos, removendo automaticamente o tráfego dos servidores que não estejam;

4.3.187. Deverá permitir que o health check seja feito, ao menos, via ICMP, TCP em porta configurável e HTTP.

- FUNCIONALIDADE DE VIRTUALIZAÇÃO -

4.3.188. Deverá suportar a criação de, ao menos, 10 (dez) instâncias virtuais no mesmo hardware;

4.3.189. Deverá permitir a criação de administradores independentes para cada uma das instâncias virtuais;

4.3.190. Deverá permitir a criação de um administrador global que tenha acesso a todas as configurações das instâncias virtuais criadas.

- FUNCIONALIDADE DE CONTROLADORA WIRELESS -

4.3.191. Deverá ser capaz de gerenciar, de forma centralizada, outros Pontos de Acesso do mesmo fabricante;
4.3.192. Deverá suportar o serviço de servidor DHCP por SSID para prover endereçamento IP automático para os clientes wireless;
4.3.193. Deverá suportar monitoração e supressão de Ponto de Acesso indevido;
4.3.194. Deverá prover autenticação para a rede wireless através de bases externas, como: LDAP, RADIUS ou TACACS+;
4.3.195. Deverá permitir a visualização dos clientes conectados;
4.3.196. Deverá prover suporte a Fast Roaming;
4.3.197. Deverá ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF;
4.3.198. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;
4.3.199. Deverá possuir Captive Portal por SSID;
4.3.200. Deverá permitir configurar o bloqueio de tráfego entre SSIDs;
4.3.201. Deverá suportar Wi-Fi Protected Access (WPA), WPA2 ou WPA3 por SSID, utilizando-se de AES e/ou TKIP;
4.3.202. Deverá suportar os seguintes métodos de autenticação EAP:
    4.3.202.1. EAP-TLS
    4.3.202.2. EAP-TTLS;
    4.3.202.3. EAP-PEAP;
    4.3.202.4. EAP-SIM
    4.3.202.5. EAP-AKA;
4.3.203. Deverá suportar 802.1x através de RADIUS;
4.3.204. Deverá suportar filtro baseado em endereço MAC por SSID;
4.3.205. Deverá permitir configurar parâmetros de rádio, como: banda e canal;
4.3.206. Deverá possuir método de descoberta de novos Pontos de Acesso baseados em Broadcast ou Multicast;
4.3.207. Deverá possuir mecanismo de identificação e controle de Rogue APs, suportando supressão automática e bloqueio por endereço MAC de APs;
4.3.208. Deverá possuir lista contendo Pontos de Acesso Aceitos e Pontos de Acesso Indevidos (Rogue);
4.3.209. Deverá possuir WIDS com, ao menos, os seguintes perfis:
    4.3.209.1. Rogue/Interfering AP Detection;
    4.3.209.2. Ad-hoc Network Detection;
    4.3.209.3. Wireless Bridge Detection;
    4.3.209.4. Weak WEP Detection;
    4.3.209.5. MAC OUI Checking;

4.3.210. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;
4.3.211. A controladora deverá oferecer Firewall integrado, baseado em identidade do usuário;
4.3.212. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs;
4.3.213. Deverá permitir a criação de políticas de traffic shaping;
4.3.214. Deverá permitir a criação de políticas de firewall baseadas em horário;
4.3.215. Deverá permitir NAT nas políticas de firewall;
4.3.216. Deverá possibilitar definir número de clientes por SSID;
4.3.217. Deverá permitir e/ou bloquear o tráfego entre SSIDs;
4.3.218. Deverá possuir mecanismo de criação automática de usuários visitantes e senhas auto-geradas e/ou manual, que possam ser enviadas por e-mail ou SMS aos usuários, e com capacidade de definição de horário da expiração da senha;
4.3.219. A comunicação entre o Access Point e a Controladora Wireless deverá poder ser efetuada de forma criptografada;
4.3.220. Deverá possuir mecanismo de ajuste de potência do sinal, de forma a reduzir interferência entre canais entre 02 (dois) Access Points gerenciados;
4.3.221. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre Access Points;
4.3.222. Deverá possuir mecanismo de balanceamento de tráfego/usuários entre frequências e/ou rádios;
4.3.223. Toda a configuração do Ponto de Acesso deverá ser executada através da Controladora Wireless;
4.3.224. Deverá permitir a identificação de APs com firmware desatualizado e efetuar o upgrade via interface gráfica;
4.3.225. Deverá possuir console de monitoramento dos usuários conectados, indicando em que Access Point, em que rádio, em que canal, endereço IP do usuário, tipo de dispositivo e sistema operacional, uso de banda, potência do sinal e relação sinal/ruído;
4.3.226. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser encaminhados dentro do túnel até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional do próprio fabricante para suportar a conexão dos túneis originados dos pontos de acesso;
4.3.227. A Controladora deverá oferecer Firewall integrado, baseado em identidade do usuário, entre todas as redes cujo tráfego seja tunelado até a Controladora;
4.3.228. Deverá possuir controle baseado em política de firewall para acesso entre as WLANs cujo tráfego seja tunelado até a Controladora;
4.3.229. Deverá permitir a criação de políticas de traffic shaping entre todas as redes cujo tráfego seja tunelado até a Controladora;

4.3.230. Deverá permitir aplicar políticas de filtro de conteúdo Web, que seja baseado em categorias de sites automaticamente atualizadas, para todas as redes cujo tráfego seja tunelado até a Controladora;

4.3.231. Deverá permitir aplicar políticas de antivírus, com detecção e bloqueio de malwares e redes botnet, entre todas as redes cujo tráfego seja tunelado até a Controladora;

4.3.232. Deverá permitir aplicar políticas de IPS, bloqueando e/ou monitorando tentativas de ataques, com base de assinatura de ataques atualizada automaticamente, entre todas as redes cujo tráfego seja tunelado até a Controladora;

4.3.233. Deverá permitir aplicar políticas de controle antispam para todas as redes cujo tráfego seja tunelado até a Controladora;

4.3.234. Deverá permitir controlar, identificar e bloquear tráfego de aplicações do tipo P2P, IM, Chat, Redes Sociais, Skype, Proxies Anônimos, streamings de áudio e vídeo, jogos entre outros, e que seja baseado no padrão de comunicação de tais aplicações, entre todas as redes cujo tráfego seja tunelado até a Controladora;

4.3.235. Deverá possuir as seguintes certificações:

4.3.235.1. Certificação Wi-Fi Alliance;

4.3.235.2. Certificação ICSA para Firewall;

4.3.235.3. Certificação ICSA para Antivírus;

4.3.235.4. Certificação ICSA para VPN SSL;

4.3.235.5. Certificação ICSA para VPN IPSec;

4.3.235.6. Certificação ICSA para IPS;

- FUNCIONALIDADE DE SD-WAN -

4.3.236. A solução SD-WAN deve ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web.

4.3.237. A solução SD-WAN deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos.

4.3.238. A solução SD-WAN deve suportar segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN.

4.3.239. A solução SD-WAN deve prover capacidade de inspeção SSL para a inspeção de tráfego https nas filiais, no contexto: bloqueio de malwares e reconhecimento em camada 7 de aplicações.

4.3.240. Solução deve ser capaz de prover Zero Touch provisioning.

4.3.241. A solução de Zero Touch provisioning deve ser capaz de suportar endereçamento estáticos e dinâmicos, e que seja suportado múltiplos links WAN.

4.3.242. Solução deve ser capaz de prover uma arquitetura onde em uma comunicação Matriz x Filiais, em que a comunicação de uma Filial A para a Matriz esteja comprometida, possa ser utilizada a comunicação entre Filial B e Matriz, em que através deste circuito, a Filial A alcance a Matriz.

4.3.243. A solução deve ser capaz de criar VPN "Full-Mesh", de forma automática, e sem que o administrador precise configurar site por site.

4.3.244. Reconhecimento em camada 7 totalmente segregado da camada 4.

4.3.245. Deve de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação à um determinado IP/ range de IPs de destino.

4.3.246. O reconhecimento de aplicações deve ser realizado independente de porta e protocolo, inspecionando o payload de pacote de dados;
4.3.247. Ainda sobre o reconhecimento de Aplicações, a solução deve fornecer o reconhecimento default em camada 7, de pelo menos mais de 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook, etc);
4.3.248. A solução de SD-WAN deve suportar Roteamento dinâmico BGP com suporte a IPv6
4.3.249. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições onde a largura de banda é modificada.
4.3.250. A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN.
4.3.251. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link principal recuperado seja X% (com X variando de 10 à 50) do seu valor de Saúde melhor que o link atual.
4.3.252. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema.
4.3.253. A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN.

4.4. UNIDADE CENTRALIZADA DE ARMAZENAMENTO DE LOGS E RELATORIA

- CARACTERÍSTICAS E FUNCIONALIDADES GERAIS -

4.4.1. Solução baseada em appliance físico, possuir garantia e licença para atualização de firmware e atualização automática de base de dados de todas as funcionalidades pelo período de 60 (sessenta) meses.
4.4.2. Deverá possuir a capacidade de receber pelo menos 90 GB de logs diários.
4.4.3. Deverá possuir taxa analítica de 1.500 (um mil e quinhentos) logs por segundo.
4.4.4. Deverá possuir 04 (quatro) interfaces RJ45 1GE.
4.4.5. Deverá possuir capacidade de armazenamento de no mínimo 04 (quatro) TB.

- REQUISITOS MÍNIMOS DE FUNCIONALIDADE -

4.4.6. Deverá suportar o acesso via SSH e WEB (HTTPS) para gerenciamento de soluções.
4.4.7. Deverá possuir comunicação e autenticação criptografada com usuário e senha para obter relatórios, na interface gráfica (GUI) e via linha de comando no console de gerenciamento.
4.4.8. Deverá permitir o acesso simultâneo à administração, bem como permitir que pelo menos 2 (dois) perfis sejam criados para administração e monitoramento.
4.4.9. Deverá suportar SNMP versão 2 e 3
4.4.10. Deverá permitir a virtualização do gerenciamento e administração dos dispositivos, nos quais cada administrador só tem acesso aos computadores autorizados.
4.4.11. Deverá permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução.

4.4.12. Deverá permitir ativar e desativar para cada interface da plataforma, as permissões de acesso HTTP, HTTPS, SSH
4.4.13. Deverá possuir autenticação de usuários para acesso à plataforma via LDAP
4.4.14. Deverá possuir autenticação de usuários para acesso à plataforma via Radius
4.4.15. Deverá possuir autenticação de usuários para acesso à plataforma via TACACS+.
4.4.16. Deverá possuir geração de relatórios de tráfego em tempo real, em formato de mapa geográfico
4.4.17. Deverá possuir geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas.
4.4.18. Deverá possuir geração de relatórios de tráfego em tempo real, em formato de gráfico
4.4.19. Deverá possuir definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais.
4.4.20. Deverá possuir um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha.
4.4.21. Deverá possuir visualização da quantidade de logs enviados de cada dispositivo monitorado
4.4.22. Deverá possuir mecanismos de apagamento automático para logs antigos.
4.4.23. Deverá permitir importação e exportação de relatórios;
4.4.24. Deverá ter a capacidade de criar relatórios no formato HTML;
4.4.25. Deverá ter a capacidade de criar relatórios em formato PDF;
4.4.26. Deverá ter a capacidade de criar relatórios no formato XML;
4.4.27. Deverá ter a capacidade de criar relatórios no formato CSV;
4.4.28. Deverá permitir exportar os logs no formato CSV;
4.4.29. Deverá gerar logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário.
4.4.30. Deverá permitir que os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar.
4.4.31. Deverá ter relatórios predefinidos.
4.4.32. Deverá poder enviar automaticamente os logs para um servidor FTP externo para a solução
4.4.33. Deverá permitir a duplicação de relatórios existentes, deve ser possível para edição posterior.
4.4.34. Deverá ter a capacidade de personalizar a capa dos relatórios obtidos.
4.4.35. Deverá permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos mesmos logs.
4.4.36. Deverá ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas
4.4.37. Deverá ter um mecanismo de "pesquisa detalhada" para navegar pelos relatórios em tempo real.
4.4.38. Deverá permitir que os arquivos de log sejam baixados da plataforma para uso externo.

4.4.39. Deverá ter a capacidade de gerar e enviar relatórios periódicos automaticamente.
4.4.40. Deverá permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades.
4.4.41. Deverá permitir o envio por e-mail relatórios automaticamente.
4.4.42. Deverá permitir que o relatório seja enviado por email ao destinatário específico.
4.4.43. Deverá permitir a programação da geração de relatórios, conforme calendário definido pelo administrador.
4.4.44. Deverá exibir graficamente em tempo real a taxa de geração de logs para cada dispositivo gerenciado.
4.4.45. Deverá permitir o uso de filtros nos relatórios.
4.4.46. Deverá permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros.
4.4.47. Deverá permitir especificar o idioma dos relatórios criados
4.4.48. Deverá gerar alertas automáticos por email, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros.
4.4.49. Deverá permitir o envio automático de relatórios para um servidor SFTP ou FTP externo.
4.4.50. Deverá ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios.
4.4.51. Deverá possibilitar visualizar nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros.
4.4.52. Deverá ter uma ferramenta que permita analisar o desempenho na geração de relatórios, a fim de detectar e corrigir problemas na geração deles.
4.4.53. Deverá importar arquivos com logs de dispositivos compatíveis conhecidos e não conhecidos pela plataforma, para geração posterior de relatórios.
4.4.54. Deverá ser possível definir o espaço que cada instância de virtualização pode usar para armazenamento de log.
4.4.55. Deverá fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado.
4.4.56. Deverá ser compatível com a autenticação de fator duplo (token) para usuários do administrador da plataforma.
4.4.57. Deverá permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos
4.4.58. Deverá permitir visualizar em tempo real os logs recebidos.
4.4.59. Deverá permitir o encaminhamento de log no formato syslog.
4.4.60. Deverá permitir o encaminhamento de log no formato CEF (Common Event Format).
4.4.61. Deverá permitir a criação de painéis personalizados para monitorar operações SOC.
4.4.62. Deverá gerar alertas de eventos a partir de logs recebidos
4.4.63. Deverá permitir a criação de incidentes a partir de alertas de eventos para o terminal.

4.4.64. Deverá permitir a integração ao sistema de tickets do ServiceNow.
4.4.65. Deverá permitir o suporte a logs na nuvem pública do Amazon S3.
4.4.66. Deverá permitir o suporte a logs na nuvem pública do Microsoft Azure.
4.4.67. Permitir o suporte aos registros de nuvem pública do Gooogle Cloud.
4.4.68. Suportar o padrão SAML para autenticação do usuário administrador.

- FUNCIONALIDADES DE RELATÓRIO -

4.4.69. Deverá possuir relatório de conformidade com o PCI DSS;
4.4.70. Deverá possuir um relatório de uso do aplicativo SaaS
4.4.71. Deverá possuir um relatório de prevenção de perda de dados (DLP)
4.4.72. Deverá possuir um relatório de VPN
4.4.73. Deverá possuir um relatório IPS (Intruder Prevention System)
4.4.74. Deverá possuir um relatório de reputação do cliente
4.4.75. Deverá possuir um relatório de análise de segurança do usuário
4.4.76. Deverá possuir um relatório de análise de ameaças cibernéticas
4.4.77. Deverá possuir um breve relatório resumido diário de eventos e incidentes de segurança
4.4.78. Deverá possuir um relatório de tráfego DNS
4.4.79. Deverá possuir um relatório de tráfego de e-mail
4.4.80. Deverá possuir um relatório dos 10 principais aplicativos usados na rede
4.4.81. Deverá possuir um relatório dos 10 principais sites usados na rede
4.4.82. Deverá possuir um relatório de uso de mídia social

4.5. UNIDADE DE GERÊNCIA CENTRALIZADA DE EQUIPAMENTOS

4.5.1. A solução poderá ser entregue em applince ou no formato de solução virtual, compatível com as plataformas VMware, Microsoft Hyper-V, Citrix XenServer, KVM, no caso de solução virtualizada a responsabilidade pela implantação de servidor/hardware com licenciamento necessário será da CONTRATANTE.
4.5.2. Deverá possuir garantia e licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades pelo período de 60 (sessenta) meses.
4.5.3. Deve possuir licença para gerenciar de forma centralizada de no mínimo 20 dispositivos.
4.5.4. Deve garantir a integridade do item de configuração, através de bloqueio de alterações, em caso de acesso simultâneo de dois ou mais administradores no mesmo ativo;
4.5.5. Deve possuir definição de perfis de acesso ao console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
4.5.6. Deve gerar alertas automáticos via e-mail e snmp;
4.5.7. Deve monitorar a performance e Status dos links conectados a Solução de Segurança dos links de Internet;
4.5.8. Deve possibilitar a criação e administração de políticas de firewall, controle de aplicação, sistema prevenção a intrusão (IPS – intrusion prevention system), antivírus, pontos de acesso sem fio e de filtro de URL;
4.5.9. Deve permitir usar palavras chaves ou cores para facilitar identificação de regras;

4.5.10. Deve permitir localizar quais regras um objeto (ex. Computador, serviço, etc.) está sendo utilizado;
4.5.11. Deve atribuir sequencialmente um número a cada regra de firewall, de NAT ou de QoS;
4.5.12. Deve permitir criação de regras que fiquem ativas em horário definido;
4.5.13. Deve permitir criação de regras com data de expiração;
4.5.14. Deve permitir realizar o backup das configurações para permitir o retorno (rollback) de uma configuração salva;
4.5.15. Deve possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (shadowing), ou garantir que esta exigência seja plenamente atendida por meio diverso.
4.5.16. Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;
4.5.17. Deve garantir que todos os componentes da Solução de Segurança dos Links de Internet sejam controlados de forma centralizada, utilizando apenas um servidor de gerência;
4.5.18. Deve garantir que os dispositivos de segurança sejam visualizados na operação integrada da rede através de geolocalização, e integrados com uma aplicação de mapas online (google maps, bing maps ou outra equivalente);
4.5.19. Deve possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;
4.5.20. Deve permitir ao administrador transferir os backups para um servidor SFTP;
4.5.21. Deve realizar a função de gerência em um equipamento exclusivo, não exercendo outras funções (como firewall);
4.5.22. Deve garantir que quando houver novas versões de software dos equipamentos, seja realizada a distribuição e instalação remota, de maneira centralizada;
4.5.23. Deve permitir aos administradores se autenticarem nos servidores de gerência através de contas de usuários locais, de bases externas LDAP e RADIUS.
4.5.24. Deve suportar e realizar a sincronização do relógio interno dos equipamentos da solução via protocolo NTP;
4.5.25. Deve gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas;
4.5.26. Deve permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como licenças, horário do sistema e firmware;
4.5.27. Deve permitir criar os objetos que serão utilizados nas políticas, de forma centralizada;

4.6. ATIVOS DE REDE WIRELESS INDOOR

4.6.1. Deve possuir garantia e suporte pelo período de 60 (sessenta) meses.
4.6.2. Deverá possuir, ao menos, 02 (duas) interfaces de rede 10/100/1000 Base-T RJ-45.
4.6.3. Deverá possuir, ao menos, 01 (uma) interface de console RS-232 RJ-45.
4.6.4. Deverá possuir, ao menos 01 rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento.

4.6.5. Deverá suportar, ao menos, 16 (dezesseis) SSIDs simultâneos por Ponto de Acesso, sendo, pelo menos, 08 (oito) por rádio.
4.6.6. Deverá possuir potência de transmissão de, ao menos, 21 dBm.
4.6.7. Deverá possuir antenas internas e integradas com padrão de irradiação omnidirecional compatíveis com as frequências de rádio dos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax com ganhos de, no mínimo, 3 dBi para 5GHz.
4.6.8. Deverá suportar operação na temperatura de 0 a 40 °C.
4.6.9. Deverá ser fornecido com todos os acessórios necessários para que seja feita sua fixação em teto ou parede.
4.6.10. Deverá suportar os padrões 802.11 a/b/g/n/ac/ax.
4.6.11. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;
4.6.12. O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (WIPS/WIDS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação;
4.6.13. Deverá possuir a tecnologia MU-MIMO com operação 2x2 e 2 spatial streams.
4.6.14. Deverá suportar taxas de conexão (data rate) de até 1.2 Gbps.
4.6.15. Deverá atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac Wave1/Wave2 e IEEE 802.11ax, com operação nas frequências de 2.4 GHz e 5 GHz de forma simultânea.
4.6.16. Deverá possuir PoE (Power over Ethernet), padrão 802.3at, possibilitando seu uso sem a necessidade de fontes de energia externas em qualquer porta Ethernet.
4.6.17. Deverá possuir Injetor PoE padrão 802.3at compatível com a solução.
4.6.18. Deve ser compatível e gerenciável pelos ITEM 1, 2 e 3 deste Termo de Referência ou por solução do mesmo fabricante que possua gerência centralizada.
4.6.19. Deverá suportar a criação de redes mesh.
4.6.20. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser encaminhados via túnel seguro (com criptografia) até o controlador wireless;
4.6.21. Deverá suportar a criação de enlaces de bridge entre 02 (dois) Access Points.
4.6.22. Deverá permitir a configuração individual para cada SSID, se o tráfego for tunelado até a Controladora ao qual ele está registrado e/ou se for comutado localmente.
4.6.23. Deverá suportar associação dinâmica de usuários a VLANs de acordo com parâmetros de autenticação.
4.6.24. Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz;

4.6.25. Deverá possuir funcionalidade de ajuste de potência automática, de forma a reduzir interferência entre canais.
4.6.26. Deverá implementar UL MU-MIMO 802.11ax mode.
4.6.27. Deverá implementar Spectrum Analyzer.
4.6.28. Deverá implementar Spatial Reuse (BSS Coloring).
4.6.29. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;
4.6.30. Deve suportar consultas diretamente ao ponto de acesso via SNMP e REST API;
4.6.31. Deverá possuir certificação WiFi Alliance.
4.6.32. Deverá possuir homologação da ANATEL, de acordo com a Resolução número 242.

4.7. SOLUÇÃO DE SEGURANÇA, APPLIANCE DE PROTEÇÃO PARA APLICAÇÕES WEB (WAF)

4.7.1. Throughput mínimo para HTTP de 240 Mbps;
4.7.2. Mínimo de 4 interfaces de 1Gbps RJ-45;
4.7.3. Mínimo de 4 interfaces de 1Gbps SFP;
4.7.4. Mínimo de 2 portas USB;
4.7.5. Deve possuir disco (storage), de no mínimo 460 GB SSD.

- FUNCIONALIDADES GERAIS -

4.7.6. Solução deve ser do tipo appliance físico.
4.7.7. Cada equipamento deve possuir software específico, destinado a finalidade de Firewall de Aplicação Web (WAF – Web Application Firewall), bem como as licenças necessárias para o seu funcionamento e proteção de servidores e aplicações Web.
4.7.8. O sistema proposto deve ser formado por software e hardware do mesmo fabricante.
Possuir porta de console RS-232 ou RJ45, para acesso à interface de linha de comando do appliance.

- FUNCIONALIDADES DE REDE -

4.7.9. Possuir LEDs para a indicação do status e atividade das interfaces;
4.7.10. A solução deve ser capaz de ser implementada no modo Proxy (Transparente e Reverso), Passivo e Inline Transparente (Bridge);
4.7.11. A solução deve ser capaz de ser implementada com protocolo WCCP
4.7.12. Suportar VLANs no padrão IEEE 802.1q;
4.7.13. Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP) - IEEE 802.3ad;
4.7.14. Suportar endereçamento IPv4 e IPv6 nas interfaces físicas e virtuais (VLANs);
4.7.15. A solução deve suportar cluster de alta disponibilidade entre dois dispositivos no modo Ativo-Passivo e Ativo-Ativo, para que quando o principal falhar o tráfego possa continuar sendo processado;
4.7.16. A solução deve suportar a sincronização de configuração entre dois appliances iguais, com o objetivo de operar no modo ativo-ativo, com a distribuição de tráfego sendo realizada por balanceador de carga externo ou pela própria solução.
4.7.17. A solução deve suportar roteamento por política (policy route).

- FUNCIONALIDADES DE GERÊNCIA -

4.7.18. O sistema operacional / firmware deve suportar interface gráfica web para a configuração das funções do sistema operacional, utilizando navegadores disponíveis gratuitamente e protocolo HTTPS, e através de CLI (interface de linha de comando), acessando localmente, via porta de console, ou remotamente via SSH;
4.7.19. Deve possuir administração baseada em interface web HTTP;
4.7.20. Deve possuir administração baseada em interface de linha de comando via Telnet;
4.7.21. Possuir auto-complementação de comandos na CLI;
4.7.22. Possuir ajuda contextual na CLI;
4.7.23. A solução deve possuir um Dashboard com informações sobre o sistema (Informações do Cluster, hostname, número de série, modo de operação, tempo em serviço, versão do firmware);
4.7.24. Deverá ser possível visualizar através da interface gráfica de gerência informações de licenças, assinaturas e contrato de suporte;
4.7.25. A solução ofertada deverá possuir acesso à linha de comando CLI via interface gráfica de gerência;
4.7.26. Deve prover, na interface de gerência, as seguintes informações do sistema para cada gateway: consumo de CPU e estatísticas das conexões;
4.7.27. Deve ser possível visualizar na interface de gerência as informações de consumo de memória;
4.7.28. Deve ser possível visualizar na interface de gerência as informações de utilização de disco de log;
4.7.29. Deverá possuir ferramenta, na interface gráfica de gerência (dashboard) que permita visualizar os últimos logs de ataque detectados/bloqueados;
4.7.30. Deve prover as seguintes informações, na interface de gráfica de gerência: estatísticas de Throughput HTTP em tempo real, estatísticas dos eventos de ataque detectados/bloqueados, estatísticas de requisições HTTP em tempo real e últimos logs de eventos do sistema;
4.7.31. Possuir na interface gráfica estatísticas de conexões concorrentes e por segundo, de políticas de segurança do sistema;
4.7.32. Possuir um painel de visualização com informações das interfaces de rede do sistema;
4.7.33. A configuração de administração da solução deve possibilitar a utilização de perfis;
4.7.34. Deve ser possível executar e restaurar backup via interface Web (GUI);
4.7.35. Deve ter a opção para criptografar o backup utilizando algoritmo AES 128-bit ou superior;
4.7.36. Deve ser possível executar e restaurar backup utilizando-se FTP;
4.7.37. Deve ser possível instalar um firmware alternativo em disco e inicializá-lo em caso de falha do firmware principal;
4.7.38. Deve ter suporte ao protocolo de monitoração SNMP v1, SNMP v2c e SNMP v3;
4.7.39. Deve ser capaz de realizar notificações de eventos de segurança através de e-mail, traps SNMP e Syslog;
4.7.40. A solução deverá ter a capacidade de armazenar logs localmente em disco e em servidor externo via protocolo SYSLOG;

4.7.41. A solução deve ter a capacidade de enviar alertas por email de eventos baseados em severidades e/ou categorias;
4.7.42. A solução deve possuir dados analíticos contendo localização geográfica dos clientes web;
4.7.43. A solução deve possuir dados analíticos, sendo possível visualizar a contagem total de ataques e percentual de cada país de origem, o volume total de tráfego em bytes e percentual de cada país de origem e o total de acessos (hits) e percentual de cada país de origem;
4.7.44. Deverá ter a capacidade de gerar relatórios detalhados baseados em tráfego/acessos/atividades do usuário;
4.7.45. Deve ter suporte a RESTful API para gerenciamento de configurações

- FUNCIONALIDADES DE AUTENTICAÇÃO -

4.7.46. Os usuários devem ser capazes de autenticar através do cabeçalho de autorização HTTP / HTTPS;
4.7.47. Os usuários devem ser capazes de autenticar através de formulários HTML embutidos;
4.7.48. A solução deverá ser capaz de autenticar usuários através de certificados digitais pessoais;
4.7.49. Deve possuir base local para armazenamento e autenticação contas de usuários;
4.7.50. A solução deve ter a capacidade de autenticar usuários em bases externas/remotas LDAP e RADIUS;
4.7.51. Os usuários devem ser capazes de autenticar através de contas de usuários em base remota NTLM;
4.7.52. A solução deve ser capaz de criar grupos de usuários para acessos semelhantes na autenticação;

- CERTIFICAÇÕES -

4.7.53. A solução deve suportar o modelo de segurança positiva definido pelo OWASP, pelo menos o que consta no TOP 10;

- FUNCIONALIDADES DE WEB APPLICATION FIREWALL -

4.7.54. Possuir mecanismo de aprendizado automático capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários e o que se espera de cada campo;
4.7.55. O perfil aprendido de forma automatizada pode ser ajustado e editado;
4.7.56. A solução deve possuir geração de relatório com as informações obtidas em auto-aprendizagem, com as estatísticas e as políticas de tráfego coletados, os relatórios de ataques, eventos e relatórios de verificação de vulnerabilidade para fins de cumprimento das regulamentações
4.7.57. Ter a capacidade de criação de assinaturas de ataque customizáveis;
4.7.58. Ter a capacidade de proteção para ataques do tipo Adobe Flash binary (AMF) protocol;
4.7.59. Ter a capacidade de proteção para ataques do tipo Botnet;
4.7.60. Ter a capacidade de proteção para ataques do tipo Browser Exploit Against SSL/TLS (BEAST);

4.7.61. A solução deverá possuir funcionalidade de proteção positiva contra ataques como acesso por força bruta;
4.7.62. Deve suportar detecção a ataques de Clickjacking
4.7.63. Deve suportar detecção a ataques de alteração de cookie;
4.7.64. Identificar e prevenir ataques do tipo Credit Cart Theft;
4.7.65. Identificar e prevenir ataque Cross Site Request Forgery (CSRF);
4.7.66. A solução deverá possuir funcionalidade de proteção positiva contra ataques como cross site scripting (XSS);
4.7.67. Deve possuir proteção contra ataques de Denial of Service (DoS);
4.7.68. Ter a capacidade de proteção para ataques do tipo HTTP header overflow;
4.7.69. Ter a capacidade de proteção para ataques do tipo Local File inclusion (FLI);
4.7.70. Ter a capacidade de proteção para ataques do tipo Man-in-the0middle (MITM);
4.7.71. Ter a capacidade de proteção para ataques do tipo Remote File Inclusion (RFI);
4.7.72. Ter a capacidade de proteção para ataques do tipo Server Information Leakage;
4.7.73. Proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection);
4.7.74. Ter a capacidade de proteção para ataques do tipo Malformed XML;
4.7.75. Identificar e prevenir ataques do tipo Low-rate DoS;
4.7.76. Prevenção contra Slow POST attack;
4.7.77. Proteger contra ataques Slowloris;
4.7.78. Ter a capacidade de proteção para ataques do tipo SYN flood;
4.7.79. Ter a capacidade de proteção para ataques do tipo Forms Tampering;
4.7.80. A solução deverá possuir funcionalidade de proteção positiva contra ataques de manipulação de campo escondido
4.7.81. Ter a capacidade de proteção para ataques do tipo Directory Traversal;
4.7.82. Ter a capacidade de proteção do tipo Access Rate Control;
4.7.83. Reconhecer e remediar Zero Day Attacks;
4.7.84. Ter a habilidade de configurar proteção do tipo TCP SYN flood-style para prevenção de DoS para qualquer política, através de Syn Cookie e Half Open Threshold;
4.7.85. Permitir configurar regras de bloqueio a métodos HTTP indesejados;
4.7.86. Permitir que sejam configuradas regras de limite de upload por tamanho de arquivo;
4.7.87. Deve permitir que o administrador bloqueie o tráfego de entrada e/ou tráfego de saída com base nos países, sem a necessidade de gerir manualmente os ranges de endereços IP correspondentes a cada país;
4.7.88. Deve suportar a criação de políticas por geo-localização, permitindo que o tráfego de determinado país seja bloqueado;
4.7.89. Permitir configurar listas negras de bloqueio e listas brancas de confiança, baseadas em endereço IP de origem;
4.7.90. Permitir a liberação temporária ou definitiva (white-list) de endereços IP bloqueados por terem originados ataques detectados pela solução;
4.7.91. Deve permitir adicionar, automaticamente ou manualmente, em uma lista de bloqueio, os endereços IP de origem, de acordo com a base de IP Reputation;
4.7.92. Ter a capacidade de Prevenção ao Vazamento de Informações (DLP), bloqueando o vazamento de informações de cabeçalho HTTP;

4.7.93. Ter a capacidade de investigar e analisar todo o tráfego HTTP para atestar se está em conformidade com a respectiva RFC, bloqueando ataques e tráfego em não-conformidade;
4.7.94. Deverá ser capaz de fazer aceleração de SSL, onde os certificados digitais são instalados na solução e as requisições HTTP são enviadas aos servidores sem criptografia;
4.7.95. A solução deve ser capaz de funcionar como Terminador de sessões SSL para a aceleração de tráfego;
4.7.96. Para SSL/TLS offload suportar no mínimo SSL 3.0, TLS 1.0, 1.1 e 1.2;
4.7.97. A solução deve ter a capacidade de armazenar certificados digitais de CA's;
4.7.98. A solução deve ser capaz de gerar CSR para ser assinado por uma CA;
4.7.99. A solução deve ser capaz de validar os certificados que são válidos e não foram revogados por uma lista de certificados revogados (CRL);
4.7.100. A solução deve conter as assinaturas de robôs conhecidos como link checkers, indexadores de web, search engines, spiders e web crawlers que podem ser colocados nos perfis de controle de acesso, bem como resetar tais conexões;
4.7.101. A solução deve ter um sistema de reputação de endereços IP públicos conhecidos como fontes de ataques DDoS, botnets, spammers, etc. Tal sistema deve ser atualizado automaticamente;
4.7.102. A solução deverá ser capaz de limitar o total de conexões permitidas para cada servidor real de um pool de servidores;
4.7.103. A solução deve permitir a customização ou redirecionar solicitações e respostas HTTP no HTTP Host, Request URL HTTP, HTTP Referer, HTTP Body e HTTP Location;
4.7.104. A solução deve permitir criar regras definindo a ordem em que as páginas devem ser acessados para prevenir ataques como cross-site request forgery (CSRF);
4.7.105. A solução deve ter a capacidade de definir restrições a métodos HTTP;
4.7.106. A solução deve ter a capacidade de proteger contra a detecção de campos ocultos;
4.7.107. Permitir que sejam criadas assinaturas customizadas de ataques e DLP, através de expressões regulares;
4.7.108. Deve gerar perfil de proteção automaticamente a partir de relatório em formato XML gerado por scanner de vulnerabilidade de terceiros;
4.7.109. Deverá ser capaz de fazer compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;
4.7.110. Suportar redireção e reescrita de requisições e respostas HTTP;
4.7.111. Permitir redirecionar requisições HTTP para HTTPS;
4.7.112. Permitir reescrever a linha URL no cabeçalho de uma requisição HTTP;
4.7.113. Permitir reescrever o campo "Host:" no cabeçalho de uma requisição HTTP;
4.7.114. Permitir reescrever o campo "Referer:" no cabeçalho de uma requisição HTTP;
4.7.115. Permitir redirecionar requisições para outro web site;
4.7.116. Permitir enviar resposta HTTP 403 Forbidden para requisições HTTP;
4.7.117. Permitir reescrever o parâmetro "Location:" no cabeçalho HTTP de uma resposta de redireção HTTP de um servidor web;
4.7.118. Permitir reescrever o corpo ("body") de uma resposta HTTP de um servidor web;
4.7.119. Permitir adicionar o campo X-Forwarded-For para identificação do endereço real do cliente quando no modo de proxy reverso;

4.7.120. A solução deve suportar regras para definir se as solicitações HTTP serão aceitas com base na URL e a origem do pedido e, se necessário, aplicar uma taxa específica de transferência (rate limit);
4.7.121. A solução deve suportar o mecanismo de combinação de controle de acesso e autenticação utilizando mecanismos como HTML Form, Basic e Suporte a SSO, métodos como LDAP e RADIUS para consultas e integração dos usuários da aplicação;
4.7.122. Possuir capacidade de caching para aceleração web;
4.7.123. Deve permitir ao Administrador a criação de novas assinaturas e/ou alteração de assinaturas já existentes;

- FUNCIONALIDADES DE BALANCEAMENTO DE CARGA -

4.7.124. A solução deve incluir funcionalidade de balanceamento de carga entre servidores web;
4.7.125. Deve ter a habilidade de configurar portas não-padrão para aplicação web HTTP e HTTPS;
4.7.126. Ter a capacidade de balancear/distribuir tráfego e rotear o conteúdo através de vários servidores web;
4.7.127. A solução deve permitir criar grupos de servidores (Server Farm / Pool) para distribuir as conexões dos usuários;
4.7.128. Suportar algoritmo Round Robind para balanceamento de carga de servidores;
4.7.129. Suportar algoritmo Weighted Round Robind para balanceamento de carga de servidores;
4.7.130. Suportar algoritmo Least Connections para balanceamento de carga de servidores;
4.7.131. A solução deve ser capaz de criar servidores virtuais que definem a interface de rede/bridge e endereço IP por onde o tráfego destinado ao Server Pool é recebido;
4.7.132. Os servidores virtuais devem entregar o tráfego à um único servidor web e também possuir a opção de distribuir as sessões/conexões entre os servidores web do Server Pool;
4.7.133. Deve ser possível especificar o número máximo de conexões TCP simultâneas para um determinado servidor membro do Server Pool;
4.7.134. Permitir teste de disponibilidade de servidor web através do método TCP;
4.7.135. Permitir teste de disponibilidade de servidor web através do método ICMP ECHO_REQUEST (ping)
4.7.136. Permitir teste de disponibilidade de servidor web através do método TCP Half Open;
4.7.137. Permitir teste de disponibilidade de servidor web através do método TCP SSL;
4.7.138. Permitir teste de disponibilidade de servidor web através do método HTTP;
4.7.139. Permitir teste de disponibilidade de servidor web através do método HTTPS;
4.7.140. Nos testes de disponibilidade HTTP e HTTPS, permitir indicar a URL exata a ser testada;
4.7.141. Nos testes de disponibilidade HTTP e HTTPS, permitir escolher entre os métodos HEAD, GET e POST;
4.7.142. Nos testes de disponibilidade HTTP e HTTPS, permitir indicar o nome do campo HTTP "host" a ser testado;

4.7.143. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Host";
4.7.144. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "URL";
4.7.145. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Parâmetro HTTP";
4.7.146. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Referer";
4.7.147. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Endereço IP de Origem";
4.7.148. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Cabeçalho";
4.7.149. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Cookie";
4.7.150. Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Valor de campo do Certificado X509";
4.7.151. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por endereço IP de origem;
4.7.152. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência analisando qualquer parâmetro do header HTTP;
4.7.153. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência analisando a URL acessada;
4.7.154. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por cookie – método cookie insert e cookie rewrite;
4.7.155. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em Reescrita de Cookie;
4.7.156. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em Cookie Persistente;
4.7.157. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em ASP Session ID;
4.7.158. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em PHP Session ID;
4.7.159. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em JSP Session ID;
4.7.160. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por sessão SSL;

4.8. SERVIÇOS DE IMPLANTAÇÃO PARA SOLUÇÃO DE SEGURANÇA E GERÊNCIA DE REDES NGFW EM CLUSTER DE ALTA DISPONIBILIDADE

4.8.1. Os serviços envolvendo a execução de atividade de rotinas de implantação deverão ser prestados de maneira a apoiar os processos de trabalho e atividades pontuais para atender a necessidades específicas apresentadas pela CONTRATANTE.

4.8.2. Os serviços envolverão todas as atividades de implantação, configurações, programações e atendimento às demandas apresentadas pela CONTRATANTE.

4.8.3. A execução do Contrato deverá seguir metodologia de trabalho baseado no conceito de Delegação de Responsabilidade Supervisionada. À CONTRATANTE caberá a responsabilidade de definir demandas, bem como realizar a gestão qualitativa dos serviços. A CONTRATADA deverá disponibilizar um Gerente do Projeto, o qual deverá supervisionar todas as atividades dos profissionais vinculados à dedicação exclusiva. Ao Gerente do Projeto será atribuída a responsabilidades de desenvolvimento e acompanhamento de todo plano de trabalho às atividades demandadas pela CONTRATANTE.

4.8.4. Os serviços deverão ser realizados nas dependências do CONTRATANTE, utilizando-se de equipamentos e infraestrutura com capacidade operacional.

4.8.5. Os serviços deverão ser realizados por profissionais detentores de diplomas de nível superior em áreas afins da Tecnologia da Informação, com experiência comprovada mínima de 03 (três) anos em implantação, operação e suporte de dispositivos de Segurança da Informação, com características similares às apresentadas pela CONTRATANTE.

4.8.6. Os profissionais deverão receber todas as demandas sob as responsabilidades apresentadas pela CONTRATANTE, providenciando sua inspeção, conferência, classificação e prestação de contas.

4.8.7. Os profissionais deverão tomar ciência e analisar detalhadamente os projetos, bem como todos os documentos que o complementarem, fornecidos pela CONTRATANTE.

4.8.8. Deve ser realizado o desenvolvimento de plano de implementação; planejamento; análise; configuração; integração; migração; testes de verificação; ajustes; otimização; troubleshooting; updates; upgrades; ensaios de contingência; criação de regras de segurança;

4.8.9. Deve ser realizado definição da arquitetura lógica e física do projeto, garantindo a qualidade durante a implantação e o atendimento de todos os requisitos funcionais e não funcionais;

4.8.10. Deve ser realizado gerenciamento de projetos: gerenciamento do projeto propriamente dito, considerando controle de prazos, esforço, elaboração de relatórios de posicionamento executivo, indicadores do projeto e qualquer outra métrica prevista no PMBOOK. O objetivo de todas estas atividades é a garantia de qualidade do projeto no que tange prazos e esforço.

4.9. SERVIÇOS DE IMPLANTAÇÃO E CONFIGURAÇÃO PARA SOLUÇÃO DE SEGURANÇA E GERENCIA DE REDES NGFW TIPOS "2" E "3"

4.9.1. Os serviços envolvendo a execução de atividade de rotinas de implantação deverão ser prestados de maneira a apoiar os processos de trabalho e atividades

pontuais para atender a necessidades específicas apresentadas pela CONTRATANTE

4.9.2. Os serviços envolverão todas as atividades de implantação, configurações, programações e atendimento às demandas apresentadas pela CONTRATANTE.

4.9.3. A execução do Contrato deverá seguir metodologia de trabalho baseado no conceito de Delegação de Responsabilidade Supervisionada. À CONTRATANTE caberá a responsabilidade de definir demandas, bem como realizar a gestão qualitativa dos serviços. A CONTRATADA deverá disponibilizar um Gerente do Projeto, o qual deverá supervisionar todas as atividades dos profissionais vinculados à dedicação exclusiva. Ao Gerente do Projeto será atribuída a responsabilidades de desenvolvimento e acompanhamento de todo plano de trabalho às atividades demandadas pela CONTRATANTE.

4.9.4. Os serviços poderão ser realizados nas dependências da CONTRATANTE ou realizados de forma remota e assistida pela equipe de TI da CONTRATANTE.

4.9.5. Os serviços deverão ser realizados por profissionais, detentores de diplomas de nível superior em áreas afins da Tecnologia da Informação, com experiência comprovada mínima de 03 (três) anos em implantação, operação e suporte de dispositivos de Segurança da Informação, com características similares às apresentadas pela CONTRATANTE.

4.9.6. Os profissionais deverão receber todas as demandas sob as responsabilidades apresentadas pela CONTRATANTE, providenciando sua inspeção, conferência, classificação e prestação de contas.

4.9.7. Os profissionais deverão tomar ciência e analisar detalhadamente os projetos, bem como todos os documentos que o complementarem, fornecidos pela CONTRATANTE.

4.9.8. Deve ser realizado o desenvolvimento de plano de implementação; planejamento; análise; configuração; integração; migração; testes de verificação; ajustes; otimização; troubleshooting; updates; upgrades; ensaios de contingência; criação de regras de segurança;

4.9.9. Deve ser realizado definição da arquitetura lógica e física do projeto, garantindo a qualidade durante a implantação e o atendimento de todos os requisitos funcionais e não funcionais;

4.10. SERVIÇOS DE IMPLANTAÇÃO E CONFIGURAÇÃO DE UNIDADE CENTRALIZADA DE ARMAZENAMENTO DE LOGS E RELATORIA.

4.10.1. Os serviços envolvendo a execução de atividade de rotinas de implantação deverão ser prestados de maneira a apoiar os processos de trabalho e atividades pontuais para atender a necessidades específicas apresentadas pela CONTRATANTE

4.10.2. Os serviços envolverão todas as atividades de implantação, configurações, programações e atendimento às demandas apresentadas pela CONTRATANTE.

4.10.3. A execução do Contrato deverá seguir metodologia de trabalho baseado no conceito de Delegação de Responsabilidade Supervisionada. À CONTRATANTE caberá a responsabilidade de definir demandas, bem como realizar a gestão qualitativa dos serviços. A CONTRATADA deverá disponibilizar um Gerente do Projeto, o qual deverá supervisionar todas as atividades dos profissionais

vinculados à dedicação exclusiva. Ao Gerente do Projeto será atribuída a responsabilidades de desenvolvimento e acompanhamento de todo plano de trabalho às atividades demandadas pela CONTRATANTE.

4.10.4. Os serviços deverão ser realizados nas dependências do CONTRATANTE, utilizando-se de equipamentos e infraestrutura com capacidade operacional.

4.10.5. Os serviços deverão ser realizados por profissionais, detentores de diplomas de nível superior em áreas afins da Tecnologia da Informação, com experiência comprovada mínima de 03 (três) anos em implantação, operação e suporte de dispositivos de Segurança da Informação, com características similares às apresentadas pela CONTRATANTE.

4.10.6. Os profissionais deverão receber todas as demandas sob as responsabilidades apresentadas pela CONTRATANTE, providenciando sua inspeção, conferência, classificação e prestação de contas.

4.10.7. Os profissionais deverão tomar ciência e analisar detalhadamente os projetos, bem como todos os documentos que o complementarem, fornecidos pela CONTRATANTE.

4.11. SERVIÇOS DE IMPLANTAÇÃO E CONFIGURAÇÃO DE UNIDADE DE GERENCIA CENTRALIZADA DE EQUIPAMENTOS.

4.11.1. Os serviços envolvendo a execução de atividade de rotinas de implantação deverão ser prestados de maneira a apoiar os processos de trabalho e atividades pontuais para atender a necessidades específicas apresentadas pela CONTRATANTE

4.11.2. Os serviços envolverão todas as atividades de implantação, configurações, programações e atendimento às demandas apresentadas pela CONTRATANTE.

4.11.3. A execução do Contrato deverá seguir metodologia de trabalho baseado no conceito de Delegação de Responsabilidade Supervisionada. À CONTRATANTE caberá a responsabilidade de definir demandas, bem como realizar a gestão qualitativa dos serviços. A CONTRATADA deverá disponibilizar um Gerente do Projeto, o qual deverá supervisionar todas as atividades dos profissionais vinculados à dedicação exclusiva. Ao Gerente do Projeto será atribuída a responsabilidades de desenvolvimento e acompanhamento de todo plano de trabalho às atividades demandadas pela CONTRATANTE.

4.11.4. Os serviços poderão ser realizados nas dependências da CONTRATANTE ou realizados de forma remota e assistida pela equipe de TI da CONTRATANTE.

4.11.5. Os serviços deverão ser realizados por profissionais, detentores de diplomas de nível superior em áreas afins da Tecnologia da Informação, com experiência comprovada mínima de 03 (três) anos em implantação, operação e suporte de dispositivos de Segurança da Informação, com características similares às apresentadas pela CONTRATANTE.

4.11.6. Os profissionais deverão receber todas as demandas sob as responsabilidades apresentadas pela CONTRATANTE, providenciando sua inspeção, conferência, classificação e prestação de contas.

4.11.7. Os profissionais deverão tomar ciência e analisar detalhadamente os projetos, bem como todos os documentos que o complementarem, fornecidos pela CONTRATANTE.

4.12. SERVIÇOS DE IMPLANTAÇÃO E CONFIGURAÇÃO DOS ATIVOS DE REDE WIRELESS INDOOR

4.12.1. Os serviços envolvendo a execução de atividade de rotinas de implantação deverão ser prestados de maneira a apoiar os processos de trabalho e atividades pontuais para atender a necessidades específicas apresentadas pela CONTRATANTE

4.12.2. Os serviços envolverão todas as atividades de configurações, programações e atendimento às demandas apresentadas pela CONTRATANTE.

4.12.3. A execução do Contrato deverá seguir metodologia de trabalho baseado no conceito de Delegação de Responsabilidade Supervisionada. À CONTRATANTE caberá a responsabilidade de definir demandas, bem como realizar a gestão qualitativa dos serviços. A CONTRATADA deverá disponibilizar um Gerente do Projeto, o qual deverá supervisionar todas as atividades dos profissionais vinculados à dedicação exclusiva. Ao Gerente do Projeto será atribuída a responsabilidades de desenvolvimento e acompanhamento de todo plano de trabalho às atividades demandadas pela CONTRATANTE.

4.12.4. Os serviços poderão ser realizados nas dependências da CONTRATANTE ou realizados de forma remota e assistida pela equipe de TI da CONTRATANTE.

4.12.5. Os serviços deverão ser realizados por profissionais, detentores de diplomas de nível superior em áreas afins da Tecnologia da Informação, com experiência comprovada mínima de 03 (três) anos em implantação, operação e suporte de dispositivos de Segurança da Informação, com características similares às apresentadas pela CONTRATANTE.

4.12.6. Os profissionais deverão receber todas as demandas sob as responsabilidades apresentadas pela CONTRATANTE, providenciando sua inspeção, conferência, classificação e prestação de contas.

4.12.7. Os profissionais deverão tomar ciência e analisar detalhadamente os projetos, bem como todos os documentos que o complementarem, fornecidos pela CONTRATANTE.

4.13. SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO DE SEGURANÇA WAF

4.13.1. Os serviços envolverão todas as atividades de implantação, configurações, programações e atendimento às demandas apresentadas pela CONTRATANTE.

4.13.2. Os serviços deverão ser realizados nas dependências do CONTRATANTE, utilizando-se de equipamentos e infraestrutura com capacidade operacional.

4.13.3. Os serviços deverão ser realizados por profissionais com experiência comprovada mínima de 03 (três) anos em implantação, operação e suporte de dispositivos de Segurança da Informação, com características similares às apresentadas pela CONTRATANTE.

4.13.4. Os profissionais deverão receber todas as demandas sob as responsabilidades apresentadas pela CONTRATANTE, providenciando sua inspeção, conferência, classificação e prestação de contas.

4.13.5. Os profissionais deverão tomar ciência e analisar detalhadamente os projetos, bem como todos os documentos que o complementarem, fornecidos pela CONTRATANTE.

4.13.6. A instalação e configuração da solução deverá ser realizada de acordo com o horário de funcionamento do DPE/BA, de segunda à sexta-feira, das 8:30 às 18:00h, em horário e dias a serem combinados entre o DPE/BA e a contratada;

4.13.7. Deve ser realizado o desenvolvimento de plano de implementação; planejamento; análise; configuração; integração; migração; testes de verificação; ajustes; otimização; troubleshooting; updates; upgrades; ensaios de contingência; criação de regras de segurança;

4.13.8. Deve ser realizado definição da arquitetura lógica e física do projeto, garantindo a qualidade durante a implantação e o atendimento de todos os requisitos funcionais e não funcionais;

4.13.9 Deverá ser oferecido treinamento hands-on da solução implantada, com o mínimo de 16 (dezesseis) horas, em dias úteis, nas instalações da contratante, para no mínimo 2 (dois) técnicos do DPE/BA;

5. CONDIÇÕES DO FORNECIMENTO

5.1. Todos os equipamentos a serem fornecidos deverão ser novos, estar em linha de produção e fabricação atual do fabricante, não se encontrando nas fases de "End of Sale", "End of Support" ou qualquer outra que indique que já está na direção descendente de seu ciclo de vida.

5.2. A CONTRATADA deverá entregar, às suas expensas, todos os itens acessórios de hardware necessários à perfeita instalação e funcionamento dos equipamentos, incluindo conectores, cabos, suportes e demais itens necessários para instalação e funcionamento da solução contratada, em plena compatibilidade com as especificações constantes neste Termo de Referência e recomendadas pelo fabricante.

5.3. Todos os equipamentos fornecidos e seus componentes deverão ser novos, de primeiro uso e devem estar acondicionados adequadamente em caixa original lacrados de fábrica, de forma a propiciar completa segurança durante e transporte.

5.4. Toda a solução e suas implantações serão supervisionadas pela Defensoria Pública.

5.5. A CONTRATADA será responsável por projetar, instalar, configurar e dar suporte na solução ofertada durante todo o período de licenciamento e garantia das licenças.

5.6. A implementação das políticas de segurança será de responsabilidade exclusiva da CONTRATADA mediante determinações da CONTRATANTE.

6. PARCELAMENTO E ADJUDICAÇÃO DO OBJETO

6.1. Não haverá parcelamento, cada ordem de fornecimento derivado do Registro de Preços deverá ser realizada de maneira integral.

6.2. A proposta deve contemplar o fornecimento de todos os insumos de Hardware, Software, Subscrições dos Fabricantes nos principais componentes e subcomponentes que os integram objetivando garantir a total conectividade e interoperabilidade entre seus componentes, que deverão resultar na prestação dos serviços com níveis de desempenho adequados aos fins a que se destinam e desta forma a adjudicação será por lote.

7. OBRIGAÇÕES DA CONTRATANTE

7.1. Atestar as notas fiscais/faturas, por servidor/comissão competente, emitidas pela Contratada, recusando-as quando inexatas ou incorretas, efetuando todos os pagamentos nas condições pactuadas, pós o recebimento definitivo;

7.2. Acompanhar e fiscalizar a execução do objeto da Ata de Registro de Preços e do(s) contrato(s) dela decorrentes, por meio de servidor(es) designado(s), de modo a garantir o fiel cumprimento do mesmo e da proposta;

7.3. Proporcionar todas as facilidades indispensáveis à boa execução das obrigações contratuais;

7.4. Aplicar as sanções conforme previsto no contrato, assegurando à Contratada o contraditório e ampla defesa.

8. OBRIGAÇÕES DA CONTRATADA

8.1. Fornecer o(s) equipamento(s) conforme especificações, quantidades, prazos e demais condições estabelecidas no Edital, na Ata de Registro de Preços, na Ordem de Fornecimento, na Proposta e no Contrato;

8.2. Fornecer a documentação necessária à instalação e à operação dos produtos (manuais, termos de garantia, etc.), completa, atualizada e em português do Brasil, caso exista, ou em inglês;

8.3. Disponibilizar Central de Atendimento para a abertura e fechamento de chamados técnicos, conforme períodos, horários e condições estabelecidas no Edital e em seus Anexos;

8.4. Comunicar formal e imediatamente ao Gestor ou Responsável Técnico da Administração sobre mudanças nos dados para contato com a Central de Atendimento;

8.5. Prestar as informações e os esclarecimentos que venham a ser solicitados pelo representante da Administração, referentes a qualquer problema detectado ou ao andamento de atividades da garantia;

8.6. Comunicar imediatamente ocorrências de qualquer natureza que impeçam o bom andamento do serviço;

8.7. Responder por quaisquer prejuízos que seus profissionais causarem ao patrimônio da Administração ou a terceiros, por ocasião da execução do objeto, procedendo imediatamente aos reparos ou às indenizações cabíveis e assumindo o ônus decorrente;

8.8. Responsabilizar-se integralmente pelo fornecimento dos equipamentos e pela execução dos serviços de garantia técnica, primando pela qualidade, desempenho, eficiência e produtividade na execução dos trabalhos, dentro dos prazos estipulados e cujo descumprimento será considerado infração passível de aplicação das penalidades previstas neste Termo de Referência;

8.9. Comunicar ao Gestor ou Responsável Técnico, formal e imediatamente, todas as ocorrências anormais e/ou que possam comprometer a execução do objeto;

8.10. Manter sigilo sobre todo e qualquer assunto de interesse da Administração ou de terceiros de que tomar conhecimento em razão da execução do objeto, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros pertinentes, sob pena de responsabilidade civil, penal e administrativa;

8.11 Cumprir e garantir que seus profissionais estejam cientes, aderentes e obedeçam rigorosamente às normas e aos procedimentos estabelecidos na Política de Segurança da Informação da DPE/BA;

8.12 Responsabilizar-se pela conservação dos ambientes onde desempenhe as atividades necessárias para prestar, se for o caso;

8.13 Prestar as informações e os esclarecimentos que venham a ser solicitados pela Administração, referentes a qualquer problema detectado ou ao andamento de atividades da garantia técnica;

8.14 Responsabilizar-se por todas as despesas de instalação inicial, suporte técnico remoto bem como deslocamento dos seus técnicos ao local da instalação e manutenção dos equipamentos, seja para retirada e/ou entrega, incluindo todas as despesas de transporte, frete e seguro correspondentes;

8.15 A contratada não poderá transferir a outrem os compromissos assumidos, no todo ou em parte dos serviços objeto desta contratação;

8.16 Assegurar a correta integração e funcionalidade dos serviços, em função do projeto e das especificações técnicas constantes neste Termo de Referência;

8.17 Arcar com todas as despesas, diretas ou indiretas, decorrente do cumprimento das obrigações assumidas sem qualquer ônus a DPE/BA;

8.18 Responsabilizar-se integralmente com todas as despesas inerentes à execução dos serviços, tais como, combustíveis, manutenção, seguros, taxas, impostos, tributos e salários;

8.19 Zelar pela boa e completa execução dos serviços e facilitar, por todos os meios ao seu alcance, a ampla ação fiscalizadora dos prepostos designados pela DPE/BA, atendendo prontamente às observações e exigências que lhe forem solicitadas.

9. DA GARANTIA E DA ASSISTÊNCIA TÉCNICA

9.1. Todos os componentes de hardware e software, deverão possuir garantia de, no mínimo, 60 (sessenta) meses, com suporte técnico de 8 (oito) horas por dia, 5 (cinco) dias por semana, na cidade de Salvador (BA).

9.2. O serviço deverá ser prestado por profissional de nível superior, devidamente certificado nas soluções tecnológicas utilizadas na prestação dos serviços contratados.

9.3. Durante o período de execução dos serviços, a CONTRATADA deverá garantir o funcionamento do software, com suporte técnico do FABRICANTE prestado em caso de falha.

9.4. Deverá ser garantida, neste prazo, a atualização de versões, releases, componentes (bibliotecas, filtros, dentre outros) e módulos dos softwares e equipamentos utilizados na prestação dos serviços.

10. SUPORTE TÉCNICO E ACORDO DE NÍVEL DE SERVIÇO

10.1. Atender às necessidades da DPE/BA para suporte técnico de todas as Soluções de Segurança da Informação que compõem esse termo de referência, compreendendo hardware e software, com o objetivo de proteger a rede corporativa e aumentar o nível de conformidade com a política de segurança.

10.2. Composta de técnicos certificados pelo fabricante do software fornecido, e preparada para dar todo o suporte técnico e ajuda necessária para maximizar os benefícios oferecidos pelo software, aumentando a sua performance.

10.3. O suporte técnico ao produto fornecido deverá ser através de contato Telefônico (telefone 0800 do fabricante ou telefone com numeração comum do fornecedor), Sitio de Internet (website do fabricante ou do fornecedor), Correio Eletrônico (e-mail do fabricante ou do fornecedor) ou no Local (provido pelo fabricante ou pelo fornecedor), em casos de grande emergência;

10.4. O suporte técnico deverá ser fornecido pelo fornecedor da solução de segurança ou pelo fabricante, no Brasil e na língua portuguesa;

10.5. Deverão ser executados pela empresa CONTRATADA serviços de Instalação e configuração para uso da solução CONTRATADA com supervisão da equipe técnica da DPE/BA;

10.6. Deverá ser executada pela empresa CONTRATADA uma análise da situação atual e elaborar, em conjunto com a equipe interna da DPE/BA, um plano de otimização de recursos, rotinas, procedimentos e processos para o novo ambiente de segurança. Essa documentação deverá ser entregue, pela empresa CONTRATADA, em formato digital;

10.7. A empresa CONTRATADA deverá preservar todo ambiente computacional existente, de forma a manter a integridade dos dados, aplicativos e sistemas operacionais em funcionamento;

10.8. A empresa CONTRATADA deverá preparar o ambiente de modo a operar conforme o estabelecido no plano de otimização de recursos, rotinas, procedimentos e processos;

10.9. A instalação e configuração da solução deverá ser realizada de acordo com o horário de funcionamento da DPE/BA, de segunda à sexta-feira, das 8:30 às 18:00h, em horário e dia a serem combinados entre a DPE/BA e a CONTRATADA;

10.10 Deverá ser oferecido treinamento hands-on de atualização tecnológica das soluções implantadas, com o mínimo de 16 (dezesseis) horas, em dias úteis, nas instalações da contratante, na cidade de Salvador, para no mínimo 2 (dois) técnicos da DPE/BA;

10.11 O treinamento ou hands-on deverá ser iniciado imediatamente após a instalação e configuração das licenças;

10.12 O prazo de execução dos serviços de Instalação e configuração para uso da solução de segurança no parque omputacional da DPE/BA deverá ser concluído em no máximo 45 (quarenta e cinco) dias consecutivos, a contar da data da entrega das licenças;

10.13 A empresa CONTRATADA deverá realizar duas avaliações on-site durante o período de vigência do contrato, perante solicitação da CONTRATANTE, do ambiente da DPE/BA, mediante verificação de instalações e configurações de toda a solução de segurança, adequando-as às melhores práticas, essa atividade deve gerar relatório para posterior melhoria pela equipe da DPE/BA;

10.14. O suporte técnico deverá ser prestado nas seguintes formas:

10.14.1. Plantão Telefônico, Website e E-mail - Serviço de uso ilimitado, no período de 8 (oito) horas por dia, 5 (cinco) dias por semana;

10.14.2. No Local (on site) - Serviço de uso ilimitado para atividades não solucionadas através de atendimento remoto, prestado em caso de emergência, ou outra necessidade maior e também compreendendo os seguintes tipos de atendimento local previstos: suporte para upgrade de versões e releases do software; solução de problemas detectados (troubleshoot); análise e correção de eventos relacionados à segurança e à performance do software e do ambiente; integração dos ambientes da configuração do software na rede da DPE/BA. Neste caso a CONTRATADA deve possuir plantão de 8 (oito) horas por dia, 5 (cinco) dias por semana, para este tipo de atendimento;

10.15 Para a execução do suporte técnico, a CONTRATADA deverá contar com equipe técnica certificada pelo fabricante e com suporte ilimitado (quantidade de chamados) ao centro de suporte mundial do fabricante a nível internacional, a fim de garantir transferência diretamente ao fabricante dos problemas de maior complexidade que não tenham sido resolvidos em seu próprio laboratório;

10.16 O encaminhamento de chamados deverá ser efetuado pelos técnicos responsáveis no prazo máximo conforme os níveis de severidade indicados no item 6. Após este prazo, em caso de não solução, a CONTRATADA deverá acionar o atendimento, no local designado pela DPE/BA, de acordo com o nível de serviço acordado. O suporte prestado pela empresa terá chamados ilimitados;

10.17 O atendimento no Local (on site) quando necessário deve ser provido nas unidades da DPE/BA, nos endereços informados no item 17.

10.18 A CONTRATADA deverá responder aos acionamentos, dentro dos prazos fixados no item 11, a partir da abertura do acionamento;

10.19 O término do atendimento deverá ocorrer dentro dos prazos fixados no item 11, a partir do contato do técnico da CONTRATADA, responsável pelo atendimento;

10.20 Entende-se por início do atendimento a hora do contato do técnico de suporte da CONTRATADA com a equipe da CONTRATANTE;

10.21 Entende-se por término de atendimento a disponibilidade do produto para uso em perfeitas condições de funcionamento no local onde está instalado;

10.22 O nível de severidade será informado pela CONTRATANTE no momento da abertura de cada chamado;

10.23 O nível de severidade poderá ser reclassificado a critério da CONTRATANTE. Caso isso ocorra haverá o início de nova contagem de prazo, conforme o novo nível de severidade;

10.24 Todas as solicitações de suporte técnico devem ser registradas pela CONTRATADA, para acompanhamento e controle da execução do serviço;

10.25 A CONTRATADA deverá apresentar relatório de atendimento para cada solicitação de suporte, contendo data e hora da solicitação de suporte técnico, do início e do término do atendimento, identificação do problema, providências adotadas e demais informações pertinentes;

10.26 O relatório de atendimento deverá ser assinado pelo servidor da CONTRATANTE que solicitou o suporte técnico;

10.27 Para a execução do atendimento, é necessária a autorização da CONTRATANTE para instalação ou desinstalação de quaisquer softwares ou equipamentos que não façam parte da solução de segurança fornecida.

10.28 Comprovação de Garantia: para assegurar a esta Instituição a garantia total solicitada e demais condições exigidas, será necessário comprovar por meio de documentação do FABRICANTE específica para este Processo licitatório, anexada à proposta comercial, que o equipamento ofertado terá garantia, mínima, de 5 (cinco) anos e tempo de atendimento exigidos no Edital.

11. ACORDO DE NÍVEL DE SERVIÇO (ANS)

11.1 A CONTRATADA deverá possuir Central de Atendimento (contato telefônico, sítio na Internet e e-mail) para consultas, aberturas de chamados técnicos e envio de arquivos para análise, durante 8 (oito) horas por dia, 5 (cinco) dias por semana;

11.2 A CONTRATADA deverá prestar serviços de suporte técnico 8 horas por dia, 5 dias por semana, relativos à prestação do serviço objeto deste Termo de Referência, sem ônus para a CONTRATANTE;

11.3 Para efeito dos atendimentos técnicos, a CONTRATADA deverá observar os níveis de severidade e respectivos prazos máximos fixados abaixo;

11.4 Todos os chamados, inclusive os que podem resultar em manutenção de natureza corretiva, bem como o fluxo de resolução de problemas, deverão ser documentados. Esta documentação, bem como outras geradas em processos de atendimento, auditorias, manutenção ou configurações, deverá ser entregue à CONTRATANTE através de relatórios (impressos ou em mídia digital) mediante solicitação.

11.5 A CONTRATADA deverá fazer análises dos chamados e enviar recomendações de possíveis treinamentos necessários ao desenvolvimento da equipe da CONTRATANTE.

11.6 A CONTRATADA deverá apresentar relatório contendo as ações adotadas para a solução do problema.

11.7 A CONTRATADA deverá disponibilizar à CONTRATANTE serviço de atendimento de um Gestor do contrato de Suporte, responsável este que será o ponto focal de todas as necessidades de suporte da CONTRATANTE para casos de escalações ou problemas de atendimento do Suporte Técnico. Caso a CONTRATADA tenha seus laboratórios em outros países que não seja o território nacional, o Gestor deverá ter fluência na língua para facilitar a comunicação entre as partes.

11.8 A CONTRATANTE permitirá o acesso dos técnicos credenciados pela CONTRATADA às instalações onde se encontrarem os equipamentos para a prestação dos serviços de manutenção. Entretanto, tais técnicos ficarão sujeitos às normas internas de segurança da CONTRATANTE, notadamente àquelas atinentes à identificação, trânsito e permanência nas dependências;

11.9 Mesmo se permitido pela CONTRATANTE, a permanência do técnico além do tempo de resolução do problema, para a continuidade de solução de um problema, não deverá representar qualquer ônus adicional à CONTRATANTE.

11.10 Níveis de Serviço e Tempo Esperados:

11.10.1. Plantão Telefônico por número 0800 como serviço de uso ilimitado, no período de 8 (oito) horas por dia, 5 (cinco) dias por semana;

11.10.2. No Local (on site) – Serviço de uso ilimitado para atividades não solucionadas através do atendimento remoto, prestado em caso de emergência, ou outra necessidade maior e também compreendendo os seguintes tipos de atendimento local: suporte para upgrade de versões e releases do software; solução de problemas detectados (troubleshoot); análise e correção de eventos relacionados à segurança e à performance do software e do ambiente; atualização simultânea nos ambientes dos órgãos e entidades da CONTRATANTE.

11.10.3. Para efeito dos atendimentos técnicos, a CONTRATADA deverá observar os níveis de severidade e respectivos prazos máximos fixados abaixo:

NÍVEIS DE SEVERIDADE DOS CHAMADOS	
Nível	**Descrição**
1	Serviços totalmente indisponíveis.
2	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso aos aplicativos.
3	Serviços disponíveis com ocorrência de alarmes de avisos, consultas sobre problemas, dúvidas gerais sobre o equipamento fornecido.

Tabela de Prazos de Atendimento ao Software

Modalidade	**Prazos**	**Níveis de Severidade**		
		1	**2**	**3**
On Site Salvador e RMS	Início atendimento	1 hora útil	2 horas úteis	24 horas úteis
	Término atendimento	2 horas úteis	4 horas úteis	72 horas úteis
On Site Interior do Estado da Bahia	Início atendimento	4 horas úteis	8 horas úteis	24 horas úteis
	Término atendimento	8 horas úteis	16 horas úteis	72 horas úteis

Tabela de Prazos de Atendimento ao Software				
Modalidade	**Prazos**	**Níveis de Severidade**		
		1	**2**	**3**
Telefone, email e web	Início atendimento	-	-	24 horas
	Término atendimento	-	-	72 horas

11.10.4. Todo o chamado somente será caracterizado como "encerrado" mediante concordância da Coordenação de Modernização e Informática;

11.10.5. Para as situações em que a solução definitiva de problemas no ambiente demande reimplantação, reestruturação ou reinstalação do produto, este deverá ser programado e planejado, com a antecedência necessária, de modo a não prejudicar a operação dos demais sistemas da CONTRATANTE.

11.11 A CONTRATADA deverá disponibilizar à CONTRATANTE um serviço preventivo de verificação e atualização de versões ou correções (patches) que se fizerem necessários, específicos para a solução ofertada, sem ônus para a CONTRATANTE;

11.12 No caso de necessidade de ações preventivas ou corretivas a CONTRATANTE agendará com antecedência junto a CONTRATADA as implementações das correções, fora do horário comercial, preferencialmente em feriados e finais de semana, sem ônus para a CONTRATANTE;

11.13 A CONTRATADA deverá prestar suporte a todos os componentes de software fornecidos que forem necessários para a implementação e utilização da solução, sem ônus para a CONTRATANTE durante 60 (sessenta) meses.

11.14 A CONTRATADA deverá ainda realizar os seguintes suportes proativos:

11.14.1. Duas avaliações on-site por ano do ambiente da CONTRATANTE, mediante verificação de instalações e configurações de toda a solução, adequando-as às melhores práticas de segurança, essa atividade deve gerar relatório para posterior melhoria pela equipe da CONTRATANTE.

11.14.2. Uma avaliação on-site por ano do ambiente da CONTRATANTE, mediante verificação de instalações e configurações de toda a solução de gerência centralizada, adequando-as às melhores práticas de segurança, essa atividade deve gerar relatório para posterior melhoria pela equipe da CONTRATANTE.

11.14.3. Quatro visitas técnicas on-site na unidade de Salvador, durante o ano de profissionais certificados pelo fabricante para apoiar nas implementações e nos controles gerados pelas ações proativas.

12. CRITÉRIOS OBRIGATÓRIOS

12.1. Atendimento da Assistência Técnica: Prazo de 60 (sessenta) meses com suporte fornecido pelo fabricante do equipamento em Salvador;

12.2. A empresa licitante deverá atender a todos os requisitos mínimos exigidos, e no caso da não comprovação acarretará na sua desclassificação.

12.3. Todo suporte deve ser prestado por técnicos certificados pelo fabricante.

12.4. A empresa proponente deverá apresentar obrigatoriamente, comprovação de que possui em seu quadro técnico no mínimo um profissional com a certificação técnica do fabricante.

12.5. A licitante deverá apresentar os certificados dos técnicos e comprovação de vínculo destes com a empresa.

12.6. As propostas deverão prever e especificar o período de garantia (mínimo de 60 sessenta meses) com atendimento ON-SITE, para hipótese de o atendimento não poder ser executado remoto.

12.7. A Empresa licitante deve apresentar declaração de que dispõe de mão-de-obra adequada e disponível, local, para execução dos serviços.

12.8. A Empresa licitante, não poderá transferir a outrem os compromissos assumidos, no todo ou em parte, os serviços.

12.9. O não cumprimento destes requisitos implicará na desclassificação imediata da licitante.

12.10 Deverá ser apresentado prospecto com as características técnicas de todos os componentes do equipamento, incluindo especificação de marca, modelo, e outros elementos que de forma inequívoca identifiquem e comprovem as configurações cotadas, possíveis expansões e upgrades, através de certificados, manuais técnicos, folders e demais literaturas técnicas editadas pelos fabricantes. Serão aceitas cópias das especificações obtidas em sítios dos fabricantes na Internet, em que constem o respectivo endereço eletrônico. O licitante deverá informar exatamente o Marca e modelo dos equipamento e Software ofertado e os catálogos devem obrigatoriamente ser públicos, ou seja, devem estar publicados no website do fabricante.

12.11 As propostas deverão prever e especificar o período de garantia (mínimo de 60 sessenta meses) com atendimento ON-SITE, para hipótese de o atendimento não poder ser executado remoto.

13.DA VISTORIA FACULTATIVA

13.1. É facultativo à LICITANTE visitar e vistoriar as instalações da Defensoria Pública do Estado da Bahia, a fim de conhecer o ambiente operacional existente e garantir a execução dos serviços.

13.2. Na Vistoria Técnica, a LICITANTE deve inteirar-se das condições dos serviços e do ambiente operacional, não se admitindo, posteriormente, qualquer alegação de desconhecimento das mesmas.

13.3. A CONTRATANTE disponibilizará o seu ambiente até 5 (cinco) dias anterior à data da abertura do certame, para que as empresas interessadas façam uma visita técnica, com vistas a avaliar as condições dos equipamentos, estrutura e demais informações necessárias ao dimensionamento dos serviços.

13.4. A empresa que realizar a vistoria deverá apresentar Declaração de que vistoriou, por intermédio de seu representante, os locais, instalações da prestação dos serviços, tendo então, pleno conhecimento das condições e eventuais dificuldades para a execução dos mesmos, bem como de todas as informações necessárias à formulação da sua proposta de preços, devendo tal vistoria, ser realizada até 03 (três) dias úteis antes da data fixada para a sessão pública, dentro do horário das 08h às 12h e das 14h às 17h, por meio de agendamento com a Coordenação de Modernização e Informática.

14.DOCUMENTAÇÃO TÉCNICA

14.1. A documentação técnica a ser fornecida deverá conter no mínimo os módulos descritos a seguir:

14.1.1. Documentação das Funcionalidades: Este documento conterá as características técnicas do produto e suas funções, procedimentos e parâmetros de configuração, tabelas, ilustrações etc.;

14.1.2. Documentação de Instalação e Operação: Este documento conterá informações quanto aos procedimentos de instalação e operação, comandos e teste aplicáveis, procedimentos de inicialização, de configuração e gerência de desempenho, de falhas e de segurança pertinentes.

14.1.3. A CONTRATADA deverá apresentar juntamente com a documentação dos produtos, certificado ou título, concedido pelo fabricante, que comprove o credenciamento da CONTRATADA como representante autorizada;

14.1.4. A CONTRATADA deverá apresentar juntamente com a documentação do produto, as licenças dos produtos fornecidos necessários para a implantação;

14.1.5. A documentação dos produtos abrange: manuais operacionais dos produtos, documento com as especificações técnicas dos produtos e seus recursos, as licenças dos produtos, mídias contendo os produtos para instalação fornecidos e toda documentação acessórias relativas aos produtos fornecidos.

15.TESTE E VERIFICAÇÃO PRELIMINAR

15.1. Todos os componentes disponíveis nas licenças fornecidas serão testados por meio de procedimentos designados pela CONTRATANTE, findo os quais será elaborado relatório técnico com a análise dos resultados;

15.2. O processo de realização dos testes de verificação preliminar do software será desenvolvido de acordo com os eventos e atividades descritos a seguir:

15.2.1. Conferência da Entrega: consiste na identificação e conferência das licenças fornecidas;

15.2.2. Teste de Instalação: consiste na verificação da instalação e da configuração das funcionalidades instaladas;

15.2.3. Testes de Ativação: consiste na operacionalização do software, após a conclusão dos testes de instalação, com a verificação de suas características, de suas funcionalidades e de sua compatibilidade;

15.3. A verificação preliminar não implica em recebimento definitivo do software fornecido;

15.4. O relatório gerado em função dos Testes de Verificação Preliminar será documento integrante do Termo de Recebimento e Aceitação do software fornecido.

16.ENTREGA, ACEITE E INSTALAÇÃO

16.1. O aceite do software será feito pela DPE/BA, após a implantação e entrada em operação das licenças fornecido;

16.2. A entrega e instalação das licenças será feita de acordo com plano de implantação, apresentado pela CONTRATADA e aprovado pela CONTRATANTE;

16.3. A instalação deverá seguir cronograma previsto no plano de implantação;

16.4. Como parte dos documentos de aceite do software fornecido, a CONTRATADA deverá apresentar "Tabela de Comprovação Técnica " das especificações exigidas neste Termo.

17. PRAZO DE ENTREGA

17.1. O prazo de entrega deverá ser de até 60 (sessenta) dias corridos, contados da data da assinatura do contrato.

18. LOCAL DE EXECUÇÃO DOS SERVIÇOS

Alagoinhas	Rua Marcela Bueron Cardoso, 184, centro.
Barreiras	Rua 26 de maio, nº 568, centro.
Camaçari	Rua Monte Gordo, 63 – bairro inocoop.
Feira de Santana	Avenida Maria Quitéria, nº 1.235 – ponto central
Ilhéus	Rua rotary, nº 255, edf. Office, salas 301, 401, 501, 601, 701, bairro cidade nova.
Irecê	Rua Antônio Carlos Magalhães, nº 84-a, centro.
Itabuna	Rua José Soares Pinheiro, nº 732, centro.
Jequié	Rua Manoel Vitorino, nº 510, campo do américa.
Juazeiro	Rua do paraíso, nº 152, Santo Antônio.
Paulo Afonso	Rua marechal Floriano Peixoto, nº 500, centro.
Porto Seguro	Rua Pero Vaz de Caminha, nº 178, centro.
Santo Antônio de Jesus	Rua vereador Albertino lira, nº 01, bairro quitandinha.
Vitória da Conquista	Rua Mem de Sá, n° 10 – bairro alto maron
Salvador	Casa de Acesso à Justiça I - Rua Arquimedes Gonçalves, nº 271, jardim baiano, cep: 40050-300
Salvador	Casa Cível e Fazenda Pública - Rua Boulevard Almeida, nº 07, jardim baiano, cep: 40050-320
Salvador	Casa das Famílias - Rua Arquimedes Gonçalves, 188 – Nazaré, cep: 40050-300
Salvador	Casa de Direitos Humanos - Rua Arquimedes Gonçalves, nº 482, jardim baiano, cep: 40050-300.

19. PROPRIEDADE INTELECTUAL

19.1. A CONTRATADA entregará a CONTRATANTE toda e qualquer documentação gerada em função da prestação de serviços decorrente deste Termo de Referência.

19.2. A CONTRATADA concorda que os direitos patrimoniais autorais relativos aos resultados produzidos durante a vigência do Contrato são de propriedade exclusiva da CONTRATANTE, devidamente amparada pela Lei nº 9.610/1998, de Diretos Autorais, respeitados os direitos morais do autor. Entendem-se por resultados quaisquer estudos, relatórios, especificações, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, páginas na Intranet e Internet e documentação didática em papel ou em mídia eletrônica.

19.3. A CONTRATADA fica proibida de veicular e comercializar todos e quaisquer produtos e informações geradas ou conhecidas relativas ao objeto da prestação dos serviços, salvo se houver a prévia autorização por escrito da CONTRATANTE.

20. PRAZO DE VIGÊNCIA

20.1. O período de vigência da Ata de Registro de Preços é de 12 (doze) meses, conforme o artigo 17, do Dec. nº 19.252 de 17 de setembro de 2019 e, do contrato a ser formalizado, 12 (doze) meses prorrogáveis em conformidade com o dispositivo 142 da Lei nº 9.433/2005.

21. ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

ITEM	DESCRIÇÃO	QUANTIDADE	VALOR
1	SOLUÇÃO DE SEGURANÇA E GERENCIA DE REDES NGFW **EM CLUSTER** – TIPO 1	01	R$ 307.813,80
2	SOLUÇÃO DE SEGURANÇA E GERENCIA DE REDES NGFW – TIPO 2	03	R$ 289.846,15
3	SOLUÇÃO DE SEGURANÇA E GERENCIA DE REDES NGFW – TIPO 3	13	R$ 369.688,93
4	UNIDADE CENTRALIZADA DE ARMAZENAMENTO DE LOGS E RELATORIA	01	R$ 298.852,52
5	UNIDADE DE GERÊNCIA CENTRALIZADA DE EQUIPAMENTOS	01	R$ 226.058,25
6	ATIVOS DE REDE WIRELESS INDOOR	80	R$ 748.930,93
7	SOLUÇÃO DE SEGURANÇA, FIREWALL DE APLICAÇÕES WEB, DORAVANTE DENOMINADO SOLUÇÃO **WAF**, COM SUPORTE, GARANTIA E ATUALIZAÇÕES	01	R$ 448.750,42
8	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO PARA SOLUÇÃO DE SEGURANÇA E GERÊNCIA DE REDES NGFW EM CLUSTER DE ALTA DISPONIBILIDADE	01	R$ 19.375,46
9	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO PARA SOLUÇÃO DE SEGURANÇA E GERENCIA DE REDES NGFW TIPOS "2" E "3"	16	R$ 42.674,93
10	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO DE UNIDADE CENTRALIZADA DE ARMAZENAMENTO DE LOGS E RELATORIA	01	R$ 19.121,87
11	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO DE UNIDADE DE GERENCIA CENTRALIZADA DE EQUIPAMENTOS.	01	R$ 12.633,92
12	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO DOS ATIVOS DE REDE WIRELESS INDOOR	80	R$ 67.093,33
13	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO DE SEGURANÇA **WAF**	01	R$ 31.828,57
		VALOR GLOBAL	**R$ 2.882.669,10**

22. A ADESÃO À ATA DE REGISTRO DE PREÇO

22.1. A ata de registro de preços, durante sua vigência, poderá ser utilizada por qualquer órgão ou entidade da Administração Pública Direta, Autárquica e Fundacional do Estados da Bahia, que não tenha participado do certame licitatório, mediante anuência do órgão gerenciador, desde que devidamente justificada a vantagem e respeitadas, no que couber, as condições e as regras estabelecidas no Decreto estadual nº 19.252/2019 e na Lei Federal nº 8.666, de 21 de junho de 1993.

22.2. Caberá ao fornecedor beneficiário da Ata de Registro de Preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento, desde que este fornecimento não prejudique as obrigações anteriormente assumidas com o órgão gerenciador e órgãos participantes.

22.3. As contratações adicionais não poderão exceder os limites quantitativos para adesões definidos no edital de origem, não podendo extrapolar, em qualquer caso, por cada órgão ou entidade aderente, a 50% (cinquenta por cento) dos quantitativos dos itens do instrumento convocatório e registrados na ata de registro de preços para o órgão gerenciador e para os órgãos ou entidades participantes

22.4. O quantitativo decorrente das adesões à ata de registro de preços não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o órgão gerenciador e para os órgãos ou entidades participantes, independentemente do número de órgãos ou entidades não participantes que aderirem.

22.5. A análise da juridicidade da participação, da inexistência de norma interna impeditiva, bem assim da adequação e compatibilidade com o regime jurídico de licitação a que está submetido o órgão gerenciador, deverá ser procedida pelo órgão ou entidade que pretende a adesão.

22.6. Após a autorização do órgão gerenciador, o órgão não participante deverá efetivar a contratação solicitada em até noventa dias, observado o prazo de validade da Ata de Registro de Preços. Caberá a Defensoria Pública do Estado da Bahia autorizar, excepcional e justificadamente, a prorrogação do prazo para efetivação da contratação, respeitado o prazo de vigência da ata, desde que solicitada pelo órgão não participante.

22.7. Competem ao órgão ou entidade aderente os atos relativos à cobrança do cumprimento pelo fornecedor das obrigações contratualmente assumidas e a aplicação, observada a ampla defesa e o contraditório, de eventuais penalidades decorrentes do descumprimento de cláusulas contratuais, em relação às suas próprias contratações, devendo informar as ocorrências ao órgão gerenciador

22.8. A abrangência territorial da ata de registro de preços: Estados da Federação e Distrito Federal.

23. ANEXOS

ANEXO I - TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE
ANEXO II - DECLARAÇÃO DE VISTORIA
ANEXO III - PROPOSTA DE PREÇOS

Responsável pelas informações constantes do termo de referência:

Servidor responsável: Ricardo Borges
Lotação: Coordenação de Modernização e Informática- CMO.

Defensoria Pública
BAHIA

ANEXO I

TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE

Os abaixo-assinados, de um lado a_____, CNPJ nº _____/_____, situada na cidade de_____, à Rua: _____, bairro_____, doravante denominada CONTRATANTE, e de outro lado_____, CNPJ nº_____/_, situada na cidade de_____, à Rua: _____, bairro_____, doravante denominada CONTRATADA, tem entre si justa e acertada, a celebração do presente TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE, através do qual a CONTRATADA aceita não divulgar sem autorização prévia e formal segredos e informações sensíveis de propriedade da DEFENSORIA PÚBLICA DO ESTADO DA BAHIA e se compromete a praticar procedimentos de segurança da informação, em conformidade com as seguintes cláusulas e condições:

PRIMEIRA – A CONTRATADA reconhece que em razão das suas atividades profissionais, estabelece contato com informações sigilosas, que devem ser entendidas como segredo. Estas informações devem ser tratadas confidencialmente sob qualquer condição e não podem ser divulgadas a terceiros não autorizados, aí se incluindo os próprios Colaboradores da _____, sem a expressa e escrita autorização da Defensoria Pública do Estado da Bahia.

SEGUNDA - As informações, exemplificadas abaixo, devem receber o tratamento de confidencialidade adequado, de acordo com o seu nível de classificação.

1. Programas de computador, suas listagens, documentação, artefatos diversos, código fonte e código objeto;

2. Toda a informação relacionada a programas existentes ou em fase de desenvolvimento no âmbito da Defensoria Pública da Bahia, inclusive fluxogramas, estatísticas, especificações, avaliações, resultados de testes, arquivos de dados, artefatos diversos e versões "beta" de quaisquer programas;

3. Documentos, informações e dados armazenados de atuação consultiva e contenciosa, de estratégias ou demais dados e/ou informações de caráter sigiloso ou restrito à Defensoria Pública do Estado da Bahia;

4. Metodologia, projetos e serviços utilizados;

5. Números e valores financeiros.

TERCEIRA – A CONTRATADA reconhece que a lista acima é meramente exemplificativa e ilustrativa e que outras hipóteses de confidencialidade que já existam ou que venham a surgir no futuro devem ser mantidas sob segredo. Em caso de dúvida acerca da confidencialidade de determinada informação a CONTRATADA deve tratar a mesma sob sigilo até que seja autorizado, formalmente, a tratá-la de forma diferente pela CONTRATANTE.

QUARTA – A CONTRATADA reconhece que, no seu desligamento definitivo, deverá entregar à CONTRATANTE todo e qualquer material de propriedade desta, inclusive notas pessoais envolvendo matérias sigilosas, registros de documentos de qualquer natureza que tenham sido usados, criados ou estado sob seu controle. A CONTRATADA também assume o compromisso de não utilizar qualquer informação adquirida quando de suas atividades para a Defensoria pública do Estado.

QUINTA – A CONTRATADA deve assegurar que todos os seus colaboradores guardarão sigilo sobre as informações que porventura tiverem acesso, mediante o ciente de seus colaboradores em Termo próprio a ser firmado entre a CONTRATADA e seus colaboradores, e que os mesmos comprometer-se-ão a informar, imediatamente, ao seu superior hierárquico, qualquer violação das regras de sigilo, por parte dele ou de qualquer pessoa, inclusive nos casos de violação não intencional.

Parágrafo Primeiro: A coleta dos Termos de Sigilo de seus colaboradores não exime a CONTRATADA das penalidades por violação das regras por parte de seus contratados.

Parágrafo Segundo: A CONTRATADA deverá fornecer cópia de todos os termos firmados com seus colaboradores à Defensoria Pública do Estado da Bahia no prazo de 10 dias após assinatura dos respectivos termos.

Parágrafo Terceiro: Sempre que um colaborador for admitido, A CONTRATADA deverá fornecer cópia dos novos termos firmados no prazo de 2 dias após assinatura dos respectivos termos.

SEXTA - O atendimento deste TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE, bem como da das Diretrizes Básicas da Política de Segurança da Informação devem ser incorporados formalmente ao contrato de trabalho dos funcionários da CONTRATADA que prestarem serviços à Defensoria Pública do Estado da Bahia.

SÉTIMA – A CONTRATADA deverá seguir a Política de Segurança da Informação definida pela CONTRATANTE.

OITAVA - O não cumprimento de quaisquer das cláusulas deste Termo implicará em responsabilização civil e criminal, de acordo com a legislação vigente.

NONA - Os casos omissos neste TERMO DE CONFIDENCIALIDADE, assim como as dúvidas surgidas em decorrência da sua execução, serão resolvidos pela DPE/BA, buscando solucionar de acordo com os princípios de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

DECIMA - O CONTRATANTE elege o foro da Salvador/BA, onde está localizada a sede do CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO, SIGILO E CONFIDENCIALIDADE é assinado pelas partes em 2 vias de igual teor e forma.

Em, _____de_____de 20___.

_____

Responsável pelo Contrato - CONTRATANTE

_____

Responsável pelo Contrato – CONTRATADA

ANEXO II

DECLARAÇÃO DE VISTORIA EXPEDIDA PELA DPE/BA

OBSERVAÇÕES SOBRE A VISITA TÉCNICA

Fica facultado as empresas licitantes a realização de visita técnica, para conhecer as instalações e condições para prestação dos serviços, saneando quaisquer dúvidas em relação ao processo de contratação dos serviços.

A visita deverá ser agendada previamente, com no mínimo 24 (vinte e quatro) horas de antecedência, junto à **Coordenação de Modernização e Informática**, pelos telefones (71) 3117- 9150 / 9151.

A visita somente poderá ser realizada nos horários de 8:30h as 17:00h, em dias de expediente regular, no prazo de até 72 (setenta e duas) horas antes da licitação.

A visita deverá ser realizada por profissional pertencente ao quadro funcional ou sócio da licitante, portador de diploma de nível superior em informática, cuja comprovação deverá ocorrer no momento da realização da visita técnica, mediante carta de apresentação assinada pelo representante legal da empresa, constando as informações inerentes às qualificações exigidas. As informações apresentadas são de inteira responsabilidade da licitante.

DECLARAÇÃO DE VISTORIA EXPEDIDA PELA ADMINISTRAÇÃO

Atesto que o responsável técnico da_____ (indicar nome da Pessoa Jurídica licitante), CNPJ nº_____(indicar CNPJ da licitante), Sr.(a)_____, CPF nº_____, interessado em participar da_____(indicar modalidade de licitação: pregão/concorrência/tomada de preço/convite) nº_____, vistoriou _____ (indicar a Unidade Administrativa vistoriada) e tomou ciência do estado das condições locais para o cumprimento das obrigações relativas ao objeto licitado.

Salvador_____de_____de 2023.

_____

(assinatura, identificação do servidor público e respectivo cadastro).

Defensoria Pública
BAHIA

ANEXO III – PROPOSTA DE PREÇOS

LOTE ÚNICO – (EQUIPAMENTOS PARA SEGURANÇA DA INFORMAÇÃO)				
ITEM	**DESCRIÇÃO**	**QUANTIDADE**	**VALOR UNITÁRIO**	**VALOR TOTAL**
01	SOLUÇÃO DE SEGURANÇA E GERENCIA DE REDES NGFW **EM CLUSTER** – TIPO 1	01	R$	R$
02	SOLUÇÃO DE SEGURANÇA E GERENCIA DE REDES NGFW – TIPO 2	03	R$	R$
03	SOLUÇÃO DE SEGURANÇA E GERENCIA DE REDES NGFW – TIPO 3	13	R$	R$
04	UNIDADE CENTRALIZADA DE ARMAZENAMENTO DE LOGS E RELATORIA	01	R$	R$
05	UNIDADE DE GERÊNCIA CENTRALIZADA DE EQUIPAMENTOS	01	R$	R$
06	ATIVOS DE REDE WIRELESS INDOOR	80	R$	R$
07	SOLUÇÃO DE SEGURANÇA, FIREWALL DE APLICAÇÕES WEB, DORAVANTE DENOMINADO SOLUÇÃO WAF, COM SUPORTE, GARANTIA E ATUALIZAÇÕES	01	R$	R$
08	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO PARA SOLUÇÃO DE SEGURANÇA E GERÊNCIA DE REDES NGFW EM CLUSTER DE ALTA DISPONIBILIDADE	01	R$	R$
09	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO PARA SOLUÇÃO DE SEGURANÇA E GERENCIA DE REDES NGFW TIPOS "2" E "3"	16	R$	R$
10	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO DE UNIDADE CENTRALIZADA DE ARMAZENAMENTO DE LOGS E RELATORIA	01	R$	R$
11	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO DE UNIDADE DE GERENCIA CENTRALIZADA DE EQUIPAMENTOS.	01	R$	R$
12	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO DOS ATIVOS DE REDE WIRELESS INDOOR	80	R$	R$
13	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO DE SEGURANÇA WAF	01	R$	R$
		VALOR GLOBAL		**R$**

Defensoria Pública
BAHIA

SEÇÃO III
ORÇAMENTO ESTIMADO EM PLANILHA

[pregão eletrônico sem orçamento sigiloso]

(**X**) Para efeito do art. 81, II, da Lei estadual no 9.433/05, o orçamento estimado em planilha de quantitativos e preços unitários é o descrito abaixo, os quais correspondem ao critério máximo de aceitabilidade dos preços unitários e global, no montante de valor total de R$ R$ 2.882.669,10 (dois milhões, oitocentos e oitenta e dois mil seiscentos e sessenta e nove reais e dez centavos).

ITEM	DESCRIÇÃO	QUANTIDADE	VALOR
1	SOLUÇÃO DE SEGURANÇA E GERENCIA DE REDES NGFW **EM CLUSTER** – TIPO 1	01	R$ 307.813,80
2	SOLUÇÃO DE SEGURANÇA E GERENCIA DE REDES NGFW – TIPO 2	03	R$ 289.846,15
3	SOLUÇÃO DE SEGURANÇA E GERENCIA DE REDES NGFW – TIPO 3	13	R$ 369.688,93
4	UNIDADE CENTRALIZADA DE ARMAZENAMENTO DE LOGS E RELATORIA	01	R$ 298.852,52
5	UNIDADE DE GERÊNCIA CENTRALIZADA DE EQUIPAMENTOS	01	R$ 226.058,25
6	ATIVOS DE REDE WIRELESS INDOOR	80	R$ 748.930,93
7	SOLUÇÃO DE SEGURANÇA, FIREWALL DE APLICAÇÕES WEB, DORAVANTE DENOMINADO SOLUÇÃO **WAF**, COM SUPORTE, GARANTIA E ATUALIZAÇÕES	01	R$ 448.750,42
8	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO PARA SOLUÇÃO DE SEGURANÇA E GERÊNCIA DE REDES NGFW EM CLUSTER DE ALTA DISPONIBILIDADE	01	R$ 19.375,46
9	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO PARA SOLUÇÃO DE SEGURANÇA E GERENCIA DE REDES NGFW TIPOS "2" E "3"	16	R$ 42.674,93
10	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO DE UNIDADE CENTRALIZADA DE ARMAZENAMENTO DE LOGS E RELATORIA	01	R$ 19.121,87
11	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO DE UNIDADE DE GERENCIA CENTRALIZADA DE EQUIPAMENTOS.	01	R$ 12.633,92
12	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO DOS ATIVOS DE REDE WIRELESS INDOOR	80	R$ 67.093,33
13	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO DE SEGURANÇA **WAF**	01	R$ 31.828,57
		VALOR GLOBAL	**R$ 2.882.669,10**

[NOTAS SOBRE O DEGRAU DE VALOR OU PERCENTUAL NO PREGÃO ELETRÔNICO]

1. É obrigatório fixar o degrau de valor ou percentual no modo de disputa aberto [NOTA: art. 11, §3° e § 5°, do Decreto n° 19.896/2020].

2. O degrau de valor será a partir de R$ 100,00 (cem reais) ora fixado para o lote em disputa.

3. Foi fixado o degrau de valor para o modo de disputa aberto.

O VALOR DO LANCE A SER EFETUADO NO SISTEMA LICITAÇÕES-E SERÁ PELO "MENOR PREÇO GLOBAL" PARA O LOTE ÚNICO DA DISPUTA.

NOTA:/OBSERVAÇÃO: O licitante deverá informar exatamente o Marca e modelo dos equipamento e Software ofertado e os catálogos devem obrigatoriamente ser públicos, ou seja, devem estar publicados no website do fabricante.

Defensoria Pública
BAHIA

SEÇÃO IV
MODELO DE DESCRIÇÃO DA PROPOSTA

1. Modelo de descrição da proposta de preços

Modalidade de Licitação	Número
PREGÃO ELETRÔNICO	17/2023

LOTE ÚNICO					
ITEM	**DESCRIÇÃO**	**MARCA/MODELO/ SOFWARE**	**QUANTIDADE**	**VALOR UNITÁRIO**	**VALOR TOTAL**
1	SOLUÇÃO DE SEGURANÇA E GERENCIA DE REDES NGFW EM CLUSTER – TIPO 1		01	R$	R$
2	SOLUÇÃO DE SEGURANÇA E GERENCIA DE REDES NGFW – TIPO 2		03	R$	R$
3	SOLUÇÃO DE SEGURANÇA E GERENCIA DE REDES NGFW – TIPO 3		13	R$	R$
4	UNIDADE CENTRALIZADA DE ARMAZENAMENTO DE LOGS E RELATORIA		01	R$	R$
5	UNIDADE DE GERÊNCIA CENTRALIZADA DE EQUIPAMENTOS		01	R$	R$
6	ATIVOS DE REDE WIRELESS INDOOR		80	R$	R$
7	SOLUÇÃO DE SEGURANÇA, FIREWALL DE APLICAÇÕES WEB, DORAVANTE DENOMINADO SOLUÇÃO WAF, COM SUPORTE, GARANTIA E ATUALIZAÇÕES		01	R$	R$
8	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO PARA SOLUÇÃO DE SEGURANÇA E GERÊNCIA DE REDES NGFW EM CLUSTER DE ALTA DISPONIBILIDADE		01	R$	R$
9	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO PARA SOLUÇÃO DE SEGURANÇA E GERENCIA DE REDES NGFW TIPOS "2" E "3"		16	R$	R$
10	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO DE UNIDADE CENTRALIZADA DE ARMAZENAMENTO DE LOGS E RELATORIA		01	R$	R$
11	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO DE UNIDADE DE GERENCIA CENTRALIZADA DE EQUIPAMENTOS.		01	R$	R$
12	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO DOS ATIVOS DE REDE WIRELESS INDOOR		80	R$	R$
13	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO DE SEGURANÇA WAF		01	R$	R$
				VALOR GLOBAL	**R$**

PRAZO DE VALIDADE DA PROPOSTA: ( ) DIAS

Conforme Termo de Referência, o período de garantia (mínimo de 60 sessenta meses) com atendimento ON-SITE, para hipótese de o atendimento não poder ser executado remoto.

O licitante deverá informar exatamente o Marca e modelo dos equipamento e Software ofertado e os catálogos devem obrigatoriamente ser públicos, ou seja, devem estar publicados no website do fabricante.

Salvador _____de _____ de 2023.

_____

NOME/RAZÃO SOCIAL CPF/ CNPJ REPRESENTANTE LEGAL / ASSINATURA

Defensoria Pública
BAHIA

SEÇÃO V
MODELO DE DECLARAÇÃO DE ELABORAÇÃO INDEPENDENTE DE PROPOSTA E DE INEXISTÊNCIA DE IMPEDIMENTO À PARTICIPAÇÃO NO CERTAME

Modalidade de Licitação	Número
PREGÃO ELETRÔNICO	17/2023

[Identificação completa do representante da licitante], como representante devidamente constituído de **[Identificação completa da licitante],** doravante denominada LICITANTE, para fins de participação no certame licitatório acima identificado, declaro, sob as penas da lei, em especial o art. 299 do Código Penal Brasileiro, que:

(a) a proposta apresentada para participar desta licitação foi elaborada de maneira independente por mim e o conteúdo da proposta não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer outro participante potencial ou de fato desta licitação, por qualquer meio ou por qualquer pessoa;

(b) a intenção de apresentar a proposta elaborada para participar desta licitação não foi informada, discutida ou recebida de qualquer outro participante potencial ou de fato desta licitação, por qualquer meio ou por qualquer pessoa;

(c) que não tentei, por qualquer meio ou por qualquer pessoa, influir na decisão de qualquer outro participante potencial ou de fato desta licitação quanto a participar ou não dela;

(d) que o conteúdo da proposta apresentada para participar desta licitação não será, no todo ou em parte, direta ou indiretamente, comunicado ou discutido com qualquer outro participante potencial ou de fato desta licitação antes da adjudicação do objeto;

(e) que o conteúdo da proposta apresentada para participar desta licitação não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer integrante do órgão licitante antes da abertura oficial das propostas; e

(f) que estou plenamente ciente do teor e da extensão desta declaração e que detenho plenos poderes e informações para firmá-la.

Declaro, ainda, para os efeitos art. 299 do Código Penal Brasileiro, não estar sujeito às hipóteses de impedimento de participação elencadas nos arts. 18 e 125 da Lei estadual nº 9.433/05, quais sejam:

Art. 18 - Não poderá participar, direta ou indiretamente, da licitação, da execução de obras ou serviços e do fornecimento de bens a eles necessários: I - o autor do projeto, básico ou executivo, pessoa física ou jurídica; II - a empresa responsável, isoladamente ou em consórcio, pela elaboração do projeto básico ou executivo ou da qual o autor do projeto seja dirigente, gerente, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto ou controlador, responsável técnico, subordinado ou subcontratado;
III - servidor ou dirigente do órgão ou entidade contratante ou responsável pela licitação; IV - demais agentes públicos, assim definidos no art. 207 desta Lei, impedidos de contratar com a Administração Pública por vedação constitucional ou legal.

§ 1º- É permitida a participação do autor do projeto ou da empresa, a que se refere o inciso II deste artigo, na licitação ou na execução da obra ou serviço, como consultor ou técnico, nas funções de fiscalização, supervisão ou gerenciamento, exclusivamente a serviço da Administração interessada.
§ 2º- O disposto neste artigo não impede a licitação ou contratação de obra ou serviço que inclua, como encargo do contratado ou pelo preço previamente fixado pela Administração, a elaboração do projeto executivo.
§ 3º- Considera-se participação indireta, para os fins do disposto neste artigo, a existência de qualquer vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou de parentesco até o 3º grau entre o autor do projeto, pessoa física ou jurídica, e o licitante ou responsável pelos serviços, fornecimentos e obras, incluindo-se o fornecimento de bens e serviços a estes necessários.
§ 4º - Aplica-se o disposto no parágrafo anterior aos membros da comissão de licitação.

Art. 125 - É vedado ao agente político e ao servidor público de qualquer categoria, natureza ou condição, celebrar contratos com a Administração direta ou indireta, por si ou como representante de terceiro, sob pena de nulidade, ressalvadas as exceções legais.
Parágrafo único - Não se inclui na vedação deste artigo a prestação de serviços em caráter eventual, de consultoria técnica, treinamento e aperfeiçoamento, bem como a participação em comissões examinadoras de concursos, no âmbito da Administração Pública.

Salvador, _____de _____ de 2023.

_____
NOME/RAZÃO SOCIAL CPF/ CNPJ REPRESENTANTE LEGAL / ASSINATURA

SEÇÃO VI
MODELO DE PROCURAÇÃO

Modalidade de Licitação	Número
PREGÃO ELETRÔNICO	**17/2023**

Através do presente instrumento, nomeamos e constituímos o(a) Senhor(a) ....., (nacionalidade, estado civil, profissão), portador do Registro de Identidade nº ....., expedido pela ....., devidamente inscrito no Cadastro de Pessoas Físicas do Ministério da Fazenda, sob o nº ....., residente à rua ....., nº ..... como nosso mandatário, a quem outorgamos amplos poderes para praticar todos os atos relativos ao procedimento licitatório indicado acima, conferindo-lhe poderes para:

(apresentar proposta de preços, interpor recursos e desistir deles, contra-arrazoar, assinar contratos, negociar preços e demais condições, confessar, firmar compromissos ou acordos, receber e dar quitação e praticar todos os demais atos pertinentes ao certame etc).

Salvador _____de _____ de 2023.

_____

NOME/RAZÃO SOCIAL CPF/ CNPJ REPRESENTANTE LEGAL / ASSINATURA

SEÇÃO VII
MODELO DE DECLARAÇÃO DE ENQUADRAMENTO (LEI COMPLEMENTAR nº 123/06)

[EXCLUSIVA PARA MICROEMPRESA E EMPRESA DE PEQUENO PORTE]

Modalidade de Licitação	Número
PREGÃO ELETRÔNICO	**17/2023**

Para os efeitos do tratamento diferenciado da Lei Complementar nº 123/06, declaramos:

que estamos enquadrados, na data designada para o início da sessão pública da licitação, na condição
( ) **de microempresa** **[ou]** ( ) **de empresa de pequeno porte**
e que não estamos incursos nas vedações a que se reporta o §4º do art. 3º da Lei Complementar nº 123/06.

Salvador, _____de _____ de 2023.

_____

NOME/RAZÃO SOCIAL CPF/ CNPJ REPRESENTANTE LEGAL / ASSINATURA

Defensoria Pública
BAHIA

SEÇÃO VIII
MODELO DE DECLARAÇÃO DE PLENO CONHECIMENTO E DE VERACIDADE DOS DOCUMENTOS

[EXCLUSIVA PARA O PREGÃO ELETRÔNICO E PRESENCIAL]

Modalidade de Licitação	Número
PREGÃO ELETRÔNICO	**17/2023**

Em cumprimento ao art. 120, II da Lei estadual nº 9.433/05 e ao art. 18, §4º do Decreto nº 19.896/20, e em face do quanto disposto no art. 184, inc. V, e no art. 195 da Lei estadual nº 9.433/05, declaro:

( ) o **pleno conhecimento e atendimento às exigências de habilitação**.

[ou]

[exclusivamente para microempresas e empresas de pequeno porte beneficiárias da Lei Complementar nº 123/06]

( ) o **pleno conhecimento e atendimento às exigências de habilitação**, ressalvada, na forma do §1º do art. 43 da Lei complementar nº 123/06, a existência de restrição fiscal e/ou trabalhista.

Declaro, ainda, a veracidade dos documentos por mim apresentados, sob as penas da lei.

Salvador _____de _____ de 2023.

_____

NOME/RAZÃO SOCIAL CPF/ CNPJ REPRESENTANTE LEGAL / ASSINATURA

Defensoria Pública
BAHIA

PARTE II – HABILITAÇÃO

SEÇÃO I
DOCUMENTOS DE HABILITAÇÃO

1. Para a habilitação dos interessados, exigir-se-ão os documentos relativos a:

1.1 Habilitação jurídica, comprovada mediante a apresentação:

(x) **Para pessoas jurídicas:**

a) de registro público, no caso de empresário individual.
b) em se tratando de sociedades empresárias, do ato constitutivo, estatuto ou contrato social, com suas eventuais alterações supervenientes em vigor, devidamente registrados, acompanhados, quando for o caso, dos documentos societários comprobatórios de eleição ou designação e investidura dos atuais administradores.
c) no caso de sociedades simples, do ato constitutivo, estatuto ou contrato social, com suas eventuais alterações supervenientes em vigor, devidamente registrados, acompanhados dos atos comprobatórios de eleição e investidura dos atuais administradores.
d) decreto de autorização, no caso de empresa ou sociedade estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

1.2 Regularidade fiscal e trabalhista:

(x) **Para pessoas jurídicas:**

1.2.1. Regularidade fiscal, mediante a apresentação de:

a) prova de inscrição no Cadastro Nacional de Pessoa Jurídica – CNPJ.
b) prova de inscrição no Cadastro de Contribuinte Municipal - serviços, relativo ao domicílio ou sede da licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual.
c) prova de regularidade para com a Fazenda Estadual e Municipal do domicílio ou sede da licitante.
d) prova de regularidade para com a Fazenda Federal, inclusive INSS.
e) prova de regularidade relativa ao Fundo de Garantia por Tempo de Serviço (FGTS), mediante a apresentação do Certificado de Regularidade do FGTS - CRF.

1.2.1.1 As microempresas e empresas de pequeno porte, beneficiárias do tratamento diferenciado e favorecido previsto na Lei Complementar nº 123/06, deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição, cumprindo-lhes assinalar a sua condição nos campos correspondentes na **Declaração Quanto à Regularidade Fiscal e Trabalhista,** conforme o modelo da **PARTE II** deste instrumento.

1.2.2 Regularidade trabalhista, mediante a apresentação de:

f) prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, através de certidão negativa, ou positiva com efeitos de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943.

1.2.2.1 As microempresas e empresas de pequeno porte, beneficiárias do tratamento diferenciado e favorecido previsto na Lei Complementar nº 123/06, deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade trabalhista, mesmo que esta apresente alguma restrição, cumprindo-lhes assinalar a sua condição nos campos correspondentes na **Declaração Quanto à Regularidade Fiscal e Trabalhista,** conforme o modelo da **PARTE II** deste instrumento.

1.3 Qualificação Técnica, comprovada através de:

a) Comprovação de aptidão para o desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto da licitação, através da apresentação de um ou mais atestados fornecidos por pessoas jurídicas de direito público ou privado, preferencialmente de acordo com o modelo constante da PARTE II deste instrumento (art. 101, II).

b) A empresa proponente deverá apresentar obrigatoriamente, comprovação de que possui em seu quadro técnico no mínimo um profissional com a certificação técnica do fabricante.

c) Apresentar Declaração das Instalações, Pessoal e Aparelhamento Técnico.

c1) A licitante deverá apresentar os certificados dos técnicos e comprovação de vínculo destes com a empresa.

d) Deverá ser apresentado prospecto com as características técnicas de todos os componentes do equipamento, incluindo especificação de marca, modelo, e outros elementos que de forma inequívoca identifiquem e comprovem as configurações cotadas, possíveis expansões e upgrades, através de certificados, manuais técnicos, folders e demais literaturas técnicas editadas pelos fabricantes. Serão aceitas cópias das especificações obtidas em sítios dos fabricantes na Internet, em que constem o respectivo endereço eletrônico. O licitante deverá informar exatamente o Marca e modelo dos equipamento e Software ofertado e os catálogos devem obrigatoriamente ser públicos, ou seja, devem estar publicados no website do fabricante.

e) VISITA TÉCNICA- Declaração de ciência dos requisitos técnicos (vistoria facultativa):

e1) É facultativo à LICITANTE visitar e vistoriar as instalações da Defensoria Pública do Estado da Bahia, a fim de conhecer o ambiente operacional existente e garantir a execução dos serviços.

e2) Na Vistoria Técnica, a LICITANTE deve inteirar-se das condições dos serviços e do ambiente operacional, não se admitindo, posteriormente, qualquer alegação de desconhecimento das mesmas.

e3) A CONTRATANTE disponibilizará o seu ambiente até 5 (cinco) dias anterior à data da abertura do certame, para que as empresas interessadas façam uma visita técnica, com vistas a avaliar as condições dos equipamentos, estrutura e demais informações necessárias ao dimensionamento dos serviços.

e4) A empresa que realizar a vistoria deverá apresentar Declaração de que vistoriou, por intermédio de seu representante, os locais, instalações da prestação dos serviços, tendo então, pleno conhecimento das condições e eventuais dificuldades para a execução dos mesmos, bem como de todas as informações necessárias à formulação da sua proposta de preços, devendo tal vistoria, ser realizada até 03 (três) dias úteis antes da data fixada para a sessão pública, dentro do horário das 08h às 12h e das 14h às 17h, por meio de agendamento com a Coordenação de Modernização e Informática.

e5) No caso de não realização da vistoria, as licitantes assumirão total concordância com todos os dispositivos constantes deste Termo de Referência, seus anexos e as condições do local, não sendo admitidas, em hipótese alguma, alegações posteriores de desconhecimento sobre os serviços, quantitativos, prazos ou dificuldades técnicas não previstas.

f) APRESENTAR A SEGUINTE DOCUMENTAÇÃO TÉCNICA

A documentação técnica a ser fornecida deverá conter no mínimo os módulos descritos a seguir:

f1) Documentação das Funcionalidades: Este documento conterá as características técnicas do produto e suas funções, procedimentos e parâmetros de configuração, tabelas, ilustrações etc.;

f2) Documentação de Instalação e Operação: Este documento conterá informações quanto aos procedimentos de instalação e operação, comandos e teste aplicáveis, procedimentos de inicialização, de configuração e gerência de desempenho, de falhas e de segurança pertinentes.

f3) A CONTRATADA deverá apresentar juntamente com a documentação do produto, as licenças dos produtos fornecidos necessários para a implantação;

f4) A documentação dos produtos abrange: manuais operacionais dos produtos, documento com as especificações técnicas dos produtos e seus recursos, as licenças dos produtos, mídias contendo os produtos para instalação fornecidos e toda documentação acessórias relativas aos produtos fornecidos.

g) A CONTRATADA deverá apresentar juntamente com a documentação dos produtos, **certificado ou título, concedido pelo fabricante, que comprove o credenciamento da CONTRATADA como representante autorizada.**

1.4 Qualificação econômico-financeira:

(X) **exigível (contratação de caráter geral)**
(X) contratação de serviços **sem** regime de dedicação exclusiva de mão de obra

I - balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, observadas as seguintes disposições:
a) A comprovação da situação financeira da empresa será constatada mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), com resultado maior que 1 (um).
b) O cálculo dos índices será feito com base nos valores extraídos do balanço patrimonial ou, para as licitantes cadastradas, se disponível, através de consulta ao Cadastro Unificado de Fornecedores, utilizando as seguintes fórmulas:

$$\text{Liquidez Geral (LG)} = \frac{\text{(Ativo Circulante + Realizável a Longo Prazo)}}{\text{(Passivo Circulante + Passivo Não Circulante)}}$$

$$\text{Solvência Geral (SG)} = \frac{\text{(Ativo Total)}}{\text{(Passivo Circulante +Passivo não Circulante);}}$$

$$\text{Liquidez Corrente (LC)} = \frac{\text{(Ativo Circulante)}}{\text{(Passivo Circulante)}}$$

c) As licitantes que apresentarem resultado igual ou menor que 1 (um), em qualquer dos índices, quando da habilitação, deverão comprovar patrimônio líquido mínimo, correspondente a 10% (dez por cento) do valor estimado da contratação, na forma do §2º do art. 102 da Lei nº 9.433/05.

I.1 O balanço patrimonial e demonstrações contábeis podem ser atualizados por índices oficiais, quando encerrados há mais de 03 (três) meses da data da apresentação da proposta, vedada a sua substituição por balancetes ou balanços provisórios.
I.2 A licitante apresentará, conforme o caso, publicação no Diário Oficial ou Jornal de Grande Circulação do Balanço ou cópia reprográfica das páginas do Livro Diário numeradas sequencialmente onde foram transcritos o Balanço e a Demonstração de Resultado, com os respectivos Termos de Abertura e Encerramento registrados na Junta Comercial ou no caso de empresas sujeitas à tributação com base no lucro real, o Balanço Patrimonial e Demonstração de Resultado emitido através do Sistema Público de Escrituração Digital –SPED, contendo Recibo de Entrega do Livro, os Termos de Abertura, Encerramento e Autenticação, podendo este último ser substituído pela Etiqueta da Junta Comercial ou Órgão de Registro.

II - certidão negativa de falência ou recuperação judicial expedida pelo distribuidor da sede da licitante, com data de expedição ou revalidação dos últimos 90 (noventa) dias anteriores à data da realização da licitação, caso o documento não consigne prazo de validade.

1.5 Declaração de Proteção ao Trabalho do Menor
Conforme o inciso XXXIII do art. 7º da Constituição Federal, para os fins do disposto no inciso V do art. 98 da Lei estadual nº 9.433/05, deverá ser apresentada declaração quanto ao trabalho do menor, conforme modelo constante da **SEÇÃO IV DA PARTE II** deste instrumento.

2. Regras acerca da participação de matriz e filial
a) Se a licitante for a matriz, todos os documentos devem estar em nome da matriz;
b) Se a licitante for filial, todos os documentos devem estar em nome da filial, exceto aqueles que a legislação permita ou exija a emissão apenas em nome da matriz;
c) A comprovação de aptidão para o desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto da licitação poderá ser feita em nome da matriz ou da filial;
d) Se a licitante participar do certame apresentando os documentos de habilitação da matriz e desejar executar o contrato pela filial, ou vice-versa, deverá fazer prova, por ocasião da assinatura do contrato, da regularidade do estabelecimento que executará o objeto licitado, a qual deverá ser mantida durante todo o curso da avença.

3. A licitante deverá incluir no envelope de habilitação os documentos acima relacionados, sob pena de inabilitação, sendo-lhe facultado apresentar, alternativamente, o Certificado de Registro Cadastral-CRC ou Certificado de Registro Simplificado-CRS, que possibilitará a substituição dos documentos de habilitação, na forma indicada neste instrumento.
3.1 Caso conste do registro algum documento vencido, a licitante deverá apresentar a versão atualizada do referido documento junto aos demais documentos de habilitação
3.2 No pregão eletrônico, os documentos de habilitação deverão ser apresentados conforme o disposto na Parte Fixa – Rito do procedimento licitatório e da contratação.

SEÇÃO II
CERTIFICADO DE REGISTRO CADASTRAL CRC/CRS

1. Pressupostos para participação:

(**X**) Serão admitidos a participar desta licitação os interessados que atenderem a todas as exigências contidas neste instrumento, que pertençam ao ramo de atividade pertinente ao objeto licitado, e que tenham realizado seu credenciamento como *usuário* junto ao Banco do Brasil, para a obtenção de chave de identificação ou senha individual. **[Pregão eletrônico]**

2. Documentos passíveis de substituição pelo extrato do Certificado de Registro:

2.1 O Certificado de Registro Cadastral-CRC ou Certificado de Registro Simplificado–CRS, estando no prazo de validade, poderá substituir os documentos relativos à habilitação constantes do sistema de registro, **exceto os concernentes à Qualificação Técnica**.
2.2 A substituição dos documentos está condicionada à verificação da regularidade destes, mediante a emissão do extrato do fornecedor pelo órgão licitante.

Defensoria Pública
BAHIA

SEÇÃO III
MODELOS DE PROVA DE QUALIFICAÇÃO TÉCNICA

COMPROVAÇÃO DE APTIDÃO PARA O DESEMPENHO

Modalidade de Licitação	Número
PREGÃO ELETRÔNICO	**17/2023**

Declaramos, para fins de habilitação em processo licitatório, que a empresa XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX, CNPJ XXXXXXXXXXXXXX, com endereço na XXXXXXXXXXXXXXXXXXXXXX, prestou serviço de xxxxxxxxxxxxxxx, atendendo integralmente as especificações contratadas, inexistindo, até a presente data, registros negativos que comprometam a prestação.

Especificação	Quantitativo	Prazo de execução

Salvador _____de _____ de 2023.

_____

NOME/RAZÃO SOCIAL CPF/ CNPJ REPRESENTANTE LEGAL / ASSINATURA

Defensoria Pública
BAHIA

NDICAÇÃO DAS INSTALAÇÕES, DO APARELHAMENTO E DO PESSOAL TÉCNICO

Modalidade de Licitação Pregão Eletrônico	Número 17/2023

DECLARAÇÃO FORMAL DE DISPONIBILIDADE

Declaro, em observância ao art. 101, §6º, da Lei estadual nº 9.433/05, para fins de prova de qualificação técnica, que disporei das instalações, do aparelhamento e do pessoal técnico, conforme relação abaixo, em estrita consonância com os requisitos estabelecidos do instrumento convocatório, conforme estipulado no item 1.3 Qualificação Técnica da Seção I - DOCUMENTOS DE HABILITAÇÃO da PARTE II – HABILITAÇÃO deste edital, estando ciente de que a declaração falsa caracteriza o ilícito administrativo previsto no art. 184, V, da Lei estadual nº 9.433/05.

Instalações, Aparelhamento (Máquinas/Equipamentos) e Pessoal Técnico	Quantidade

a) Atendimento da Assistência Técnica: Prazo de 60 (sessenta) meses com suporte fornecido pelo fabricante do equipamento em Salvador;

b) Todos os componentes de hardware e software, deverão possuir garantia de, no mínimo, 60 (sessenta) meses, com suporte técnico de 8 (oito) horas por dia, 5 (cinco) dias por semana, na cidade de Salvador (BA).

c) Durante o período de execução dos serviços, a CONTRATADA deverá garantir o funcionamento do software, com suporte técnico do FABRICANTE prestado em caso de falha.

d) 9Deverá ser garantida, neste prazo, a atualização de versões, releases, componentes (bibliotecas, filtros, dentre outros) e módulos dos softwares e equipamentos utilizados na prestação dos serviços.

e) DOS TÉCNICOS INDICADOS:

e1) Todo suporte deve ser prestado por técnicos certificados pelo fabricante.

e2) O serviço deverá ser prestado por profissional de nível superior, devidamente certificado nas soluções tecnológicas utilizadas na prestação dos serviços contratados.

e3) A licitante deverá apresentar os certificados dos técnicos e comprovação de vínculo destes com a empresa.

e4) licitante deve anexar a comprovação de que o pessoal técnico indicado vincular-se-á à execução contratual, a qual pode ser feita através de uma das seguintes formas: a) Carteira de Trabalho; b) Certidão do Conselho Profissional; c) Contrato social; d) Contrato de prestação de serviços; e) Termo através do qual o profissional assuma o compromisso de integrar o quadro técnico da empresa no caso do objeto contratual vir a ser a esta adjudicado.]

Salvador _____de _____ de 2023.

_____

RAZÃO SOCIAL / CNPJ / NOME DO REPRESENTANTE LEGAL / ASSINATURA

Defensoria Pública
BAHIA

DECLARAÇÃO DE CIÊNCIA DOS REQUISITOS TÉCNICOS (VISITA TÉCNICA)

DECLARAÇÃO DE VISTORIA EXPEDIDA PELA DPE/BA

OBSERVAÇÕES SOBRE A VISITA TÉCNICA

Fica facultado as empresas licitantes a realização de visita técnica, para conhecer as instalações e condições para prestação dos serviços, saneando quaisquer dúvidas em relação ao processo de contratação dos serviços.

A visita deverá ser agendada previamente, com no mínimo 24 (vinte e quatro) horas de antecedência, junto à **Coordenação de Modernização e Informática**, pelos telefones (71) 3117- 9150 / 9151.

A visita somente poderá ser realizada nos horários de 8:30h as 17:00h, em dias de expediente regular, no prazo de até 72 (setenta e duas) horas antes da licitação.

A visita deverá ser realizada por profissional pertencente ao quadro funcional ou sócio da licitante, portador de diploma de nível superior em informática, cuja comprovação deverá ocorrer no momento da realização da visita técnica, mediante carta de apresentação assinada pelo representante legal da empresa, constando as informações inerentes às qualificações exigidas. As informações apresentadas são de inteira responsabilidade da licitante.

DECLARAÇÃO DE VISTORIA EXPEDIDA PELA ADMINISTRAÇÃO

Atesto que o responsável técnico da_____ (indicar nome da Pessoa Jurídica licitante), CNPJ nº_____(indicar CNPJ da licitante), Sr.(a)_____, CPF nº_____, interessado em participar da_____(indicar modalidade de licitação: pregão/concorrência/tomada de preço/convite) nº_____, vistoriou _____ (indicar a Unidade Administrativa vistoriada) e tomou ciência do estado das condições locais para o cumprimento das obrigações relativas ao objeto licitado.

Salvador _____de _____ de 2023.

_____
(assinatura, identificação do servidor público e respectivo cadastro)

[OU]

Declaro, em atenção ao procedimento licitatório _____[IDENTIFICAR A LICITAÇÃO], para os fins do disposto no inciso IV do art. 101 da Lei estadual nº 9.433/05, ter ciência de todas as informações e das condições para o cumprimento das obrigações objeto da licitação, pelo que **dispenso** a realização de VISITA TÉCNICA, com o que não poderei alegar desconhecimento supervenientemente.

Salvador _____de _____ de 2023.

_____
NOME/RAZÃO SOCIAL CPF/ CNPJ REPRESENTANTE LEGAL / ASSINATURA

SEÇÃO IV
MODELO DE DECLARAÇÃO DE PROTEÇÃO AO TRABALHO DO MENOR

Modalidade de Licitação	Número
PREGÃO ELETRÔNICO	**17/2023**

Declaramos, sob as penas da lei, em atendimento ao quanto previsto no inciso XXXIII do art. 7º da Constituição Federal, para os fins do disposto no inciso V do art. 98 da Lei estadual nº 9.433/05, que não empregamos menor de 18 anos em trabalho noturno, perigoso ou insalubre,

( ) nem menor de 16 anos.

ou

( ) nem menor de 16 anos, salvo na condição de aprendiz, a partir de 14 anos.

Salvador _____de _____ de 2023.

_____

NOME/RAZÃO SOCIAL CPF/ CNPJ REPRESENTANTE LEGAL / ASSINATURA

Defensoria Pública
BAHIA

SEÇÃO V
MODELO DE DECLARAÇÃO QUANTO À REGULARIDADE FISCAL E TRABALHISTA (LEI COMPLEMENTAR nº 123/06)

[EXCLUSIVA PARA MICROEMPRESA E EMPRESA DE PEQUENO PORTE QUE TENHA RESTRIÇÃO NA REGULARIDADE FISCAL E/OU TRABALHISTA]

Modalidade de Licitação	Número
PREGÃO ELETRÔNICO	**17/2023**

Em cumprimento ao disposto no instrumento convocatório acima identificado, **declaro**, para os efeitos da Lei Complementar nº 123/06

Haver restrição na comprovação da nossa regularidade ( ) fiscal ( ) trabalhista, a cuja regularização procederemos no prazo de 05 (cinco) dias úteis, cujo termo inicial corresponderá à data da declaração do vencedor.

Salvador _____de _____ de 2023.

_____

NOME/RAZÃO SOCIAL CPF/ CNPJ REPRESENTANTE LEGAL / ASSINATURA

PARTE III – CRITÉRIOS ESPECÍFICOS

SEÇÃO I
AMOSTRAS/DEMONSTRAÇÃO DE COMPATIBILIDADE

(**X**) Não se exigirá a apresentação de **demonstração de compatibilidade**

SEÇÃO II
PARTICIPAÇÃO DE EMPRESAS REUNIDAS EM CONSÓRCIO

(**x**) Não poderão participar desta licitação pessoas jurídicas reunidas em consórcio.

SEÇÃO III
PARTICIPAÇÃO DE COOPERATIVAS

(**x**) Não poderão participar cooperativas nesta licitação.

SEÇÃO IV
AVALIAÇÃO DAS PROPOSTAS TÉCNICAS [NOTA: TIPO TÉCNICA E PREÇO]

(**X**) Não se aplica

SEÇÃO V
RESERVA DE COTA PARA MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE

(**X**) Não se aplica

SEÇÃO VI
ADESÃO POSTERIOR À ATA DE REGISTRO DE PREÇOS (CARONA)

(X) Sim.

A ADESÃO À ATA DE REGISTRO DE PREÇO

a) A ata de registro de preços, durante sua vigência, poderá ser utilizada por qualquer órgão ou entidade da Administração Pública Direta, Autárquica e Fundacional do Estados da Bahia, que não tenha participado do certame licitatório, mediante anuência do órgão gerenciador, desde que devidamente justificada a vantagem e respeitadas, no que couber, as condições e as regras estabelecidas no Decreto estadual nº 19.252/2019 e na Lei Federal nº 8.666, de 21 de junho de 1993.

b) Caberá ao fornecedor beneficiário da Ata de Registro de Preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento, desde que este fornecimento não prejudique as obrigações anteriormente assumidas com o órgão gerenciador e órgãos participantes.

c) As contratações adicionais não poderão exceder os limites quantitativos para adesões definidos no edital de origem, não podendo extrapolar, em qualquer caso, por cada órgão ou entidade aderente, a 50% (cinquenta por cento) dos quantitativos dos itens do instrumento convocatório e registrados na ata de registro de preços para o órgão gerenciador e para os órgãos ou entidades participantes

d) O quantitativo decorrente das adesões à ata de registro de preços não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o órgão gerenciador e para os órgãos ou entidades participantes, independentemente do número de órgãos ou entidades não participantes que aderirem.

e) A análise da juridicidade da participação, da inexistência de norma interna impeditiva, bem assim da adequação e compatibilidade com o regime jurídico de licitação a que está submetido o órgão gerenciador, deverá ser procedida pelo órgão ou entidade que pretende a adesão.

f) Após a autorização do órgão gerenciador, o órgão não participante deverá efetivar a contratação solicitada em até noventa dias, observado o prazo de validade da Ata de Registro de Preços. Caberá a Defensoria Pública do Estado da Bahia autorizar, excepcional e justificadamente, a prorrogação do prazo para efetivação da contratação, respeitado o prazo de vigência da ata, desde que solicitada pelo órgão não participante.

g) Competem ao órgão ou entidade aderente os atos relativos à cobrança do cumprimento pelo fornecedor das obrigações contratualmente assumidas e a aplicação, observada a ampla defesa e o contraditório, de eventuais penalidades decorrentes do descumprimento de cláusulas contratuais, em relação às suas próprias contratações, devendo informar as ocorrências ao órgão gerenciador

h) A abrangência territorial da ata de registro de preços: Estados da Federação e Distrito Federal.

SEÇÃO VII
DA LEI GERAL DE PROTEÇÃO DE DADOS- LGPD

(✓) Informações da LGPD.

A empresa ao se credenciar para participação da presente licitação reconhece que tomou conhecimento do disposto na Lei Geral de Proteção de Dados- LGPD, que assume o compromisso e que adota na execução das suas atividades as medidas previstas na legislação de proteção de dados pessoais e dos seguintes pontos:

Do cumprimento da Lei Geral de Proteção de Dados - Lei n° 13.709/2018:

Inclui-se as seguintes obrigações da Contratada e da Contratante do Contrato:

a) É vedado às partes a utilização de todo e qualquer dado pessoal repassado em decorrência da execução contratual para finalidade distinta daquela do objeto da contratação, sob pena de responsabilização administrativa, civil e criminal.

b) As partes se comprometem a manter sigilo e confidencialidade de todas as informações em especial os dados pessoais e os dados pessoais sensíveis repassados em decorrência da execução contratual, em consonância com o disposto na Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), sendo vedado o repasse das informações a outras empresas ou pessoas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do instrumento contratual.

c) As partes responderão administrativa e judicialmente em caso de danos patrimoniais, morais, individuais ou coletivos, aos titulares de dados pessoais repassados em decorrência da execução contratual, por inobservância à Lei Geral de Proteção de Dados.

d) Em atendimento ao disposto na Lei Geral de Proteção de Dados, a CONTRATANTE, para a execução do serviço objeto deste contrato, tem acesso a dados pessoais dos representantes da CONTRATADA, tais como número do CPF e do RG, endereços eletrônico e residencial, e cópia do documento de identificação.

e) A CONTRATADA declara que tem ciência da existência da Lei Geral de Proteção de Dados e se compromete a adequar todos os procedimentos internos ao disposto na legislação com o intuito de proteger os dados pessoais repassados pelo CONTRATANTE.

f) A CONTRATADA fica obrigada a comunicar ao CONTRATANTE em até 48 (quarenta e oito) horas qualquer incidente de acessos não autorizados aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, bem como adotar as providências dispostas no art. 48 da Lei Geral de Proteção de Dados.

g) "Leis Aplicáveis à Proteção de Dados" significa todas as leis, normas e regulamentos que regem o tratamento de dados pessoais, em especial, a Lei Geral de Proteção de Dados (Lei Federal n. 13.709/2018, "LGPD"), além das normas e dos regulamentos adotados ou a serem adotados pela Defensoria Pública do Estado da Bahia, e determinações de órgãos reguladores/fiscalizadores sobre a matéria.

h) As expressões utilizadas no presente contrato, tais como, 'titular dos dados', 'dados pessoais', 'tratamento', 'violação de dados pessoais', etc., serão interpretadas com base no significado atribuído pela LGPD.

i) A Defensoria Pública do Estado da Bahia/Contratante agirá como "controlador", nos termos do art.5°, VI da Lei nº13.709/2018, e a Contratada assume o papel como "operador", nos termos do art. 5º, VII, da mesma Lei 13.709/2018, no sentido estrito da LGPD, salvo nos casos em que o operador/Contratado(a), passe a atuar em desconformidade com as orientações do "controlador/Contratante", passando assim a se responsabilizar como controlador, perante os órgãos de controle/fiscalização.

j) O Contratado(a) declara que conhece a Política de Governança de Privacidade e de Proteção de Dados Pessoais da Defensoria Pública do Estado da Bahia (Portaria nº 811, de 30.08.2021, publicada no DOE/DPE de 31/08/2021), e se compromete ao seu cumprimento e fiel observância, tudo de conformidade com o art. 39, da Lei nº 13.709/2018.

DA CONFIDENCIALIDADE NA RELAÇÃO CONTRATUAL

II - Inclui-se, ainda, as seguintes obrigações à Cláusula Sétima (OBRIGAÇÕES DA CONTRATADA) do presente Contrato:

a) O Contratado será expressamente responsabilizado quanto à manutenção de sigilo absoluto sobre quaisquer dados, informações, artefatos, contidos em quaisquer documentos e em quaisquer mídias, de que venha a ter conhecimento durante a execução do contrato, não podendo, sob qualquer pretexto divulgar, reproduzir ou utilizar, sob pena de sanções legais, independentemente da classificação de sigilo conferida pela Defensoria Pública do Estado da Bahia a tais documentos ou dados, mesmo após a conclusão do vínculo contratual.

b) Será mantido em rigoroso sigilo e confidencialidade as informações, não podendo divulgar a terceiros, por quaisquer meios, qualquer informação, documento e material produzido a que tenha ou venha a ter acesso durante a vigência deste Contrato, e em razão do serviço objeto do presente Contrato, que não seja conhecida do público em geral.

c) O Contratado não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos ou de que tenha tomado conhecimento em decorrência da execução do objeto do contrato, sem autorização da Autoridade Competente da Defensoria Pública do Estado da Bahia, por escrito, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos.

d) Toda a produção intelectual, inovações e de toda e qualquer documentação, dados, relatórios, além de materiais e outros gerados em razão da prestação de serviços é de propriedade da Defensoria Pública do Estado da Bahia.

e) O descumprimento da obrigação de sigilo e confidencialidade sujeitará o Contratado ao pagamento, ou recomposição, de todas as perdas e danos resultantes do descumprimento, bem como a sua responsabilização civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo, nos termos do Regulamento Interno de Licitações e Contratos - RILC (normativos competentes e aplicáveis) da Defensoria Pública do Estado da Bahia.

Defensoria Pública
BAHIA

PARTE IV – CONTRATO

MINUTA DO CONTRATO

CONTRATO Nº XX/2023

CONTRATO QUE ENTRE SI CELEBRAM A DEFENSORIA PÚBLICA DO ESTADO DA BAHIA E A [PESSOA JURÍDICA] PARA OS FINS QUE NELE SE DECLARAM.

A DEFENSORIA PÚBLICA DO ESTADO DA BAHIA, neste ato representado pelo Defensor Público Geral, titular da DPE, CNPJ n° 07.778.585/0001-14, situada na Avenida Ulisses Guimaraes, n° 3386, Sussuarana, Salvador (BA), CEP 41.219-000, autorizado pelo Decreto de delegação de competência, doravante denominado **CONTRATANTE**, e a **[PESSOA JURÍDICA/PESSOA NATURAL**], CNPJ nº_____, Inscrição Estadual/Municipal nº _____, situada na _____, neste ato representada pelo Sr. _____, portador da cédula de identidade nº _____, emitida por _____, inscrito no CPF/MF sob o nº _____, adjudicatária do Pregão Eletrônico 17/2023, Processo Administrativo nº 01.0485.2023.000003249-0 , doravante denominada **CONTRATADA**, celebram o presente contrato, que se regerá pela Lei estadual nº 9.433/05, pelas normas gerais da Lei nº 8.666/93, e respectivas alterações, bem como pela legislação específica, mediante as cláusulas e condições a seguir ajustadas

CLÁUSULA PRIMEIRA – OBJETO

Constitui objeto Registro de preço, para eventual aquisição de soluções de Segurança da Informação com o propósito de ampliar a segurança da rede da DPE/BA, incluindo repasse de conhecimento, manutenção e suporte técnico por 60 (sessenta) meses de acordo com as condições, características e especificações constantes da Seção II -Termo de Referência objeto da licitação e da proposta apresentada pela CONTRATADA, que integram este instrumento na qualidade de Anexos I e II, respectivamente.

§1º A CONTRATADA fica obrigada a aceitar, nas mesmas condições contratuais, acréscimos ou supressões que se fizerem no objeto, de até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato, na forma dos §1º e 2º do art. 143 da Lei estadual nº 9.433/05.

§2º As supressões poderão ser superiores a 25% (vinte e cinco por cento), desde que haja resultado de acordo entre os contratantes.

§3º É vedada a subcontratação parcial do objeto, a associação da CONTRATADA com outrem, a cessão ou transferência, total ou parcial do contrato, não se responsabilizando o CONTRATANTE por nenhum compromisso assumido por aquela com terceiros. **[NOTA: subcontratação vedada]**

CLÁUSULA SEGUNDA – PRAZO

O prazo de vigência do contrato, a contar da data da sua assinatura será de 12 (doze) meses, admitindo-se a sua prorrogação nos termos do inc. II do art. 140 da Lei estadual nº 9.433/05.

§1º A prorrogação do prazo de vigência está condicionada à obtenção de preços e condições mais vantajosas.

§2º A prorrogação deverá ser previamente justificada e autorizada pela autoridade competente para celebrar o ajuste e será realizada por meio de termo aditivo, devendo o pedido ser realizado no prazo máximo de 60 (sessenta) dias antes do término do contrato.

§3º O prazo de entrega deverá ser de até 60 (sessenta) dias corridos, contados da data da assinatura do contrato.

CLÁUSULA TERCEIRA – REGIME DE EXECUÇÃO

(**X**) **Serviço** com empreitada por preço ( ) global (X) Unitário

§ 1ºCONDIÇÕES DO FORNECIMENTO

I. Todos os equipamentos a serem fornecidos deverão ser novos, estar em linha de produção e fabricação atual do fabricante, não se encontrando nas fases de "End of Sale", "End of Support" ou qualquer outra que indique que já está na direção descendente de seu ciclo de vida.

II. A CONTRATADA deverá entregar, às suas expensas, todos os itens acessórios de hardware necessários à perfeita instalação e funcionamento dos equipamentos, incluindo conectores, cabos, suportes e demais itens necessários para instalação e funcionamento da solução contratada, em plena compatibilidade com as especificações constantes neste Termo de Referência e recomendadas pelo fabricante.

III. Todos os equipamentos fornecidos e seus componentes deverão ser novos, de primeiro uso e devem estar acondicionados adequadamente em caixa original lacrados de fábrica, de forma a propiciar completa segurança durante e transporte.

IV. Toda a solução e suas implantações serão supervisionadas pela Defensoria Pública.

V. A CONTRATADA será responsável por projetar, instalar, configurar e dar suporte na solução ofertada durante todo o período de licenciamento e garantia das licenças.

VI. A implementação das políticas de segurança será de responsabilidade exclusiva da CONTRATADA mediante determinações da CONTRATANTE.

VII. Observar as demais condições do Termo de Referência.

§2° ENTREGA, ACEITE E INSTALAÇÃO

I. O aceite do software será feito pela DPE/BA, após a implantação e entrada em operação das licenças fornecido;

II. A entrega e instalação das licenças será feita de acordo com plano de implantação, apresentado pela CONTRATADA e aprovado pela CONTRATANTE;

III. A instalação deverá seguir cronograma previsto no plano de implantação;

IV. Como parte dos documentos de aceite do software fornecido, a CONTRATADA deverá apresentar "Tabela de Comprovação Técnica " das especificações exigidas no Termo de Referência.

CLÁUSULA QUARTA – PREÇO

O CONTRATANTE pagará à CONTRATADA pelos serviços efetivamente prestados os valores abaixo especificados:

LOTE ÚNICO – (EQUIPAMENTOS PARA SEGURANÇA DA INFORMAÇÃO)				
ITEM	**DESCRIÇÃO**	**QUANTIDADE**	**VALOR UNITÁRIO**	**VALOR TOTAL**
01	SOLUÇÃO DE SEGURANÇA E GERENCIA DE REDES NGFW **EM CLUSTER** – TIPO 1	01	R$	R$
02	SOLUÇÃO DE SEGURANÇA E GERENCIA DE REDES NGFW – TIPO 2	03	R$	R$
03	SOLUÇÃO DE SEGURANÇA E GERENCIA DE REDES NGFW – TIPO 3	13	R$	R$
04	UNIDADE CENTRALIZADA DE ARMAZENAMENTO DE LOGS E RELATORIA	01	R$	R$
05	UNIDADE DE GERÊNCIA CENTRALIZADA DE EQUIPAMENTOS	01	R$	R$
06	ATIVOS DE REDE WIRELESS INDOOR	80	R$	R$
07	SOLUÇÃO DE SEGURANÇA, FIREWALL DE APLICAÇÕES WEB, DORAVANTE DENOMINADO SOLUÇÃO WAF, COM SUPORTE, GARANTIA E ATUALIZAÇÕES	01	R$	R$
08	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO PARA SOLUÇÃO DE SEGURANÇA E GERÊNCIA DE REDES NGFW EM CLUSTER DE ALTA DISPONIBILIDADE	01	R$	R$
09	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO PARA SOLUÇÃO DE SEGURANÇA E GERENCIA DE REDES NGFW TIPOS "2" E "3"	16	R$	R$
10	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO DE UNIDADE CENTRALIZADA DE ARMAZENAMENTO DE LOGS E RELATORIA	01	R$	R$
11	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO DE UNIDADE DE GERENCIA CENTRALIZADA DE EQUIPAMENTOS.	01	R$	R$
12	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO DOS ATIVOS DE REDE WIRELESS INDOOR	80	R$	R$
13	SERVIÇOS PROFISSIONAIS DE IMPLANTAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO DE SEGURANÇA WAF	01	R$	R$
			VALOR TOTAL GLOBAL (R$)	**R$**

§1º Estima-se para o contrato o valor global de R$

§2º Nos preços contratados estão incluídos todos os custos com material de consumo, salários, encargos sociais, previdenciários e trabalhistas de todo o pessoal da CONTRATADA, como também fardamento, transporte de qualquer natureza, materiais empregados, inclusive ferramentas, utensílios e equipamentos utilizados, depreciação, aluguéis, administração, tributos, impostos, taxas, emolumentos e quaisquer outros custos que, direta ou indiretamente, se relacionem com o fiel cumprimento pela CONTRATADA das obrigações.

CLÁUSULA QUINTA – GARANTIA

(**X**) A garantia contratual será de **5% (cinco por cento)** do valor do contrato, podendo recair sobre qualquer das modalidades previstas no §1º do art. 136 da Lei estadual nº 9.433/05.

§1º Sob pena da caracterização de inadimplemento contratual, a prova da garantia, na hipótese de opção pela modalidade caução em dinheiro ou títulos da dívida pública, deverá ser apresentada no prazo máximo de 05 (cinco) dias contados da data de assinatura do contrato, admitindo-se, para o seguro-garantia e a fiança bancária, que a comprovação seja feita no prazo máximo de 30 (trinta) dias daquela data, sem o que fica vedada, em qualquer caso, a realização de pagamento.

§2º A garantia responderá pelo inadimplemento das obrigações contratuais e pelas multas impostas, independentemente de outras cominações legais.

A CONTRATADA ficará obrigada a repor o valor da garantia quando esta for utilizada, bem como a atualizar o seu valor nas mesmas condições do contrato.

§4º No caso de seguro-garantia ou fiança bancária, não será admitida a existência de cláusulas que restrinjam ou atenuem a responsabilidade do segurador ou fiador.

§5º A CONTRATADA deverá atualizar a garantia sempre que houver alteração contratual, no mesmo prazo deferido para a comprovação da garantia originária, visando assegurar a cobertura das modificações procedidas.

§6º Será recusada a garantia que não atender às especificações solicitadas, devendo ser notificada a CONTRATADA para que, no prazo de 05 (cinco) dias, sane a incorreção apontada ou, no caso de títulos da dívida pública, seguro-garantia ou fiança bancária, promova a substituição por caução em dinheiro.

§7º O retardamento, a falta da apresentação ou a não substituição da garantia impedirá a realização do pagamento das faturas apresentadas, sem prejuízo da incidência de multa moratória, da rescisão do contrato nos termos do art. 167, inc. III, da Lei nº 9.433/05 e das demais cominações legais.

§8º A devolução da garantia ocorrerá após o recebimento definitivo da totalidade do objeto do contrato, com a demonstração de cumprimento, pela CONTRATADA, das obrigações pactuadas.

§9° Conforme Termo de Referência, observar para fins de garantia e assistência técnica:

I. Todos os componentes de hardware e software, deverão possuir garantia de, no mínimo, 60 (sessenta) meses, com suporte técnico de 8 (oito) horas por dia, 5 (cinco) dias por semana, na cidade de Salvador (BA).

II. O serviço deverá ser prestado por profissional de nível superior, devidamente certificado nas soluções tecnológicas utilizadas na prestação dos serviços contratados.

III Durante o período de execução dos serviços, a CONTRATADA deverá garantir o funcionamento do software, com suporte técnico do FABRICANTE prestado em caso de falha.

IV Deverá ser garantida, neste prazo, a atualização de versões, releases, componentes (bibliotecas, filtros, dentre outros) e módulos dos softwares e equipamentos utilizados na prestação dos serviços.

CLÁUSULA SEXTA – DOTAÇÃO ORÇAMENTÁRIA

As despesas para o pagamento deste contrato correrão por conta dos recursos da Dotação Orçamentária a seguir especificada:

Unidade FIPLAN	Atividade/Projeto	Elemento de Despesa	Fonte	Região/planejamento

CLÁUSULA SÉTIMA – OBRIGAÇÕES DA CONTRATADA

A CONTRATADA, além das determinações contidas no instrumento convocatório, bem como daquelas decorrentes de lei, obriga-se a:

I. designar de sua estrutura administrativa um preposto permanentemente responsável pela perfeita execução do contrato, inclusive para atendimento de emergência, servindo de interlocutor e canal de comunicação entre as partes;

II. executar o objeto deste contrato de acordo com as especificações técnicas constantes do instrumento convocatório e do presente contrato, nos locais, dias, turnos e horários determinados;

III. manter, sob sua exclusiva responsabilidade, toda a supervisão, direção e recursos humanos para execução completa e eficiente do objeto deste contrato;

IV. zelar pela boa e completa execução dos serviços contratados e facilitar, por todos os meios ao seu alcance, a ampla ação fiscalizadora dos prepostos designados pelo CONTRATANTE, atendendo prontamente às observações e exigências que lhe forem solicitadas;

V. comunicar ao CONTRATANTE qualquer anormalidade que interfira no bom andamento dos serviços;

VI. atender com presteza as reclamações sobre a qualidade dos serviços executados, providenciando sua imediata correção, sem ônus para o CONTRATANTE;

VII. respeitar e fazer com que seus empregados respeitem as normas de segurança do trabalho, disciplina e demais regulamentos vigentes no CONTRATANTE, bem como atentar para as regras de cortesia no local onde serão executados os serviços;

VIII. reparar, repor ou restituir, nas mesmas condições e especificações, dentro do prazo que for determinado, os equipamentos e utensílios eventualmente recebidos para uso nos serviços objeto deste contrato, deixando as instalações na mais perfeita condição de funcionamento;

IX. arcar com todo e qualquer dano ou prejuízo de qualquer natureza causado ao CONTRATANTE e terceiros, por sua culpa, ou em conseqüência de erros, imperícia própria ou de auxiliares que estejam sob sua responsabilidade, bem como ressarcir o equivalente a todos os danos decorrentes de paralisação ou interrupção dos serviços contratados, exceto quando isto ocorrer por exigência do CONTRATANTE ou ainda por caso fortuito ou força maior, circunstâncias que deverão ser comunicadas no prazo de 48 (quarenta e oito) horas após a sua ocorrência;

X. manter durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação, inclusive de apresentar, ao setor de liberação de faturas e como condição de pagamento, os documentos necessários;

XI. providenciar e manter atualizadas todas as licenças e alvarás junto às repartições competentes, necessários à execução dos serviços;

XII. efetuar pontualmente o pagamento de todas as taxas e impostos que incidam ou venham a incidir sobre as suas atividades e/ou sobre a execução do objeto do presente contrato;

XIII. adimplir os fornecimentos exigidos pelo instrumento convocatório e pelos quais se obriga, visando à perfeita execução deste contrato;

XIV. emitir notas fiscais/faturas de acordo com a legislação;

XV. observar a legislação federal, estadual e municipal relativa ao objeto do contrato;

XVI. executar os serviços sem solução de continuidade durante todo o prazo da vigência do contrato;

XVII. prover as instalações, aparelhamento e pessoal técnico exigidos na licitação;

XVIII. alocar durante todo o período de execução do objeto a equipe técnica mínima exigida no instrumento convocatório, admitindo-se a sua substituição por profissionais de experiência equivalente ou superior, desde que aprovada pelo CONTRATANTE.

XIX. providenciar o cadastramento de seu representante legal ou procurador no site www.defensoria.ba.def.br, para a prática de atos através do Sistema Eletrônico de Informações – SEI-DPE/BA.

§1º Além do quanto descrito acima, deverá observar as condições do Termo de Referência e as especificações abaixo:

I. Fornecer o(s) equipamento(s) conforme especificações, quantidades, prazos e demais condições estabelecidas no Edital, na Ata de Registro de Preços, na Ordem de Fornecimento, na Proposta e no Contrato;

II. Fornecer a documentação necessária à instalação e à operação dos produtos (manuais, termos de garantia, etc.), completa, atualizada e em português do Brasil, caso exista, ou em inglês;
III. Disponibilizar Central de Atendimento para a abertura e fechamento de chamados técnicos, conforme períodos, horários e condições estabelecidas no Edital e em seus Anexos;
IV. Comunicar formal e imediatamente ao Gestor ou Responsável Técnico da Administração sobre mudanças nos dados para contato com a Central de Atendimento;
V. Prestar as informações e os esclarecimentos que venham a ser solicitados pelo representante da Administração, referentes a qualquer problema detectado ou ao andamento de atividades da garantia;
VI. Comunicar imediatamente ocorrências de qualquer natureza que impeçam o bom andamento do serviço;
VII. Responder por quaisquer prejuízos que seus profissionais causarem ao patrimônio da Administração ou a terceiros, por ocasião da execução do objeto, procedendo imediatamente aos reparos ou às indenizações cabíveis e assumindo o ônus decorrente;
VIII. Responsabilizar-se integralmente pelo fornecimento dos equipamentos e pela execução dos serviços de garantia técnica, primando pela qualidade, desempenho, eficiência e produtividade na execução dos trabalhos, dentro dos prazos estipulados e cujo descumprimento será considerado infração passível de aplicação das penalidades previstas neste Termo de Referência;
IX. Comunicar ao Gestor ou Responsável Técnico, formal e imediatamente, todas as ocorrências anormais e/ou que possam comprometer a execução do objeto;
X. Manter sigilo sobre todo e qualquer assunto de interesse da Administração ou de terceiros de que tomar conhecimento em razão da execução do objeto, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, regras de negócios, documentos, entre outros pertinentes, sob pena de responsabilidade civil, penal e administrativa;
XI. Cumprir e garantir que seus profissionais estejam cientes, aderentes e obedeçam rigorosamente às normas e aos procedimentos estabelecidos na Política de Segurança da Informação da DPE/BA;
XII. Responsabilizar-se pela conservação dos ambientes onde desempenhe as atividades necessárias para prestar, se for o caso;
XIII. Prestar as informações e os esclarecimentos que venham a ser solicitados pela Administração, referentes a qualquer problema detectado ou ao andamento de atividades da garantia técnica;
XIV. Responsabilizar-se por todas as despesas de instalação inicial, suporte técnico remoto bem como deslocamento dos seus técnicos ao local da instalação e manutenção dos equipamentos, seja para retirada e/ou entrega, incluindo todas as despesas de transporte, frete e seguro correspondentes;
XV. A contratada não poderá transferir a outrem os compromissos assumidos, no todo ou em parte dos serviços objeto desta contratação;
XVI. Assegurar a correta integração e funcionalidade dos serviços, em função do projeto e das especificações técnicas constantes neste Termo de Referência;
XVII. Arcar com todas as despesas, diretas ou indiretas, decorrente do cumprimento das obrigações assumidas sem qualquer ônus a DPE/BA;
XVIII. Responsabilizar-se integralmente com todas as despesas inerentes à execução dos serviços, tais como, combustíveis, manutenção, seguros, taxas, impostos, tributos e salários;
XIX. Zelar pela boa e completa execução dos serviços e facilitar, por todos os meios ao seu alcance, a ampla ação fiscalizadora dos prepostos designados pela DPE/BA, atendendo prontamente às observações e exigências que lhe forem solicitadas.

§2º QUANTO AO TERMO DE REFERENCIA, SUPORTE TÉCNICO E ACORDO DE NÍVEL DE SERVIÇO:

I. Atender às necessidades da DPE/BA para suporte técnico de todas as Soluções de Segurança da Informação que compõem esse termo de referência, compreendendo hardware e software, com o objetivo de proteger a rede corporativa e aumentar o nível de conformidade com a política de segurança.
II. Composta de técnicos certificados pelo fabricante do software fornecido, e preparada para dar todo o suporte técnico e ajuda necessária para maximizar os benefícios oferecidos pelo software, aumentando a sua performance.
III. O suporte técnico ao produto fornecido deverá ser através de contato Telefônico (telefone 0800 do fabricante ou telefone com numeração comum do fornecedor), Sitio de Internet (website do fabricante ou do fornecedor), Correio Eletrônico (e-mail do fabricante ou do fornecedor) ou no Local (provido pelo fabricante ou pelo fornecedor), em casos de grande emergência;
IV. O suporte técnico deverá ser fornecido pelo fornecedor da solução de segurança ou pelo fabricante, no Brasil e na língua portuguesa;
V. Deverão ser executados pela empresa CONTRATADA serviços de Instalação e configuração para uso da solução CONTRATADA com supervisão da equipe técnica da DPE/BA;
VI. Deverá ser executada pela empresa CONTRATADA uma análise da situação atual e elaborar, em conjunto com a

equipe interna da DPE/BA, um plano de otimização de recursos, rotinas, procedimentos e processos para o novo ambiente de segurança. Essa documentação deverá ser entregue, pela empresa CONTRATADA, em formato digital;

VII. A empresa CONTRATADA deverá preservar todo ambiente computacional existente, de forma a manter a integridade dos dados, aplicativos e sistemas operacionais em funcionamento;

VIII. A empresa CONTRATADA deverá preparar o ambiente de modo a operar conforme o estabelecido no plano de otimização de recursos, rotinas, procedimentos e processos;

IX. A instalação e configuração da solução deverá ser realizada de acordo com o horário de funcionamento da DPE/BA, de segunda à sexta-feira, das 8:30 às 18:00h, em horário e dia a serem combinados entre a DPE/BA e a CONTRATADA;

X. Deverá ser oferecido treinamento hands-on de atualização tecnológica das soluções implantadas, com o mínimo de 16 (dezesseis) horas, em dias úteis, nas instalações da contratante, na cidade de Salvador, para no mínimo 2 (dois) técnicos da DPE/BA;

XI. O treinamento ou hands-on deverá ser iniciado imediatamente após a instalação e configuração das licenças;

XII. 2O prazo de execução dos serviços de Instalação e configuração para uso da solução de segurança no parque omputacional da DPE/BA deverá ser concluído em no máximo 45 (quarenta e cinco) dias consecutivos, a contar da data da entrega das licenças;

XIII. A empresa CONTRATADA deverá realizar duas avaliações on-site durante o período de vigência do contrato, perante solicitação da CONTRATANTE, do ambiente da DPE/BA, mediante verificação de instalações e configurações de toda a solução de segurança, adequando-as às melhores práticas, essa atividade deve gerar relatório para posterior melhoria pela equipe da DPE/BA;

XIV. O suporte técnico deverá ser prestado nas seguintes formas:

XV. Plantão Telefônico, Website e E-mail - Serviço de uso ilimitado, no período de 8 (oito) horas por dia, 5 (cinco) dias por semana;

No Local (on site) - Serviço de uso ilimitado para atividades não solucionadas através de atendimento remoto, prestado em caso de emergência, ou outra necessidade maior e também compreendendo os seguintes tipos de atendimento local previstos: suporte para upgrade de versões e releases do software; solução de problemas detectados (troubleshoot); análise e correção de eventos relacionados à segurança e à performance do software e do ambiente; integração dos ambientes da configuração do software na rede da DPE/BA. Neste caso a CONTRATADA deve possuir plantão de 8 (oito) horas por dia, 5 (cinco) dias por semana, para este tipo de atendimento;

XVI. Para a execução do suporte técnico, a CONTRATADA deverá contar com equipe técnica certificada pelo fabricante e com suporte ilimitado (quantidade de chamados) ao centro de suporte mundial do fabricante a nível internacional, a fim de garantir transferência diretamente ao fabricante dos problemas de maior complexidade que não tenham sido resolvidos em seu próprio laboratório;

XVII. O encaminhamento de chamados deverá ser efetuado pelos técnicos responsáveis no prazo máximo conforme os níveis de severidade indicados no item 6. Após este prazo, em caso de não solução, a CONTRATADA deverá acionar o atendimento, no local designado pela DPE/BA, de acordo com o nível de serviço acordado. O suporte prestado pela empresa terá chamados ilimitados;

XVIII. O atendimento no Local (on site) quando necessário deve ser provido nas unidades da DPE/BA, nos endereços informados no item 17.

XIX A CONTRATADA deverá responder aos acionamentos, dentro dos prazos fixados no item 11, a partir da abertura do acionamento;

XX O término do atendimento deverá ocorrer dentro dos prazos fixados no item 11, a partir do contato do técnico da CONTRATADA, responsável pelo atendimento;

XXI Entende-se por início do atendimento a hora do contato do técnico de suporte da CONTRATADA com a equipe da CONTRATANTE;

XXII Entende-se por término de atendimento a disponibilidade do produto para uso em perfeitas condições de funcionamento no local onde está instalado;

XXIII O nível de severidade será informado pela CONTRATANTE no momento da abertura de cada chamado;

XXIV O nível de severidade poderá ser reclassificado a critério da CONTRATANTE. Caso isso ocorra haverá o início de nova contagem de prazo, conforme o novo nível de severidade;

XXV Todas as solicitações de suporte técnico devem ser registradas pela CONTRATADA, para acompanhamento e controle da execução do serviço;

XXVI A CONTRATADA deverá apresentar relatório de atendimento para cada solicitação de suporte, contendo data e hora da solicitação de suporte técnico, do início e do término do atendimento, identificação do problema, providências adotadas e demais informações pertinentes;

XXVII O relatório de atendimento deverá ser assinado pelo servidor da CONTRATANTE que solicitou o suporte técnico;

XXVIII Para a execução do atendimento, é necessária a autorização da CONTRATANTE para instalação ou desinstalação de quaisquer softwares ou equipamentos que não façam parte da solução de segurança fornecida.

XXIX Comprovação de Garantia: para assegurar a esta Instituição a garantia total solicitada e demais condições exigidas, será necessário comprovar por meio de documentação do FABRICANTE específica para este Processo licitatório, anexada à proposta comercial, que o equipamento ofertado terá garantia, mínima, de 5 (cinco) anos e tempo de atendimento exigidos no Edital.

§ 3° <u>ACORDO DE NÍVEL DE SERVIÇO (ANS)</u>

I. A CONTRATADA deverá possuir Central de Atendimento (contato telefônico, sítio na Internet e e-mail) para consultas, aberturas de chamados técnicos e envio de arquivos para análise, durante 8 (oito) horas por dia, 5 (cinco) dias por semana;

II. A CONTRATADA deverá prestar serviços de suporte técnico 8 horas por dia, 5 dias por semana, relativos à prestação do serviço objeto deste Termo de Referência, sem ônus para a CONTRATANTE;

III. Para efeito dos atendimentos técnicos, a CONTRATADA deverá observar os níveis de severidade e respectivos prazos máximos fixados abaixo;

IV. Todos os chamados, inclusive os que podem resultar em manutenção de natureza corretiva, bem como o fluxo de resolução de problemas, deverão ser documentados. Esta documentação, bem como outras geradas em processos de atendimento, auditorias, manutenção ou configurações, deverá ser entregue à CONTRATANTE através de relatórios (impressos ou em mídia digital) mediante solicitação.

V. A CONTRATADA deverá fazer análises dos chamados e enviar recomendações de possíveis treinamentos necessários ao desenvolvimento da equipe da CONTRATANTE.

VI. A CONTRATADA deverá apresentar relatório contendo as ações adotadas para a solução do problema.

VII. A CONTRATADA deverá disponibilizar à CONTRATANTE serviço de atendimento de um Gestor do contrato de Suporte, responsável este que será o ponto focal de todas as necessidades de suporte da CONTRATANTE para casos de escalações ou problemas de atendimento do Suporte Técnico. Caso a CONTRATADA tenha seus laboratórios em outros países que não seja o território nacional, o Gestor deverá ter fluência na língua para facilitar a comunicação entre as partes.

VIII. A CONTRATANTE permitirá o acesso dos técnicos credenciados pela CONTRATADA às instalações onde se encontrarem os equipamentos para a prestação dos serviços de manutenção. Entretanto, tais técnicos ficarão sujeitos às normas internas de segurança da CONTRATANTE, notadamente àquelas atinentes à identificação, trânsito e permanência nas dependências;

IX. Mesmo se permitido pela CONTRATANTE, a permanência do técnico além do tempo de resolução do problema, para a continuidade de solução de um problema, não deverá representar qualquer ônus adicional à CONTRATANTE.

X. Níveis de Serviço e Tempo Esperados:

a) Plantão Telefônico por número 0800 como serviço de uso ilimitado, no período de 8 (oito) horas por dia, 5 (cinco) dias por semana;

b) No Local (on site) – Serviço de uso ilimitado para atividades não solucionadas através do atendimento remoto, prestado em caso de emergência, ou outra necessidade maior e também compreendendo os seguintes tipos de atendimento local: suporte para upgrade de versões e releases do software; solução de problemas detectados (troubleshoot); análise e correção de eventos relacionados à segurança e à performance do software e do ambiente; atualização simultânea nos ambientes dos órgãos e entidades da CONTRATANTE.

c) Para efeito dos atendimentos técnicos, a CONTRATADA deverá observar os níveis de severidade e respectivos prazos máximos fixados abaixo:

NÍVEIS DE SEVERIDADE DOS CHAMADOS	
Nível	**Descrição**
1	Serviços totalmente indisponíveis.
2	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso aos aplicativos.
3	Serviços disponíveis com ocorrência de alarmes de avisos, consultas sobre problemas, dúvidas gerais sobre o equipamento fornecido.

Modalidade	Prazos	Níveis de Severidade		
		1	2	3
On Site Salvador e RMS	Início atendimento	1 hora útil	2 horas úteis	24 horas úteis
	Término atendimento	2 horas úteis	4 horas úteis	72 horas úteis
On Site Interior do Estado da Bahia	Início atendimento	4 horas úteis	8 horas úteis	24 horas úteis
	Término atendimento	8 horas úteis	16 horas úteis	72 horas úteis

Tabela de Prazos de Atendimento ao Software				
Modalidade	**Prazos**	**Níveis de Severidade**		
		1	**2**	**3**
Telefone, email e web	Início atendimento	-	-	24 horas
	Término atendimento	-	-	72 horas

d) Todo o chamado somente será caracterizado como "encerrado" mediante concordância da Coordenação de Modernização e Informática;

e) Para as situações em que a solução definitiva de problemas no ambiente demande reimplantação, reestruturação ou reinstalação do produto, este deverá ser programado e planejado, com a antecedência necessária, de modo a não prejudicar a operação dos demais sistemas da CONTRATANTE.

XI. A CONTRATADA deverá disponibilizar à CONTRATANTE um serviço preventivo de verificação e atualização de versões ou correções (patches) que se fizerem necessários, específicos para a solução ofertada, sem ônus para a CONTRATANTE;

XII. No caso de necessidade de ações preventivas ou corretivas a CONTRATANTE agendará com antecedência junto a CONTRATADA as implementações das correções, fora do horário comercial, preferencialmente em feriados e finais de semana, sem ônus para a CONTRATANTE;

XIII. A CONTRATADA deverá prestar suporte a todos os componentes de software fornecidos que forem necessários para a implementação e utilização da solução, sem ônus para a CONTRATANTE durante 60 (sessenta) meses.

XIV. A CONTRATADA deverá ainda realizar os seguintes suportes proativos:

a) Duas avaliações on-site por ano do ambiente da CONTRATANTE, mediante verificação de instalações e configurações de toda a solução, adequando-as às melhores práticas de segurança, essa atividade deve gerar relatório para posterior melhoria pela equipe da CONTRATANTE.

b) Uma avaliação on-site por ano do ambiente da CONTRATANTE, mediante verificação de instalações e configurações de toda a solução de gerência centralizada, adequando-as às melhores práticas de segurança, essa atividade deve gerar relatório para posterior melhoria pela equipe da CONTRATANTE.

c) Quatro visitas técnicas on-site na unidade de Salvador, durante o ano de profissionais certificados pelo fabricante para apoiar nas implementações e nos controles gerados pelas ações proativas.

§ 4° TESTE E VERIFICAÇÃO PRELIMINAR

I. Todos os componentes disponíveis nas licenças fornecidas serão testados por meio de procedimentos designados pela CONTRATANTE, findo os quais será elaborado relatório técnico com a análise dos resultados;

II. O processo de realização dos testes de verificação preliminar do software será desenvolvido de acordo com os eventos e atividades descritos a seguir:

a) Conferência da Entrega: consiste na identificação e conferência das licenças fornecidas;

b) Teste de Instalação: consiste na verificação da instalação e da configuração das funcionalidades instaladas;

c) Testes de Ativação: consiste na operacionalização do software, após a conclusão dos testes de instalação, com a verificação de suas características, de suas funcionalidades e de sua compatibilidade;

III. A verificação preliminar não implica em recebimento definitivo do software fornecido;

IV. O relatório gerado em função dos Testes de Verificação Preliminar será documento integrante do Termo de Recebimento e Aceitação do software fornecido.

§ 5° PROPRIEDADE INTELECTUAL

I. A CONTRATADA entregará a CONTRATANTE toda e qualquer documentação gerada em função da prestação de serviços decorrente deste Termo de Referência.

II. A CONTRATADA concorda que os direitos patrimoniais autorais relativos aos resultados produzidos durante a vigência do Contrato são de propriedade exclusiva da CONTRATANTE, devidamente amparada pela Lei nº 9.610/1998, de Diretos Autorais, respeitados os direitos morais do autor. Entendem-se por resultados quaisquer estudos, relatórios, especificações, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, páginas na Intranet e Internet e documentação didática em papel ou em mídia eletrônica.

III. A CONTRATADA fica proibida de veicular e comercializar todos e quaisquer produtos e informações geradas ou conhecidas relativas ao objeto da prestação dos serviços, salvo se houver a prévia autorização por escrito da CONTRATANTE.

CLÁUSULA OITAVA – OBRIGAÇÕES DO CONTRATANTE

O **CONTRATANTE,** além das obrigações contidas neste contrato por determinação legal, obriga-se a:

I. fornecer à CONTRATADA os elementos indispensáveis ao cumprimento do contrato no prazo máximo de 10 (dez) dias da assinatura;

II. realizar o pagamento pela execução do objeto contratual;

III. proceder à publicação resumida do instrumento de contrato e de seus aditamentos, na imprensa oficial, no prazo legal.

IV. A critério da DPE poderá ser feita inspeção do material, quando da sua entrega, para fins de verificação de conformidade com a especificação do item.

CLÁUSULA NONA – FISCALIZAÇÃO DO CONTRATO

Competirá ao CONTRATANTE proceder ao acompanhamento da execução do contrato, na forma do art. 154 da Lei estadual nº 9.433/05, ficando esclarecido que a ação ou omissão, total ou parcial da fiscalização não eximirá a CONTRATADA da total responsabilidade pela execução do contrato.

§1º O adimplemento da obrigação contratual por parte da CONTRATADA ocorrerá com a efetiva prestação do serviço, a realização da obra, a entrega do bem ou de parcela destes, bem como qualquer outro evento contratual cuja ocorrência esteja vinculada à emissão de documento de cobrança, nos termos do art. 8º, inc. XXXIV, da Lei estadual nº 9.433/05.

§2º Cumprida a obrigação pela CONTRATADA, caberá ao CONTRATANTE proceder ao recebimento do objeto, a fim de aferir os serviços ou fornecimentos efetuados, para efeito de emissão da habilitação de pagamento, conforme o art. 154, inc. V, e art. 155, inc. V, da Lei estadual nº 9.433/05.

§3º Compete especificamente à fiscalização, sem prejuízo de outras obrigações legais ou contratuais:

I. exigir da CONTRATADA o cumprimento integral das obrigações pactuadas;

II. rejeitar todo e qualquer material de má qualidade ou não especificado;

III. relatar ao Gestor do Contrato ocorrências ou circunstâncias que possam acarretar dificuldades no desenvolvimento dos serviços em relação a terceiros;

IV. dar à autoridade superior imediata ciência de fatos que possam levar à aplicação de penalidades contra a CONTRATADA, ou mesmo à rescisão do contrato.

§4º Fica indicada como a área responsável pela gestão do contrato: Coordenação de Serviços Administrativos-CSA.

§5º Fica indicado como gestor deste Contrato o servidor **_____,** matrícula: _____**[NOTA: alternativamente, a nomeação do gestor do contrato pode ser feita por portaria]**

§6º Fica(m) indicado(s) como fiscal(is) deste Contrato o(s) servidor(es): **_____** matrícula: _____ **[NOTA: alternativamente, a nomeação do fiscal e/ou comissão pode ser feita por portaria]**

CLÁUSULA DÉCIMA – RECEBIMENTO DO OBJETO

O recebimento do objeto, consistente na aferição da efetiva prestação do serviço, realização da obra, entrega do bem ou de parcela destes, se dará segundo o disposto no art. 161 da Lei estadual nº 9.433/05, observando-se os seguintes prazos, se outros não houverem sido fixados no Termo de Referência:

I. se a verificação da conformidade do objeto com a especificação, bem assim do cumprimento das obrigações acessórias puder ser realizada de imediato, será procedido de logo o recebimento definitivo;

II. quando, em razão da natureza, do volume, da extensão, da quantidade ou da complexidade do objeto, não for possível proceder-se a verificação imediata de conformidade, será feito o recebimento provisório, devendo ser procedido ao recebimento definitivo no prazo de 15 (quinze) dias.

§1º Nos casos de aquisição de equipamentos de grande vulto, o recebimento definitivo far-se-á mediante termo circunstanciado e, nos demais, mediante recibo.

§2º Na hipótese de não ser lavrado o termo circunstanciado ou de não ser procedida a verificação dentro dos prazos fixados, reputar-se-ão como realizados, desde que comunicados ao CONTRATANTE nos 15 (quinze) dias anteriores à exaustão dos mesmos

§3º O recebimento definitivo de compras ou serviços, cujo valor do objeto seja superior ao limite estabelecido para a modalidade de convite, deverá ser confiado a uma comissão de, no mínimo, 03 (três) membros.

§4º Esgotado o prazo de vencimento do recebimento provisório sem qualquer manifestação do CONTRATANTE, não dispondo o TERMO DE REFERÊNCIA de forma diversa, considerar-se-á definitivamente aceito pela Administração o objeto contratual, para todos os efeitos.

§5º Poderá ser dispensado o recebimento provisório nos seguintes casos:

I. gêneros perecíveis e alimentação preparada;

II. serviços profissionais;

III. serviços de valor até o limite previsto para compras e serviços, que não sejam de engenharia, na modalidade de convite, desde que não se componham de aparelhos, equipamentos e instalações sujeitos à verificação de funcionamento e produtividade.

§6º Salvo disposições em contrário constantes do TERMO DE REFERÊNCIA, os ensaios, testes e demais provas exigidas por normas técnicas oficiais para a boa execução do objeto do contrato correm por conta do contratado.

§7º O CONTRATANTE rejeitará, no todo ou em parte, obra, serviço ou fornecimento em desacordo com as condições pactuadas, podendo, entretanto, se lhe convier, decidir pelo recebimento, neste caso com as deduções cabíveis.

§8º O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança da obra ou do serviço, nem a ético-profissional pela perfeita execução do contrato, dentro dos limites estabelecidos pela lei ou pelo contrato.

§9º Com a conclusão da etapa do recebimento definitivo, a CONTRATADA estará habilitada a apresentar as nota(s) fiscal(is)/fatura(s) para pagamento.

CLÁUSULA DÉCIMA–PRIMEIRA - PAGAMENTO

Os pagamentos devidos à CONTRATADA serão efetuados através de ordem bancária ou crédito em conta ~~corrente~~ aberta em instituição financeira contratada pelo Estado da Bahia, no prazo não superior a 08 (oito) dias úteis, contados da data da apresentação da fatura, após concluído o recebimento definitivo, em consonância com o disposto no art. 6º, §5º; art. 8º, XXXIV; art. 79, XI, "a"; art. 154, V e art. 155, V da Lei estadual nº 9.433/05.

§1º A(s) nota(s) fisca(l)is/fatura(s) somente deverá(ao) ser apresentada(s) para pagamento após a conclusão da etapa do recebimento definitivo, indicativo da satisfação pela CONTRATADA de todas as obrigações pertinentes ao objeto contratado.

§2º Ainda que a nota fiscal/fatura seja apresentada antes do prazo definido para recebimento definitivo, o prazo para pagamento somente fluirá após o efetivo atesto do recebimento definitivo.

§3º O CONTRATANTE descontará da fatura mensal o valor correspondente às faltas ou atrasos no cumprimento da obrigação, com base no valor do preço vigente.

§4º A(s) nota(s) fisca(l)is/fatura(s) deverá(ao) atender as exigências legais pertinentes aos tributos e encargos relacionados com a obrigação, sujeitando-se às retenções tributárias previstas em lei, e, as situações específicas, à adoção da forma eletrônica.

§5º O processo de pagamento, para efeito do art. 126, inciso XVI, da Lei estadual nº 9.433/05, deverá ser instruído com a prova da manutenção das condições de habilitação e qualificação exigidas no certame, o que poderá ser aferido mediante consulta ao Registro Cadastral ou a sites oficiais, considerando-se como marco final desta demonstração a data de conclusão da etapa do recebimento definitivo.

§6º Em havendo alguma pendência impeditiva do pagamento, a exemplo de erro na apresentação da nota fiscal/fatura ou dos documentos pertinentes à contratação, ou, ainda, de circunstância que impeça a liquidação da despesa, como obrigações financeiras pendentes, decorrentes de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o CONTRATANTE.

§7º Em caso de mora nos pagamentos devidos pelo CONTRATANTE, será observado o que se segue:

I. a atualização monetária será calculada considerando a data do vencimento da obrigação e do seu efetivo pagamento, de acordo com a variação do INPC do IBGE *pro rata tempore*;

II. nas compras para entrega imediata, assim entendidas aquelas com prazo de entrega até 15 (quinze) dias contados da data da celebração do ajuste, será dispensada a atualização financeira correspondente ao período compreendido entre as datas do adimplemento e a prevista para o pagamento, desde que não superior a quinze dias, em conformidade com o inc. II do art. 82 da Lei nº 9.433/05.

§8º Optando a CONTRATADA por receber os créditos em instituição financeira diversa da indicada no **caput**, deverá arcar com os custos de transferências bancárias, os quais serão deduzidos dos pagamentos devidos.

CLÁUSULA DÉCIMA-SEGUNDA – MANUTENÇÃO DAS CONDIÇÕES DA PROPOSTA

Os preços contratados são fixos e irreajustáveis durante o prazo de 12 meses da data de apresentação da proposta.

§1º Após o prazo de 12 meses a que se refere o *caput*, a concessão de reajustamento será feita mediante a aplicação do INPC/IBGE, nos termos do inc. XXV do art. 8º da Lei estadual nº 9.433/05.

§2º A revisão de preços, nos termos do inc. XXVI do art. 8º da Lei estadual nº 9.433/05, dependerá de requerimento da CONTRATADA quando visar recompor o preço que se tornou *insuficiente*, devendo ser instruído com a documentação que comprove o desequilíbrio econômico-financeiro do contrato.

§3º O requerimento de revisão de preços deverá ser formulado pela CONTRATADA no prazo máximo de um ano a partir do fato que a ensejou, sob pena de decadência, em consonância com o art. 211 da Lei nº 10.406/02.

§4º A revisão de preços pode ser instaurada pelo CONTRATANTE quando possível a redução do preço ajustado para compatibilizá-lo ao valor de mercado ou quando houver diminuição, devidamente comprovada, dos preços dos insumos básicos utilizados no contrato, conforme o art. 143, inc. II, alínea "e", da Lei estadual nº 9.433/05.

CLÁUSULA DÉCIMA-TERCEIRA– ALTERAÇÕES CONTRATUAIS

A prorrogação, suspensão ou rescisão sujeitar-se-ão às mesmas formalidades exigidas para a validade deste contrato.

§1º A admissão da fusão, cisão ou incorporação da CONTRATADA está condicionada à manutenção das condições de habilitação e à demonstração, perante o CONTRATANTE, da inexistência de comprometimento das condições originariamente pactuadas para a adequada e perfeita execução do contrato.

§2º Independem de termo contratual aditivo, podendo ser registrado por simples apostila:

I. a simples alteração na indicação dos recursos orçamentários ou adicionais custeadores da despesa, sem modificação dos respectivos valores;

II. reajustamento de preços previsto no edital e neste contrato, bem como as atualizações, compensações ou apenações financeiras decorrentes das condições de pagamento dos mesmos constantes;

III. o empenho de dotações orçamentárias suplementares até o limite do seu valor corrigido.

CLÁUSULA DÉCIMA-QUARTA - INEXECUÇÃO E RESCISÃO

A inexecução total ou parcial do contrato ensejará a sua rescisão, com as conseqüências contratuais e as previstas na Lei estadual nº 9.433/05.

§1º A rescisão poderá ser determinada por ato unilateral e escrito do CONTRATANTE nos casos enumerados nos incisos I a XV, XX e XXI do art. 167 da Lei estadual nº 9.433/05.

§2º Quando a rescisão ocorrer com base nos incisos I e XVI a XX do art. 167 da Lei estadual nº 9.433/05, sem que haja culpa da CONTRATADA, será este ressarcido dos prejuízos regularmente comprovados que houver sofrido, na forma do §2º do art. 168 do mesmo diploma.

CLÁUSULA DÉCIMA-QUINTA – PENALIDADES

Constituem ilícitos administrativos as condutas previstas nos arts. 184, 185 e 199 da Lei estadual nº 9.433/05, sujeitando-se os infratores às cominações legais, especialmente as definidas no art. 186 do mesmo diploma, garantida a prévia e ampla defesa em processo administrativo.

§1º Para a aplicação das penalidades serão levados em conta a natureza e a gravidade da falta, os prejuízos dela advindos para a Administração Pública e a reincidência na prática do ato, observando-se os critérios de dosimetria estabelecidos pelo Decreto estadual nº 13.967/12.

§2º Serão punidos com a pena de declaração de inidoneidade para licitar e contratar com a Administração, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a autoridade competente para aplicar a punição, os que incorram nos ilícitos previstos nos incisos I a V do art. 184, nos incisos II, III e V do art. 185 e no art. 199 da Lei estadual nº 9.433/05.

§3º Serão punidos com a pena de suspensão temporária do direito de cadastrar e licitar e impedimento de contratar com a Administração os que incorram nos ilícitos previstos nos incisos VI e VII do art. 184 e nos incisos I, IV, VI e VII do art. 185 da Lei estadual nº 9.433/05.

§4º A CONTRATADA será descredenciada do Sistema de Registro Cadastral quando, em razão da ocorrência das faltas previstas na Lei estadual nº 9.433/05, deixar de satisfazer as exigências relativas à habilitação jurídica, qualificação técnica, qualificação econômico-financeira, regularidade fiscal e trabalhista exigidas para cadastramento.

§5º A inexecução contratual, inclusive por atraso injustificado na execução do contrato, sujeitará a CONTRATADA à multa de mora, na forma prevista na cláusula seguinte, que será graduada de acordo com a gravidade da infração, observado o disposto na Lei estadual nº 9.433/05 e no Decreto estadual nº 13.967/12.

CLÁUSULA DÉCIMA-SEXTA – SANÇÃO DE MULTA

A pena de multa será aplicada em função de inexecução contratual, inclusive por atraso injustificado na execução do contrato, sem prejuízo da rescisão unilateral do contrato, a qualquer tempo, e a aplicação das demais sanções previstas na Lei estadual nº 9.433/05.

§1º Quanto à obrigação principal, será observado o que se segue:

I. Em caso de descumprimento total da obrigação principal, será aplicada multa no percentual de 10% (dez por cento) incidente sobre o valor global do contrato.

II. Caso o cumprimento da obrigação principal, uma vez iniciado, seja descontinuado, será aplicado o percentual de 10% (dez por cento) sobre o saldo do contrato, isto é, sobre a diferença entre o valor global do contrato e o valor da parte do fornecimento ou do serviço já realizado.

III. O atraso no cumprimento da obrigação principal ensejará a aplicação de multa no percentual de 0,3% (três décimos por cento) ao dia, até o trigésimo dia de atraso, e de 0,7% (sete décimos por cento) por cada dia subseqüente ao trigésimo, calculados sobre o valor da parcela do fornecimento ou do serviço em mora.

§2º Quanto à obrigação acessória, assim considerada aquela que coadjuva a principal, será observado o que se segue:

I. Em caso de descumprimento total da obrigação acessória, será aplicada multa no percentual de 10% (dez por cento) incidente sobre o valor ou custo da obrigação descumprida.

II. Caso o cumprimento da obrigação acessória, uma vez iniciado, seja descontinuado, será aplicado o percentual de 5% (cinco por cento) sobre o valor ou custo da obrigação descumprida.

III. O atraso no cumprimento da obrigação acessória ensejará a aplicação de multa no percentual de 0,2% (dois décimos por cento) ao dia, até o trigésimo dia de atraso, e de 0,6% (seis décimos por cento) por cada dia subseqüente ao trigésimo, calculados sobre o valor ou custo da obrigação descumprida.

IV. Caso não seja possível identificar o valor ou custo da obrigação acessória descumprida, a multa será arbitrada pelo CONTRANTE, em valor que não supere 1% da sanção pecuniária que seria cabível pelo descumprimento da obrigação principal.

§3° Se a multa moratória atingir o patamar de 10% (dez por cento) do valor global do contrato, deverá, salvo justificativa escrita devidamente fundamentada, ser recusado o recebimento do objeto, sem prejuízo da aplicação das demais sanções previstas em lei.

§4º Na hipótese de o contratado se negar a efetuar o reforço da caução, dentro de 10 (dez) dias contados da data de sua convocação, será aplicada multa no percentual de 2,5% (dois e meio por cento) incidente sobre o valor global do contrato.

§5º As multas previstas nesta cláusula não têm caráter compensatório e o seu pagamento não eximirá a CONTRATADA da responsabilidade por perdas e danos decorrentes das infrações cometidas.

§6º A multa, aplicada após regular processo administrativo, será descontada da garantia do contratado faltoso.

§7º Se o valor da multa exceder ao da garantia prestada, além da perda desta, a CONTRATADA responderá pela sua diferença, que será descontada dos pagamentos eventualmente devidos pela Administração ou, ainda, se for o caso, cobrada judicialmente.

§8º Caso não tenha sido exigida garantia, à Administração se reserva o direito de descontar diretamente do pagamento devido à CONTRATADA o valor de qualquer multa porventura imposta.

CLÁUSULA DÉCIMA-SÉTIMA - VINCULAÇÃO AO INSTRUMENTO CONVOCATÓRIO

Integram o presente contrato, como se nele estivessem transcritas, as cláusulas e condições estabelecidas no processo licitatório, referido no preâmbulo deste instrumento, inclusive anexos e adendos, e na proposta da licitante vencedora.

CLÁUSULA DÉCIMA-OITAVA - COMUNICAÇÃO ELETRÔNICA

Fica pactuado que os atos de comunicação processual com a CONTRATADA poderão ser realizados por meio eletrônico, na forma do disposto na Lei nº 12.290, de 20 de abril de 2011, e do Decreto nº 15.805, de 30 de dezembro de 2014.

Parágrafo único. A CONTRATADA deverá manter atualizado o endereço eletrônico cadastrado no Sistema Eletrônico de Informações - SEI, para efeito do recebimento de notificação e intimação de atos processuais.

CLÁUSULA DÉCIMA-NONA - DO CUMPRIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS - LEI N° 13.709/2018:

I – Inclui-se as seguintes obrigações da Contratada e da Contratante do Contrato:

a) É vedado às partes a utilização de todo e qualquer dado pessoal repassado em decorrência da execução contratual para finalidade distinta daquela do objeto da contratação, sob pena de responsabilização administrativa, civil e criminal.

b) As partes se comprometem a manter sigilo e confidencialidade de todas as informações em especial os dados pessoais e os dados pessoais sensíveis repassados em decorrência da execução contratual, em consonância com o disposto na Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), sendo vedado o repasse das informações a outras empresas ou pessoas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do instrumento contratual.

c) As partes responderão administrativa e judicialmente em caso de danos patrimoniais, morais, individuais ou coletivos, aos titulares de dados pessoais repassados em decorrência da execução contratual, por inobservância à Lei Geral de Proteção de Dados.

d) Em atendimento ao disposto na Lei Geral de Proteção de Dados, a CONTRATANTE, para a execução do serviço objeto deste contrato, tem acesso a dados pessoais dos representantes da CONTRATADA, tais como número do CPF e do RG, endereços eletrônico e residencial, e cópia do documento de identificação.

e) A CONTRATADA declara que tem ciência da existência da Lei Geral de Proteção de Dados e se compromete a adequar todos os procedimentos internos ao disposto na legislação com o intuito de proteger os dados pessoais repassados pelo CONTRATANTE.

f) A CONTRATADA fica obrigada a comunicar ao CONTRATANTE em até 48 (quarenta e oito) horas qualquer incidente de acessos não autorizados aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, bem como adotar as providências dispostas no art. 48 da Lei Geral de Proteção de Dados.

g) "Leis Aplicáveis à Proteção de Dados" significa todas as leis, normas e regulamentos que regem o tratamento de dados pessoais, em especial, a Lei Geral de Proteção de Dados (Lei Federal n. 13.709/2018, "LGPD"), além das normas e dos regulamentos adotados ou a serem adotados pela Defensoria Pública do Estado da Bahia, e determinações de órgãos reguladores/fiscalizadores sobre a matéria.

h) As expressões utilizadas no presente contrato, tais como, 'titular dos dados', 'dados pessoais', 'tratamento', 'violação de dados pessoais', etc., serão interpretadas com base no significado atribuído pela LGPD.

i) A Defensoria Pública do Estado da Bahia/Contratante agirá como "controlador", nos termos do art.5°, VI da Lei nº13.709/2018, e a Contratada assume o papel como "operador", nos termos do art. 5º, VII, da mesma Lei 13.709/2018, no sentido estrito da LGPD, salvo nos casos em que o operador/Contratado(a), passe a atuar em desconformidade com as orientações do "controlador/Contratante", passando assim a se responsabilizar como controlador, perante os órgãos de controle/fiscalização.

j) O Contratado(a) declara que conhece a Política de Governança de Privacidade e de Proteção de Dados Pessoais da Defensoria Pública do Estado da Bahia (Portaria nº 811, de 30.08.2021, publicada no DOE/DPE de 31/08/2021), e se compromete ao seu cumprimento e fiel observância, tudo de conformidade com o art. 39, da Lei nº 13.709/2018.

DA CONFIDENCIALIDADE NA RELAÇÃO CONTRATUAL

II - Inclui-se, ainda, as seguintes obrigações à Cláusula Sétima (OBRIGAÇÕES DA CONTRATADA) do presente Contrato:

a) O Contratado será expressamente responsabilizado quanto à manutenção de sigilo absoluto sobre quaisquer dados, informações, artefatos, contidos em quaisquer documentos e em quaisquer mídias, de que venha a ter conhecimento durante a execução do contrato, não podendo, sob qualquer pretexto divulgar, reproduzir ou utilizar, sob pena de sanções legais, independentemente da classificação de sigilo conferida pela Defensoria Pública do Estado da Bahia a tais documentos ou dados, mesmo após a conclusão do vínculo contratual.

b) Será mantido em rigoroso sigilo e confidencialidade as informações, não podendo divulgar a terceiros, por quaisquer meios, qualquer informação, documento e material produzido a que tenha ou venha a ter acesso durante a vigência deste Contrato, e em razão do serviço objeto do presente Contrato, que não seja conhecida do público em geral.

c) O Contratado não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos ou de que tenha tomado conhecimento em decorrência da execução do objeto do contrato, sem autorização da Autoridade Competente da Defensoria Pública do Estado da Bahia, por escrito, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos.

d) Toda a produção intelectual, inovações e de toda e qualquer documentação, dados, relatórios, além de materiais e outros gerados em razão da prestação de serviços é de propriedade da Defensoria Pública do Estado da Bahia.

e) O descumprimento da obrigação de sigilo e confidencialidade sujeitará o Contratado ao pagamento, ou recomposição, de todas as perdas e danos resultantes do descumprimento, bem como a sua responsabilização civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo, nos termos do Regulamento Interno de Licitações e Contratos - RILC (normativos competentes e aplicáveis) da Defensoria Pública do Estado da Bahia.

CLÁUSULA DÉCIMA-NONA – FORO

As partes elegem o Foro da Cidade do Salvador, Estado da Bahia, que prevalecerá sobre qualquer outro, por mais privilegiado que seja, para dirimir quaisquer dúvidas oriundas deste contrato.

E, por estarem assim justos e contratados, firmam o presente contrato em 02 (duas) vias de igual teor e forma na presença das testemunhas que subscrevem depois de lido e achado conforme.

Salvador, ____ de _____ de 2022.

CONTRATANTE	**CONTRATADA**
Testemunha (nome/CPF)	**Testemunha (nome/CPF)**

Defensoria Pública
BAHIA

PARTE V – ATA DE REGISTRO DE PREÇOS

MINUTA DA ATA DE REGISTRO DE PREÇOS XX/2023

Modalidade de Licitação	Número
PREGÃO ELETRÔNICO	17/2023

Aos ____ dias do mês de _____ do ano de _____, **A DEFENSORIA PÚBLICA DO ESTADO DA BAHIA**, neste ato representado pelo Dr. _____, titular da DPE/BA, CNPJ nº XX.XXX.XXX/0001-XX, situada na Avenida Ulisses Guimarães, n° 3.386, autorizado pelo Decreto de delegação de competência publicado no D.O.E. de ___/___/___, doravante denominado **CONTRATANTE**, e os proponentes **[PESSOA JURÍDICA/PESSOA NATURAL]**, CNPJ/CPF nº_____, Inscrição Estadual (serviços do art. 155 da CF) /Municipal nº _____, situada na _____, neste ato representada pelo Sr. _____, portador da cédula de identidade nº _____, emitida por _____, inscrito no CPF/MF sob o nº _____, doravante denominados **FORNECEDORES**, em decorrência do Pregão Eletrônico nº 17/2023, processo administrativo nº 01.0485.2023.000003249-0, firmam a presente **ATA DE REGISTRO DE PREÇOS,** em proveito do Órgãos e Unidades vinculadas ao registro de preços, aqui denominados **UNIDADES CONTRATANTES**, que se regerá pela Lei estadual nº 9.433/05, pelas normas gerais da Lei nº 8.666/93, e respectivas alterações, pelo Decreto estadual nº 19.252/19, bem como pela legislação específica pertinente ao objeto licitado, mediante as cláusulas e condições a seguir ajustadas:

1. Objeto

1.1 O objeto desta ata é o Registro de preço, para eventual aquisição de soluções de Segurança da Informação com o propósito de ampliar a segurança da rede da DPE/BA, incluindo repasse de conhecimento, manutenção e suporte técnico por 60 (sessenta) meses de acordo com as condições e especificações constantes no Termo de Referência, conforme especificações, condições gerais, prazos e quantitativos constantes do instrumento convocatório, que a este termo integram como se literalmente transcritos, assim como o conteúdo da proposta apresentada pela licitante.

1.2 Nos termos do art. 17, §1º, do Decreto estadual nº 19.252/19, é vedado efetuar acréscimos nos quantitativos fixados pela ata de registro de preços, inclusive o aumento de que trata o art. 143, §1º, da Lei estadual nº 9.433/05.

2. Órgão gerenciador e participantes:

2.1 O órgão gerenciador deste registro de preços é a Defensoria Pública do Estado da Bahia**.**

2.2 O cadastro de reserva será composto consoante o disposto no art. 16 do Decreto estadual nº 19.252/19, e formalizado mediante a juntada da ata da sessão pública da licitação, a qual será anexada a esta Ata de Registro de Preços.

3. Prazo de validade do registro:

3.1 O prazo de validade do registro será de 01 (um) ano, improrrogável, contados a partir da data de assinatura pelo Titular do Órgão Gerenciador.
3.2 Durante o prazo de validade do registro de preços, as propostas selecionadas ficarão à disposição da Administração para que efetue as contratações nas oportunidades e quantidades de que necessitar, segundo a conveniência dos órgãos e/ou entidades contratantes, até o limite estabelecido.

3.3 A existência de preços registrados não obriga a Administração a firmar as contratações que deles poderão advir, ficando-lhe facultada a utilização de outros meios, respeitada a legislação relativa às licitações, sendo assegurado ao beneficiário do registro a preferência em igualdade de condições.

3. Prazo de validade do registro:

3.1 O prazo de validade do registro será de 01 (um) ano, improrrogável, contados a partir da data de assinatura pelo Titular do Órgão Gerenciador.
3.2 Durante o prazo de validade do registro de preços, as propostas selecionadas ficarão à disposição da Administração para que efetue as contratações nas oportunidades e quantidades de que necessitar, segundo a conveniência dos órgãos e/ou entidades contratantes, até o limite estabelecido.

3.3 A existência de preços registrados não obriga a Administração a firmar as contratações que deles poderão advir, ficando-lhe facultada a utilização de outros meios, respeitada a legislação relativa às licitações, sendo assegurado ao beneficiário do registro a preferência em igualdade de condições.

4.3 O órgão gerenciador disponibilizará no *site* oficial da Defensoria Pública do Estado da Bahia quanto aos preços registrados, para orientação dos demais órgãos e entidades da Administração Pública Estadual.

4.4 Em nenhuma hipótese serão registrados preços incompatíveis com os preços correntes no mercado ou fixados pela Administração Pública Estadual ou por órgão oficial competente ou constantes da tabela de preços referenciais

4.5 O órgão gerenciador realizará pesquisa de mercado periodicamente, a fim de verificar a vantajosidade dos preços registrados nesta Ata.

5. Dotação orçamentária:

5.1 As despesas decorrentes da contratação correrão à conta da dotação orçamentária concernente às UNIDADES CONTRATANTES, devendo cada contratação ser precedida da emissão da declaração de compatibilidade com a Lei de Responsabilidade Fiscal - LRF.

6. Contratação:

6.1 A contratação com o FORNECEDOR obedecerá as condições do instrumento convocatório e da minuta de contrato dele constante, que a esta ata integram independentemente de transcrição, especialmente as disposições quanto: ao objeto; ao prazo de vigência contratual; à prestação de garantia; ao regime de execução ou forma de fornecimento; às obrigações das partes; à fiscalização do contrato; ao recebimento do objeto; às condições de pagamento; à manutenção das condições da proposta; às alterações contratuais; à inexecução e rescisão e penalidades.

6.1.1 A critério da Administração, é facultada a substituição do contrato por instrumento equivalente, Autorização de Fornecimento de Material - AFM ou Autorização de Prestação de Serviços – APS, conforme o caso, desde que presentes as condições do art. 132 da Lei estadual nº 9.433/05.

6.1.2 Considerar-se-ão literalmente transcritas no instrumento equivalente todas as cláusulas e condições previstas na minuta de contrato constante do convocatório.

6.1.3 As UNIDADES CONTRATANTES poderão solicitar ao fornecedor, dentro do prazo de validade do Registro de Preços, os quantitativos dos materiais ou serviços de acordo com suas necessidades e respeitados os limites máximos estabelecidos neste edital e a ordem de classificação das propostas.

6.1.4 A ocorrência de fato superveniente, decorrente de caso fortuito ou força maior que prejudique, ainda que temporariamente, o cumprimento da ata de registro de preços, deverá ser comunicada pelo fornecedor antes do pedido de fornecimento, o qual ficará liberado do compromisso assumido, sem aplicação de penalidade, se confirmada a veracidade dos motivos e alegações apresentadas. [NOTA: conforme §1º do art. 14 do Decreto nº 19.252/19].

6.1.5 - Na hipótese do item 6.1.4, alternativamente ao cancelamento do item registrado, poderá ser admitida a substituição da marca do produto por outro de qualidade equivalente ou superior, mediante parecer técnico fundamentado, no qual seja demonstrado o atendimento das especificações e dos requisitos pertinentes ao objeto, bem como a adequação do preço, vedada a fixação de valor superior ao anteriormente registrado. [NOTA: conforme §2º do art. 14 do Decreto nº 19.252/19].

6.2 O FORNECEDOR será convocado a assinar o termo de contrato, ou instrumento equivalente, se for o caso, no prazo fixado no edital, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas em lei, podendo solicitar sua prorrogação por igual período, por motivo justo e aceito pela Administração.

6.2.1 A assinatura do contrato deverá ser realizada pelo representante legal do FORNECEDOR ou mandatário com poderes expressos.

6.2.2 A recusa injustificada do fornecedor em subscrever o termo de contrato ou instrumento equivalente ensejará a aplicação das penalidades legalmente estabelecidas. **[NOTA: conforme §1º do art. 25 do Decreto nº 19.252/19]**

6.2.3 Equipara-se à recusa prevista no item 6.2.2 a circunstância de o fornecedor deixar de manter as condições de habilitação exigidas na licitação, ou, por qualquer meio, dar causa à impossibilidade de subscrição do contrato. **[NOTA: conforme §2º do art. 25 do Decreto nº 19.252/19]**

6.2.4 O disposto neste artigo também se aplica aos integrantes do cadastro de reserva, que, convocados na forma do *caput* deste artigo, não honrem o compromisso assumido, sem justificativa ou com justificativa recusada pela Administração. **[NOTA: conforme §3º do art. 25 do Decreto nº 19.252/19]**

6.2.5 A critério da Administração, a assinatura do contrato ou do instrumento equivalente se dará por meio do Sistema Eletrônico de Informações - SEI-DPE/BA, caso em que a licitante deverá providenciar o cadastramento de seu representante legal ou procurador no endereço eletrônico www.defensoria.ba.def.br.

6.2.6 A recusa da adjudicatária em se cadastrar ou a subscrever eletronicamente o contrato ou instrumento equivalente implicará na decadência da contratação e à sujeição às sanções cominadas na legislação.

6.3 Como condição para celebração do contrato, o FORNECEDOR deverá manter, durante todo o prazo de validade do registro, todas as condições de habilitação, ficando esclarecido que não serão contratados os fornecedores ou prestadores de serviço que não estejam com documentação regular.

6.4 Na hipótese de o FORNECEDOR convocado não assinar o termo de contrato, ou não aceitar ou retirar o instrumento equivalente, no prazo e nas condições estabelecidas no edital, a Administração poderá convocar os demais FORNECEDORES integrantes do cadastro de reserva, obedecendo a ordem de classificação.

7. Reajustamento dos preços registrados em ata:

7.1 Os preços são fixos e irreajustáveis durante o transcurso do prazo de 12 meses da data de apresentação da proposta, após o que a concessão de reajustamento, nos termos do inc. XXV do art. 8º da Lei estadual nº 9.433/05, será feita mediante a aplicação do INPC/IBGE.

8. Revisão dos preços registrados em ata:

8.1 Os preços registrados poderão ser revistos em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos serviços ou bens registrados, observados os parâmetros definidos na alínea "d" do inciso II do *caput* do art. 143 da Lei estadual nº 9.433/05.

8.1.1 A alteração ou revisão de preços registrados em Ata não implica a revisão automática dos preços dos contratos decorrentes do respectivo Registro de Preços.

8.2 Quando o preço registrado tornar-se superior ao preço praticado no mercado por motivo superveniente, o órgão gerenciador convocará os fornecedores constantes da ata de registro de preços e do cadastro de reserva para negociarem a redução dos preços aos valores praticados pelo mercado.

8.2.1 Os fornecedores que não aceitarem reduzir seus preços aos valores praticados pelo mercado serão liberados do compromisso assumido, sem aplicação de penalidade.

8.2.2 A ordem de classificação dos fornecedores que aceitarem reduzir seus preços aos valores de mercado observará a classificação original.

8.3 Quando o preço de mercado tornar-se superior aos preços registrados, poderá o fornecedor, se não puder cumprir o compromisso, pleitear a revisão de seu preço, instruindo o pedido com a demonstração da efetiva ocorrência do desequilíbrio.

8.3.1 A apreciação do pedido deve ocorrer no prazo máximo de 15 (quinze) dias, durante o qual o fornecedor ficará obrigado a garantir o fornecimento do material ou a execução dos serviços, sendo que este prazo poderá ser reiniciado, caso haja necessidade de diligência para complementar a análise do pleito.

8.3.2 Confirmada a veracidade dos motivos e alegações apresentados, o fornecedor estará liberado do compromisso assumido, sem aplicação de penalidade, caso a comunicação ocorra antes do pedido de fornecimento.

8.3.3 Não comprovada a veracidade das alegações apresentadas no pleito de revisão, deverá ser instaurado processo administrativo para aplicação de sanção, em face dos compromissos que tenha deixado de honrar.

8.3.4 Na hipótese do 8.3.2, o órgão gerenciador poderá convocar os demais fornecedores constantes do cadastro de reserva para que se manifestem acerca da manutenção do preço registrado.

8.3.5 Havendo manifestação pela manutenção do preço registrado, o órgão gerenciador promoverá as necessárias modificações na ata, compondo novo cadastro de reserva e disponibilizando-o no *site* oficial de compras eletrônicas do Estado, observada a ordem original de classificação, se presente mais de um interessado.

8.3.6 Não havendo interessados na manutenção do preço, o órgão gerenciador deverá proceder à revogação da ata de registro de preços, adotando as medidas cabíveis para obtenção da contratação mais vantajosa, sendo-lhe facultado deflagrar processo de negociação de preços com todos os fornecedores constantes da ata de registro de preços e do cadastro de reserva, nas seguintes hipóteses:

I - constatação do caráter geral do fato gerador da revisão, especialmente na hipótese de mercados regulados, em que os preços sofrem variações de modo uniforme ou homogêneo;

II - majoração dos preços correspondentes em tabela de preços referenciais adotada pela Administração Pública Estadual;

III - existência de prejuízo ante a impossibilidade de imediata deflagração de novo procedimento licitatório.

8.3.7 No processo de negociação, somente poderão apresentar novo preço os fornecedores constantes da ata de registro de preços e do cadastro de reserva.

8.3.8 O preço resultante da negociação deverá observar o disposto na cláusula 4.4 desta ata.

9. Cancelamento do registro:

9.1 Os preços registrados poderão ser cancelados:

9.1.1 por iniciativa da Administração Pública Estadual, em razão de interesse público fundamentado;

9.1.2 quando o fornecedor estiver liberado do compromisso, nas situações previstas no Decreto nº 19.252/19.

9.1.3 quando o fornecedor:

a) descumprir as condições do edital ou da ata de registro de preços;

b) não assinar o termo de contrato ou instrumento equivalente no prazo estabelecido pela Administração Pública Estadual, sem justificativa aceitável;

c) for declarado inidôneo ou suspenso do direito de licitar ou contratar, na forma da lei;

d) der causa à rescisão administrativa de contrato decorrente do registro de preços, por um dos motivos elencados nos incisos de III a XII do art. 167 da Lei estadual nº 9.433/05.

9.1.4 O cancelamento de preços registrados nas hipóteses previstas na cláusula 9.1.3. será formalizado por despacho do órgão gerenciador, assegurado o contraditório e a ampla defesa.

9.1.5 Será admitida a suspensão cautelar dos preços registrados em caso de risco iminente da ocorrência de fatos que possam trazer prejuízo ao erário ou lesão ao interesse público de difícil ou impossível reparação.

10. Penalidades:

10.1 O descumprimento da Ata de Registro de Preços ensejará aplicação das penalidades estabelecidas no Edital.

10.2 Caberá ao órgão gerenciador adotar as providências necessárias à apuração de ilícitos decorrentes:

a) de infrações concernentes ao procedimento licitatório;

b) do descumprimento do pactuado na ata de registro de preços;

c) do descumprimento das obrigações contratuais, em relação às suas próprias contratações.

10.3 Caberá a órgão ou entidade participante adotar as providências necessárias à apuração de ilícitos decorrentes do descumprimento do pactuado na ata de registro de preços ou das obrigações contratuais em relação às suas próprias contratações, informando as ocorrências ao órgão gerenciador.

11. Utilização da ata por órgãos ou entidades não participantes:

(X) 11.1 Poderá haver adesão posterior à ata de registro de preços decorrente desta licitação.

11.2. Âmbito do registro: O âmbito deste registro de preços é o designado abaixo:
Poderá haver adesão posterior à ata de registro de preços decorrente desta licitação, devendo ser observados os seguintes limites quantitativos e as regras definidas na presente Ata de Registro de Preços:

a) A ata de registro de preços, durante sua vigência, poderá ser utilizada por qualquer órgão ou entidade da Administração Pública Direta, Autárquica e Fundacional do Estados da Bahia, que não tenha participado do certame licitatório, mediante anuência do órgão gerenciador, desde que devidamente justificada a vantagem e respeitadas, no que couber, as condições e as regras estabelecidas no Decreto estadual nº 19.252/2019 e na Lei Federal nº 8.666, de 21 de junho de 1993.
b) Caberá ao fornecedor beneficiário da Ata de Registro de Preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento, desde que este fornecimento não prejudique as obrigações anteriormente assumidas com o órgão gerenciador e órgãos participantes.
c) As contratações adicionais não poderão exceder os limites quantitativos para adesões definidos no edital de origem, não podendo extrapolar, em qualquer caso, por cada órgão ou entidade aderente, a 50% (cinquenta por cento) dos quantitativos dos itens do instrumento convocatório e registrados na ata de registro de preços para o órgão gerenciador e para os órgãos ou entidades participantes
d) O quantitativo decorrente das adesões à ata de registro de preços não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o órgão gerenciador e para os órgãos ou entidades participantes, independentemente do número de órgãos ou entidades não participantes que aderirem.
e) A análise da juridicidade da participação, da inexistência de norma interna impeditiva, bem assim da adequação e compatibilidade com o regime jurídico de licitação a que está submetido o órgão gerenciador, deverá ser procedida pelo órgão ou entidade que pretende a adesão.
f) Após a autorização do órgão gerenciador, o órgão não participante deverá efetivar a contratação solicitada em até noventa dias, observado o prazo de validade da Ata de Registro de Preços. Caberá a Defensoria Pública do Estado da Bahia autorizar, excepcional e justificadamente, a prorrogação do prazo para efetivação da contratação, respeitado o prazo de vigência da ata, desde que solicitada pelo órgão não participante.
g) Competem ao órgão ou entidade aderente os atos relativos à cobrança do cumprimento pelo fornecedor das obrigações contratualmente assumidas e a aplicação, observada a ampla defesa e o contraditório, de eventuais penalidades decorrentes do descumprimento de cláusulas contratuais, em relação às suas próprias contratações, devendo informar as ocorrências ao órgão gerenciador
h) A abrangência territorial da ata de registro de preços: Estados da Federação e Distrito Federal.

12. Vinculação ao edital de licitação:

Integram a presente Ata, como se nela estivessem transcritas, todas as cláusulas e condições estabelecidas no processo licitatório referido no preâmbulo deste instrumento, inclusive anexos e adendos, e a proposta do FORNECEDOR.

13. Da Comunicação Eletrônica:

13.1 Fica pactuado que os atos de comunicação processual com o FORNECEDOR poderão ser realizados por meio eletrônico, na forma do disposto na Lei nº 12.290, de 20 de abril de 2011, e do Decreto nº 15.805, de 30 de dezembro de 2014.

13.1.1 O FORNECEDOR deverá manter atualizado o endereço eletrônico cadastrado no Sistema Eletrônico de Informações - SEI-DPE/BA, para efeito do recebimento de notificação e intimação de atos processuais.

14. Do cumprimento da Lei Geral de Proteção de Dados - Lei n° 13.709/2018:

I – Inclui-se as seguintes obrigações da Contratada e da Contratante do Contrato:

a) É vedado às partes a utilização de todo e qualquer dado pessoal repassado em decorrência da execução contratual para finalidade distinta daquela do objeto da contratação, sob pena de responsabilização administrativa, civil e criminal.

b) As partes se comprometem a manter sigilo e confidencialidade de todas as informações em especial os dados pessoais e os dados pessoais sensíveis repassados em decorrência da execução contratual, em consonância com o disposto na Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), sendo vedado o repasse das informações a outras empresas ou pessoas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do instrumento contratual.

c) As partes responderão administrativa e judicialmente em caso de danos patrimoniais, morais, individuais ou coletivos, aos titulares de dados pessoais repassados em decorrência da execução contratual, por inobservância à Lei Geral de Proteção de Dados.

d) Em atendimento ao disposto na Lei Geral de Proteção de Dados, a CONTRATANTE, para a execução do serviço objeto deste contrato, tem acesso a dados pessoais dos representantes da CONTRATADA, tais como número do CPF e do RG, endereços eletrônico e residencial, e cópia do documento de identificação.

e) A CONTRATADA declara que tem ciência da existência da Lei Geral de Proteção de Dados e se compromete a adequar todos os procedimentos internos ao disposto na legislação com o intuito de proteger os dados pessoais repassados pelo CONTRATANTE.

f) A CONTRATADA fica obrigada a comunicar ao CONTRATANTE em até 48 (quarenta e oito) horas qualquer incidente de acessos não autorizados aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, bem como adotar as providências dispostas no art. 48 da Lei Geral de Proteção de Dados.

g) "Leis Aplicáveis à Proteção de Dados" significa todas as leis, normas e regulamentos que regem o tratamento de dados pessoais, em especial, a Lei Geral de Proteção de Dados (Lei Federal n. 13.709/2018, "LGPD"), além das normas e dos regulamentos adotados ou a serem adotados pela Defensoria Pública do Estado da Bahia, e determinações de órgãos reguladores/fiscalizadores sobre a matéria.

h) As expressões utilizadas no presente contrato, tais como, 'titular dos dados', 'dados pessoais', 'tratamento', 'violação de dados pessoais', etc., serão interpretadas com base no significado atribuído pela LGPD.

i) A Defensoria Pública do Estado da Bahia/Contratante agirá como "controlador", nos termos do art.5°, VI da Lei nº13.709/2018, e a Contratada assume o papel como "operador", nos termos do art. 5º, VII, da mesma Lei 13.709/2018, no sentido estrito da LGPD, salvo nos casos em que o operador/Contratado(a), passe a atuar em desconformidade com as orientações do "controlador/Contratante", passando assim a se responsabilizar como controlador, perante os órgãos de controle/fiscalização.

j) O Contratado(a) declara que conhece a Política de Governança de Privacidade e de Proteção de Dados Pessoais da Defensoria Pública do Estado da Bahia (Portaria nº 811, de 30.08.2021, publicada no DOE/DPE de 31/08/2021), e se compromete ao seu cumprimento e fiel observância, tudo de conformidade com o art. 39, da Lei nº 13.709/2018.

DA CONFIDENCIALIDADE NA RELAÇÃO CONTRATUAL

II - Inclui-se, ainda, as seguintes obrigações à Cláusula Sétima (OBRIGAÇÕES DA CONTRATADA) do presente Contrato:

a) O Contratado será expressamente responsabilizado quanto à manutenção de sigilo absoluto sobre quaisquer dados, informações, artefatos, contidos em quaisquer documentos e em quaisquer mídias, de que venha a ter conhecimento durante a execução do contrato, não podendo, sob qualquer pretexto divulgar, reproduzir ou utilizar, sob pena de sanções legais, independentemente da classificação de sigilo conferida pela Defensoria Pública do Estado da Bahia a tais documentos ou dados, mesmo após a conclusão do vínculo contratual.

b) Será mantido em rigoroso sigilo e confidencialidade as informações, não podendo divulgar a terceiros, por quaisquer meios, qualquer informação, documento e material produzido a que tenha ou venha a ter acesso durante a vigência deste Contrato, e em razão do serviço objeto do presente Contrato, que não seja conhecida do público em geral.

c) O Contratado não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos ou de que tenha tomado conhecimento em decorrência da execução do objeto do contrato, sem autorização da Autoridade Competente da Defensoria Pública do Estado da Bahia, por escrito, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos.

d) Toda a produção intelectual, inovações e de toda e qualquer documentação, dados, relatórios, além de materiais e outros gerados em razão da prestação de serviços é de propriedade da Defensoria Pública do Estado da Bahia.

e) O descumprimento da obrigação de sigilo e confidencialidade sujeitará o Contratado ao pagamento, ou recomposição, de todas as perdas e danos resultantes do descumprimento, bem como a sua responsabilização civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo, nos termos do Regulamento Interno de Licitações e Contratos - RILC (normativos competentes e aplicáveis) da Defensoria Pública do Estado da Bahia.

15. Foro

As partes elegem o Foro da Cidade do Salvador, Estado da Bahia, que prevalecerá sobre qualquer outro, por mais privilegiado que seja, para dirimir quaisquer dúvidas oriundas deste instrumento.

Local (Salvador (BA), ____ de _____ de 2023.

DEFENSORIA PÚBLICA DO ESTADO DA BAHIA

FORNECEDOR	**FORNECEDOR**
Testemunha (nome/CPF)	**Testemunha (nome/CPF)**

Defensoria Pública
BAHIA

PARTE FIXA

RITO DO PROCEDIMENTO LICITATÓRIO E DA CONTRATAÇÃO

PREGÃO ELETRÔNICO

TÍTULO I
DOS PRINCÍPIOS

1. A licitação destina-se a garantir a observância do princípio constitucional da isonomia e a selecionar a proposta mais vantajosa para a Administração e será processada e julgada em estrita conformidade com os princípios básicos da legalidade, da impessoalidade, da moralidade, da igualdade, da publicidade, da eficiência, da probidade administrativa, da vinculação ao instrumento convocatório, do julgamento objetivo e dos que lhes são correlatos.

TÍTULO II
DOS IMPEDIMENTOS

2. Não será admitida a participação de interessados que estejam suspensos do direito de licitar ou contratar e/ou declarados inidôneos, na forma dos incisos II e III do art. 186 da Lei estadual nº 9.433/05.
3. Em consonância com o art. 200 da Lei estadual nº 9.433/05, fica impedida de participar de licitações e de contratar com a Administração Pública a pessoa jurídica constituída por membros de sociedade que, em data anterior à sua criação, haja sofrido penalidade de suspensão do direito de licitar e contratar com a Administração ou tenha sido declarada inidônea para licitar e contratar e que tenha objeto similar ao da empresa punida.
4. Não poderá participar, direta ou indiretamente, da licitação, da execução de obras ou serviços e do fornecimento de bens a eles necessários: a) o autor do projeto, básico ou executivo, pessoa natural física ou jurídica; b) a empresa responsável, isoladamente ou em consórcio, pela elaboração do projeto básico ou executivo ou da qual o autor do projeto seja dirigente, gerente, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto ou controlador, responsável técnico, subordinado ou subcontratado; c) servidor ou dirigente do órgão ou entidade contratante ou responsável pela licitação; d) demais agentes públicos, assim definidos no art. 207 da Lei estadual nº 9.433/05, impedidos de contratar com a Administração Pública por vedação constitucional ou legal.
   4.1 É permitida a participação do autor do projeto ou da empresa a que se refere a alínea b deste item na licitação ou na execução da obra ou serviço como consultor ou técnico, nas funções de fiscalização, supervisão ou gerenciamento, exclusivamente a serviço da Administração interessada.
   4.2 O disposto neste item não impede a licitação ou contratação de obra ou serviço que inclua, como encargo do contratado ou pelo preço previamente fixado pela Administração, a elaboração do projeto executivo
   4.3 Considera-se participação indireta, para os fins do disposto neste item, a existência de qualquer vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou de parentesco até o 3º grau entre o autor do projeto, pessoa física ou jurídica, e a licitante ou responsável pelos serviços, fornecimentos e obras, incluindo-se o fornecimento de bens e serviços a estes necessários.
   4.4 Aplica-se o disposto no item anterior aos membros da comissão de licitação, ao pregoeiro e equipe de apoio.
5. É vedado ao agente político e ao servidor público de qualquer categoria, natureza ou condição, celebrar contratos com a administração direta ou indireta, por si ou como representante de terceiro, sob pena de nulidade, ressalvadas as exceções legais, conforme o art. 125 da Lei estadual nº 9.433/05.
6. Os servidores públicos civis deverão observar as vedações contidas na Lei estadual nº 6.677/94, especialmente do inc. XI do art. 176, assim como as proibições específicas das respectivas carreiras e grupos ocupacionais.
7. Os policiais militares da ativa deverão atender às prescrições do art. 40 e 57 da Lei estadual nº 7.990/01.

TÍTULO III
DAS PROPOSTAS E DOS DOCUMENTOS DE HABILITAÇÃO
CAPÍTULO I
QUANTO À FORMA

8. Os documentos relativos à proposta e à habilitação serão apresentados em formato digital, sob exclusiva responsabilidade dos proponentes quanto à sua validade.
8.1 Em caso de dúvida quanto à autenticidade dos documentos, o pregoeiro poderá solicitar a apresentação dos documentos em original ou cópia autenticada, para verificação.
8.2 Os documentos eletrônicos produzidos com a utilização de processo de certificação disponibilizada pela ICP-Brasil serão recebidos e presumidos verdadeiros em relação aos signatários, dispensando-se o envio de documentos originais e cópias autenticadas em papel.
8.3 A falsidade dos documentos apresentados sujeitará a licitante à sanções previstas na legislação pertinente.
9. As certidões extraídas pela *internet* somente terão validade se confirmada sua autenticidade.

10. Como condição específica para participação do pregão por meio eletrônico, é necessário, previamente, o credenciamento pelos licitantes no sistema indicado no PREÂMBULO, através da atribuição de chave de identificação e/ou senha individual.
11. A participação no pregão eletrônico dar-se-á por meio do acesso da licitante exclusivamente por meio do sistema disponibilizado.

CAPÍTULO II
QUANTO AO CONTEÚDO

12. A proponente deverá elaborar a sua proposta de preços em moeda nacional (reais e centavos), observando as disposições do Termo de Referência, ficando esclarecido que não serão admitidas propostas alternativas.
13. Ocorrendo divergência entre o preço por item em algarismo e o expresso por extenso, será levado em conta este último.
14. A proposta apresentada deverá incluir as despesas necessárias ao fiel cumprimento do objeto da licitação.
15. Os preços cotados deverão ser referidos à data de recebimento das propostas, considerando a condição de pagamento à vista, não devendo, por isso, computar qualquer custo financeiro para o período de processamento das faturas.
16. Não será permitida previsão de sinal, ou qualquer outra forma de antecipação de pagamento na formulação das propostas, devendo ser desclassificada, de imediato, a proponente que assim o fizer.
17. Não será considerada qualquer oferta de vantagem não prevista no instrumento convocatório, nem propostas com preço global ou unitário simbólico, irrisório ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos.
18. A formulação da proposta implica para a proponente a observância dos preceitos legais e regulamentares em vigor, tornando-a responsável pela fidelidade e legitimidade das informações e dos documentos apresentados.
19. Na concorrência, tomada de preços e convite do tipo técnica e preço, a proponente deverá apresentar proposta técnica observando as disposições relativas ao modelo de descrição da proposta técnica e aos critérios para avaliação das propostas técnicas.
20. Para a habilitação dos interessados na licitação, exigir-se-ão, exclusivamente, os documentos relacionados no instrumento convocatório.
20.1 As microempresas e empresas de pequeno porte, beneficiárias do tratamento diferenciado e favorecido previsto na Lei Complementar nº 123/06, deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal e trabalhista, mesmo que esta apresente alguma restrição.

TÍTULO IV
DO PROCEDIMENTO NA LICITAÇÃO

CAPÍTULO I
DA FASE INICIAL

Seção I
Do Credenciamento

21. O site, dia e hora para recebimento das propostas e início da sessão pública estão indicados no PREÂMBULO.
21.1 Reputa-se credenciada a pessoa natural regularmente designada para representar a licitante no processo licitatório.
21.2 Cada licitante poderá credenciar apenas um representante e cada representante somente poderá representar uma única licitante.
21.3 As licitantes interessadas na concessão de tratamento diferenciado assegurado pela Lei Complementar nº 123/06 deverão estar previamente cadastradas no sistema indicado no PREÂMBULO, como microempresas ou empresas de pequeno porte.
22. O credenciamento do usuário será pessoal e intransferível para acesso ao sistema, sendo a licitante responsável por todos os atos praticados.

Seção II
Da licitante

23. Caberá à licitante interessada em participar do pregão, na forma eletrônica: **[NOTA: art. 17 do Decreto nº 19.896/20]**
a) remeter, no prazo estabelecido, exclusivamente via sistema eletrônico, os documentos de habilitação e a proposta e, quando necessário, os documentos solicitados conforme estabelecido neste edital;
b) responsabilizar-se formalmente pelas transações efetuadas em seu nome, assumir como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros;

c) acompanhar as operações no sistema eletrônico durante o processo licitatório e responsabilizar-se pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pelo sistema ou de sua desconexão;
d) comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a inviabilidade do uso da senha, para imediato bloqueio de acesso;
e) utilizar a chave de identificação e a senha de acesso para participar do pregão na forma eletrônica.
24. O credenciamento do usuário implica em sua responsabilidade legal e na presunção de capacidade técnica para realização das transações inerentes ao pregão.

Seção III
Da Interrupção da Sessão

25. Sempre que houver interrupção da sessão, as licitantes deverão ser notificadas do dia e hora em que a sessão terá continuidade.
25.1 Na hipótese de o sistema eletrônico desconectar para o pregoeiro no decorrer da etapa de envio de lances da sessão pública e permanecer acessível aos licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados. **[NOTA: art. 25 do Decreto nº 19.896/20]**
25.2 Na situação descrita no item 25.1, quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a 10 (dez) minutos, a sessão pública será suspensa e reiniciada somente decorridas 24 (vinte e quatro) horas após a comunicação do fato aos participantes, no sítio eletrônico utilizado para divulgação. **[NOTA: art. 26 do Decreto nº 19.896/20]**

Seção IV
Da Apresentação da Proposta e dos Documentos de Habilitação

26. Após a divulgação do edital no sítio eletrônico, as licitantes encaminharão, exclusivamente por meio do sistema eletrônico, concomitantemente com os documentos de habilitação exigidos no edital, proposta com a descrição do objeto ofertado e o preço, conforme as datas e horários estabelecidos no instrumento convocatório, observando-se o que se segue: **[NOTA: art. 18, caput, do Decreto nº 19.896/20]**
26.1 A licitante deverá preencher o formulário eletrônico apresentado na tela com os dados pertinentes à sua proposta de preços, vedada a identificação da proponente ou do seu representante legal, sob pena de desclassificação.
26.2 No caso de aquisições, o formulário deverá ser preenchido com as exigências relacionadas no item respectivo da Seção I – Especificações para Elaboração da Proposta de Preços, da PARTE I - Propostas.
26.3 As licitantes também deverão remeter nesta oportunidade, exclusivamente via sistema eletrônico: a) proposta escrita de preços, preferencialmente de acordo com o modelo da Seção IV – Modelo de descrição da proposta de preços, da PARTE I – Propostas; b) declaração de elaboração independente de proposta e de inexistência de impedimento à participação no certame; c) declaração de enquadramento, quando for o caso (Lei nº 123/2006); d) declaração de pleno conhecimento e de veracidade dos documentos; e) procuração, se for o caso, por instrumento público ou particular, este último acompanhado da prova da legitimidade de quem outorgou os poderes.
26.4 Os documentos exigidos para habilitação, conforme o disposto na PARTE II do edital deverão ser enviados nesta fase, exclusivamente via sistema eletrônico, observando-se o que se segue:
26.4.1 As licitantes cadastradas no Cadastro Unificado de Fornecedores do Estado da Bahia poderão deixar de apresentar os documentos de habilitação que constem no referido Cadastro, observado o disposto neste edital, para a confirmação das suas condições habilitatórias. **[NOTA: art. 18, §1º, do Decreto nº 19.896/20]**
26.4.2 Os documentos exigidos para habilitação que não estejam contemplados no Registro Cadastral, ou que dele constem como vencidos, deverão ser enviados nesta fase, cabendo ao licitante certificar-se da regularidade de sua documentação. **[NOTA: art. 18, §2º, do Decreto nº 19.896/20]**
26.5 O envio da proposta, acompanhada dos documentos de habilitação exigidos no edital, nos termos do disposto no item 26 ocorrerá por meio de chave de acesso e senha. **[NOTA: art. 18, §3º, do Decreto nº 19.896/20]**
26.6 A licitante declarará, em campo próprio do sistema eletrônico, o cumprimento dos requisitos para a habilitação e a conformidade de sua proposta com as exigências do edital. **[NOTA: art. 18, §4º, do Decreto nº 19.896/20]**
26.7 A falsidade da declaração de que trata o item 26.6 sujeitará o licitante às sanções previstas na legislação pertinente. **[NOTA: art. 18, §5º, do Decreto nº 19.896/20]**
26.8 Os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema eletrônico, até a data e o horário estabelecidos no edital para a sua apresentação. **[NOTA: art. 18, §6º, do Decreto nº 19.896/20]**
26.9 Na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, observado o disposto no item 26 não haverá ordem de classificação das propostas. **[NOTA: art. 18, §7º, do Decreto nº 19.896/20]**
26.10 Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do pregoeiro e para acesso público após o encerramento do envio de lances. **[NOTA: art. 18, §8º, do Decreto nº 19.896/20]**

CAPÍTULO II
DA CLASSIFICAÇÃO DAS PROPOSTAS
Seção I
Das propostas de preços
Subseção I
Da abertura da Sessão Pública

27. A partir do horário previsto neste edital, a sessão pública na *internet* será aberta pelo pregoeiro com a utilização de sua chave de acesso e senha. **[NOTA: art. 19, caput, do Decreto nº 19.896/20]**
27.1 As licitantes poderão participar da sessão pública na *internet*, mediante a utilização de sua chave de acesso e senha. **[NOTA: art. 19, §1º, do Decreto nº 19.896/20]**
27.2 O sistema eletrônico disponibilizará campo próprio para troca de mensagens entre o pregoeiro e as licitantes. **[NOTA: art. 19, §2º, do Decreto nº 19.896/20]**
28. Iniciada a sessão pública do pregão eletrônico, não cabe desistência da proposta.
29. O pregoeiro verificará as propostas apresentadas e desclassificará aquelas que não estejam em conformidade com os requisitos estabelecidos neste edital. **[NOTA: art. 20, caput, do Decreto nº 19.896/20]**
29.1 Serão consideradas irregulares e desclassificadas, de logo, as propostas que não contenham informação que permita a identificação do objeto proposto.
29.1.1 Também será desclassificada a proposta que identifique a licitante.
29.2 A desclassificação da proposta será fundamentada e registrada no sistema eletrônico, para acompanhamento por todos os participantes. **[NOTA: art. 20, parágrafo único, do Decreto nº 19.896/20]**
29.3 O sistema eletrônico ordenará automaticamente as propostas classificadas pelo pregoeiro. **[NOTA: art. 21, caput, do Decreto nº 19.896/20]**
29.4 Somente as propostas classificadas pelo pregoeiro participarão da etapa de envio de lances. **[NOTA: art. 21, parágrafo único, do Decreto nº 19.896/20]**
30. Havendo apenas uma oferta, esta poderá ser aceita, desde que atenda todas as condições do instrumento convocatório e seu preço seja compatível com o valor estimado para a contratação e dentro da realidade do mercado.

Subseção II
Dos lances eletrônicos

31. Classificadas as propostas, o pregoeiro dará início à fase competitiva, oportunidade em que os licitantes poderão encaminhar lances exclusivamente por meio do sistema eletrônico. **[NOTA: art. 22 do Decreto nº 19.896/20]**
31.1 É vedada a utilização de sistema robotizado que implique envio automático de lances.
31.1.1 Poderá ser fixado intervalo mínimo de tempo a ser observado entre as ofertas de lances, ou recurso de tecnologia disponibilizado pelo sistema, a fim de coibir a utilização de software lançador (robô).
31.2 Se o pregoeiro identificar que alguma licitante, ao apresentar seus lances, o fez, entre outras formas, de maneira sucessiva, padronizada, intermitente, simultânea ou em intervalos de poucos segundos entre eles, indicando a utilização de software lançador "robô", será ela desclassificada, com a consequente abertura de processo administrativo para apuração do ilícito.
31.3 A licitante será imediatamente informada do recebimento do lance e do valor consignado no registro **[NOTA: art. 22, §1º, do Decreto nº 19.896/20]**
31.4 As licitantes poderão oferecer lances sucessivos, observados o horário fixado para abertura da sessão pública e as regras estabelecidas no edital. **[NOTA: art. 22, §2º, do Decreto nº 19.896/20]**
31.5 A licitante somente poderá oferecer valor inferior ou maior percentual de desconto ao último lance por ela ofertado e registrado pelo sistema, observado, quando houver, o intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta. **[NOTA: art. 22, §3º, do Decreto nº 19.896/20]**
31.6 Não serão aceitos dois ou mais lances iguais e prevalecerá aquele que for recebido e registrado primeiro. **[NOTA: art. 22, §4º, do Decreto nº 19.896/20]**
31.7 Durante a sessão pública, as licitantes serão informadas, em tempo real, do valor do menor lance registrado, vedada a identificação da licitante. **[NOTA: art. 22, §5º, do Decreto nº 19.896/20]**

Subseção III
Do envio de lances, segundo os modos de disputa

32. No **modo de disputa aberto**, conforme opção assinalada no PREÂMBULO deste edital, será observado o seguinte procedimento:
a) as licitantes apresentarão lances públicos e sucessivos, com prorrogações, conforme o critério de julgamento adotado neste edital;
b) deverá ser observado o intervalo mínimo de diferença de valores ou de percentuais entre os lances, definido neste edital, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta;
c) a etapa de envio de lances na sessão pública durará 10 (dez) minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos 02 (dois) minutos do período de duração da sessão pública. **[NOTA: art. 23, caput, do Decreto nº 19.896/20]**

d) a prorrogação automática da etapa de envio de lances, de que trata a letra "c" será de 02 (dois) minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive quando se tratar de lances intermediários. **[NOTA: art. 23, §1º, do Decreto nº 19.896/20]**
e) na hipótese de não haver novos lances, a sessão pública será encerrada automaticamente. **[NOTA: art. 23, §2º, do Decreto nº 19.896/20]**
f) encerrada a sessão pública sem prorrogação automática pelo sistema, nos termos do disposto ~~no § 1º deste artigo~~ na letra "d", o pregoeiro poderá admitir o reinício da etapa de envio de lances, em prol da consecução do melhor preço, mediante justificativa. **[NOTA: art. 23, §3º, do Decreto nº 19.896/20]**
33. No **modo de disputa aberto e fechado**, conforme opção assinalada no PREÂMBULO deste edital, será observado o seguinte procedimento:
a) as licitantes apresentarão lances públicos e sucessivos, com lance final e fechado, conforme o critério de julgamento adotado neste edital;
b) a etapa de envio de lances da sessão pública terá duração de 15 (quinze) minutos. **[NOTA: art. 24, caput, do Decreto nº 19.896/20]**
c) encerrado o prazo previsto na letra "b, o sistema encaminhará o aviso de fechamento iminente dos lances e, transcorrido o período de até 10 (dez) minutos, aleatoriamente determinado, a recepção de lances será automaticamente encerrada **[NOTA: art. 24, §1º, do Decreto nº 19.896/20]**
d) Encerrado o prazo de que trata a letra "c", o sistema abrirá a oportunidade para que o autor da oferta de valor mais baixo e os autores das ofertas com valores até 10% (dez por cento) superiores àquela possam ofertar um lance final e fechado em até 05 (cinco) minutos, que será sigiloso até o encerramento deste prazo. **[NOTA: art. 24, §2º, do Decreto nº 19.896/20]**
e) Na ausência de, no mínimo, 03 (três) ofertas nas condições de que trata a letra "d", os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de 03 (três), poderão oferecer um lance final e fechado em até 05 (cinco) minutos, que será sigiloso até o encerramento do prazo. **[NOTA: art. 24, §3º, do Decreto nº 19.896/20]**
f) encerrados os prazos estabelecidos nas letras "d" e "e", o sistema ordenará os lances em ordem crescente de vantajosidade. **[NOTA: art. 24, §4º, do Decreto nº 19.896/20]**
g) na ausência de lance final e fechado classificado nos termos das letras "d" e "e", haverá o reinício da etapa fechada para que os demais licitantes, até o máximo de 03 (três), na ordem de classificação, possam ofertar um lance final e fechado em até 05 (cinco) minutos, que será sigiloso até o encerramento deste prazo, observado, após esta etapa, o disposto no § 4º deste artigo. **[NOTA: art. 24, §5º, do Decreto nº 19.896/20]**
h) na hipótese de não haver licitante classificado na etapa de lance fechado que atenda às exigências para habilitação, o pregoeiro poderá, auxiliado pela equipe de apoio, mediante justificativa, admitir o reinício da etapa fechada, nos termos do disposto na letra "g". **[NOTA: art. 24, §6º, do Decreto nº 19.896/20]**

Subseção IV
Critérios de desempate em licitações de itens ampla participação

34. Em licitações de itens de ampla participação, serão observadas as seguintes disposições:
34.1 Em caso de empate, real ou ficto, será assegurada, nos termos dos arts. 44 e 45 da Lei complementar nº 123/06, a preferência de contratação para as microempresas e empresas de pequeno porte beneficiárias do regime diferenciado e favorecido, nos termos que se seguem:
34.2 Entende-se por *empate ficto* as situações em que as propostas apresentadas pelas microempresas e empresas de pequeno porte sejam até 5% (cinco por cento) superiores à proposta mais bem classificada, e *empate real* as que sejam iguais.
34.3 Em qualquer das hipóteses de empate, a microempresa ou empresa de pequeno porte mais bem classificada poderá apresentar, no prazo máximo de 5 (cinco) minutos após o encerramento dos lances, proposta de preço inferior àquela de menor valor exeqüível, sob pena de preclusão.
34.4 Se a microempresa ou empresa de pequeno porte mais bem classificada não exercer o direito, ou se sua oferta não for aceita, ou se for inabilitada, será concedido idêntico direito à microempresa ou empresa de pequeno porte subseqüente em situação de empate, se houver, na ordem classificatória, até a apuração de uma proposta que atenda às condições estabelecidas no edital.
34.5 No caso de as microempresas e empresas de pequeno porte apresentarem preços iguais, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.
34.6 O disposto neste item somente se aplica quando a melhor oferta inicial não tiver sido apresentada por microempresa ou empresa de pequeno porte.
34.7 Se não ocorrer o desempate, prevalecerá a melhor oferta inicial.
34.8 Se a melhor oferta não puder ser aceita, ou se for inabilitada a sua proponente, o responsável pela licitação avaliará a proposta subsequente, procedendo a nova verificação da ocorrência do empate ficto, se for o caso, de acordo com a disciplina ora estabelecida, e assim sucessivamente, até a obtenção de proposta válida.
34.9 Ocorrendo empate de propostas formuladas por licitantes que não detenham a condição de microempresa ou de empresa de pequeno porte, será observado o disposto na Lei estadual nº 9.433/05, procedendo-se, sucessivamente, a sorteio em ato público, para o qual as licitantes serão convocadas, vedado qualquer outro critério.

34.10 No caso de empate real entre as propostas apresentadas por microempresas e empresas de pequeno porte, em razão da ausência de disputa de lances, será realizado sorteio em ato público, para o qual as licitantes serão convocadas.
34.11. Sempre que houver sorteio deverá ser lavrada ata específica.

Subseção V
Critérios de desempate em licitações de itens restritos a microempresa e empresa de pequeno porte

35. Em licitações de itens restritos a microempresa e empresa de pequeno porte, serão observadas as seguintes disposições:
35.1 No caso de empate real entre as propostas apresentadas por microempresas e empresas de pequeno porte, será realizado sorteio em ato público, para o qual as licitantes serão convocadas.
35.2 Sempre que houver sorteio deverá ser lavrada ata específica.
36. Os critérios de desempate serão aplicados nos termos do item 34 ou 35, conforme o caso, se não houver envio de lances após o início da fase competitiva.

Subseção VI
Da divulgação do orçamento

37. Na hipótese de a licitação se processar com o orçamento sigiloso, o valor estimado ou o valor máximo aceitável para a contratação, bem como os elementos de sua composição, serão tornados públicos apenas e imediatamente após o encerramento do envio de lances. **[NOTA: art. 7º, §4º, do Decreto nº 19.896/20]**

Subseção VII
Negociação da proposta

38. Encerrada a etapa de envio de lances da sessão pública, o pregoeiro deverá encaminhar, pelo sistema eletrônico, contraproposta à licitante que tenha apresentado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das previstas no edital. **[NOTA: art. 28, caput, do Decreto nº 19.896/20]**
38.1 A negociação será realizada por meio do sistema eletrônico e poderá ser acompanhada pelos demais licitantes. **[NOTA: art. 28, §1º, do Decreto nº 19.896/20]**

Subseção VIII
Da adequação da proposta

39. O pregoeiro concederá o prazo de 3 (três) horas para envio da proposta ~~escrita~~ adequada ao último lance ofertado após a negociação de que trata o item 38, podendo ser prorrogado, mediante justificativa. **[NOTA: art. 28, §2º, do Decreto nº 19.896/20] [NOTA: art. 33 do Decreto nº 19.896/20]**
39.1 A proposta deverá contemplar a planilha com os respectivos valores readequados ao valor ofertado e registrado de menor lance.
39.1.1 Na hipótese de contratação de serviços comuns em que a legislação ou o edital exija apresentação de planilha de composição de preços, esta deverá ser encaminhada exclusivamente via sistema eletrônico, no prazo do item 39 com os respectivos valores readequados ao lance vencedor. **[NOTA: art. 30, §5º, do Decreto nº 19.896/20]**
39.2 Deverão ser encaminhados juntamente com a proposta readequada, caso tenha sido exigido na Parte I deste edital, os documentos necessários à comprovação das características descritas na proposta, tais como: catálogos, manuais, fichas de especificação técnica ou páginas da *internet* impressas.
39.3 Os documentos deverão ser apresentados em formato digital, via sistema.
39.4 Caso seja necessário, o pregoeiro poderá solicitar documentos complementares à proposta, a fim de esclarecer ou confirmar situação fática ou jurídica pré-existente, os quais deverão ser apresentados em formato digital, via sistema, no prazo de três horas a contar da solicitação, sendo vedada a inclusão de elemento que devesse constar originariamente da proposta. **[NOTA: art. 30, §3º, do Decreto nº 19.896/20]**

Seção II
Do julgamento das propostas

40. Encerrada a etapa de negociação, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação. **[NOTA: art. 29 do Decreto nº 19.896/20]**

Subseção I
Da compatibilidade do preço

41. Será desclassificada a proposta que consignar valor global superior aos praticados no mercado ou, quando for o caso, que contemple preços superiores aos preços máximos definidos no instrumento convocatório, fixados pela Administração ou por órgão oficial competente ou, ainda, aos constantes do sistema de registro de preços.
41.1 Serão também desclassificadas as propostas que consignarem preços manifestamente inexeqüíveis, assim considerados aqueles que não venham a ter demonstrada sua viabilidade através de documentação que comprove que os custos dos insumos são coerentes com os de mercado e que os coeficientes de produtividade são compatíveis com a execução do objeto do contrato.
41.2 No caso de licitações de menor preço para obras e serviços de engenharia, deverá ser observado, para efeito de manifesta inexeqüibilidade, o disposto nos §§1º e 2º do art. 97 da Lei estadual nº 9.433/05.
42. Se a melhor oferta não puder ser aceita, o responsável pela licitação avaliará a proposta subsequente, procedendo a nova verificação da ocorrência do empate ficto, se for o caso, observando o mesmo rito estabelecido, e assim sucessivamente, até a obtenção de proposta válida.

Subseção II
Das amostras ou demonstração de compatibilidade

43. Havendo necessidade de apresentação de amostras ou de demonstração de compatibilidade, o pregoeiro comunicará a todas as licitantes a suspensão da sessão, franqueará ao detentor da melhor proposta a sua realização, no prazo e forma assinalados, ficando facultado aos demais licitantes o acompanhamento.
44. Se inexitosa a aferição de qualquer amostra ou demonstração de compatibilidade, o pregoeiro procederá à convocação do detentor da proposta subsequente, na ordem de classificação, até que obtenha resultado compatível.
45. A amostra ou a demonstração de compatibilidade será analisada com o objetivo de aferir a sua adequação com os requisitos e as especificações contidas no instrumento convocatório, bem como com as consignadas na proposta apresentada pela licitante, para o que poderá ser solicitada a avaliação e análise por parte de unidade técnica competente.
46. A não apresentação de amostra ou de demonstração de compatibilidade será reputada desistência do certame, com as conseqüências estabelecidas em lei.
47. A desconformidade ou incompatibilidade com os requisitos e especificações do instrumento convocatório implicará na desclassificação da proposta, devendo observar-se o que se segue:
47.1 A amostra deverá ser entregue contra-recibo, no prazo e endereço fixados pelo pregoeiro, devendo estar em embalagem lacrada, que contenha as informações que permitam identificar a licitante e o procedimento licitatório ao qual se refere.
47.2 Os produtos apresentados como amostras poderão ser abertos, desmontados, instalados e submetidos aos testes necessários, sendo devolvidos à licitante no estado em que se encontrarem ao final da avaliação, não cabendo ressarcimento do valor do objeto.
47.3 A amostra apresentada deverá possuir elementos e quantidades suficientes que permitam a identificação do objeto, bem como a constatação de suas propriedades e do seu rendimento, além do número do registro no órgão competente, quando exigido.
47.4 Entregue a amostra, não serão permitidas quaisquer modificações no produto apresentado para fins de adequá-lo à especificação constante do instrumento convocatório.
47.5 A amostra aprovada permanecerá em poder do órgão licitante para fins de confrontação quando do recebimento do material licitado, sendo liberada somente após a conclusão do contrato.
47.6 As amostras reprovadas deverão ser retiradas em até 30 (trinta) dias, contados da publicação da homologação da licitação, ficando esclarecido que as que não forem retiradas nesse prazo serão descartadas, sem direito a indenização.
47.7 Em nenhuma hipótese as amostras apresentadas serão tidas como início de entrega dos materiais ofertados.

CAPÍTULO III
DA HABILITAÇÃO

48. O pregoeiro conferirá e examinará os documentos de habilitação, emitindo o Certificado de Registro das empresas cadastradas e verificando a regularidade da documentação exigida no instrumento convocatório. **[NOTA: art. 30, caput, do Decreto nº 19.896/20]**
48.1 Serão inabilitadas as licitantes cujos documentos exigidos para habilitação não tenham sido apresentados na forma do edital, ou que não estejam contemplados no Registro Cadastral, ou que dele constem como vencidos, ressalvado o disposto no item 48.2. **[NOTA: art. 30, §1º, do Decreto nº 19.896/20]**
48.2 Desde que possível tecnicamente, a verificação pelo órgão ou entidade promotora do certame nos sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação. **[NOTA: art. 30, §2º, do Decreto nº 19.896/20]**

48.3 Caso seja necessário, o pregoeiro poderá solicitar documentos complementares à habilitação, a fim de esclarecer ou confirmar situação fática ou jurídica pré-existente, os quais deverão ser apresentados em formato digital, via sistema eletrônico, no prazo de 03 (três) horas a contar da solicitação, vedada a inclusão posterior de elemento que devesse constar originariamente dos documentos de habilitação. **[NOTA: art. 30, §3º do Decreto nº 19.896/20]**
49. Não sendo aceitável a proposta vencedora, ou se o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao edital. **[NOTA: art. 30, §4º, do Decreto nº 19.896/20]**
50. A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte será exigida nos termos do disposto nos arts. 42 e 43, ambos da Lei Complementar Federal nº 123, de 14 de dezembro de 2006. **[NOTA: art. 30, §6º do Decreto nº 19.896/20]**
51. Constatado o atendimento às exigências estabelecidas no edital, a licitante será declarada vencedora. **[NOTA: art. 30, §7º do Decreto nº 19.896/20]**
51.1 Havendo necessidade de suspensão da sessão pública para a declaração do vencedor por prazo superior a 03 (três) horas a contar do encerramento da etapa de lances, a nova sessão somente poderá ser reiniciada mediante aviso prévio no sistema eletrônico, observada a antecedência mínima de 24 (vinte e quatro) horas, e a ocorrência será registrada em ata. **[NOTA: art. 30, §8º do Decreto nº 19.896/20]**

CAPÍTULO IV
DOS RECURSOS

52. Declarado o vencedor, qualquer licitante poderá, no prazo de até 30 (trinta) minutos manifestar sua intenção de recorrer, de forma imediata e motivada, em campo próprio do sistema eletrônico. **[NOTA: art. 32 do Decreto nº 19.896/20]**
52.1 As razões do recurso de que trata o *caput* deste artigo deverão ser apresentadas no prazo de 03 (três) dias úteis. **[NOTA: art. 32, §1º, do Decreto nº 19.896/20]**
52.2 As demais licitantes ficarão intimados para, se desejarem, apresentar suas contrarrazões, no prazo de 03 (três) dias úteis, contado da data final do prazo do recorrente, assegurada vista imediata dos elementos indispensáveis à defesa dos seus interesses. **[NOTA: art. 32, §2º, do Decreto nº 19.896/20]**
52.3 A ausência de manifestação imediata e motivada da licitante quanto à intenção de recorrer, nos termos do disposto no *caput* deste artigo, importará na decadência desse direito, e o pregoeiro estará autorizado a adjudicar o objeto à licitante declarada vencedora. **[NOTA: art. 32, §3º, do Decreto nº 19.896/20]**
52.4 O acolhimento do recurso importará na invalidação apenas dos atos que não podem ser aproveitados. **[NOTA: art. 32, §4º, do Decreto nº 19.896/20]**

CAPÍTULO V
DA REGULARIZAÇÃO FISCAL E TRABALHISTA
DAS MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE

53. Sagrando-se vencedora do certame microempresa ou empresa de pequeno porte, beneficiária do regime diferenciado da Lei Complementar nº 123/06, cuja habilitação tenha sido procedida com a ressalva de existência de restrição fiscal e/ou trabalhista, será assegurado o prazo de 5 (cinco) dias úteis, cujo termo inicial corresponderá ao momento em que a proponente for declarada a vencedora do certame, prorrogável por igual período, a critério da Administração Pública, para a regularização da documentação, pagamento ou parcelamento do débito e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa.
53.1 A não-regularização da documentação no prazo previsto neste item implicará decadência do direito à contratação, sem prejuízo das sanções previstas pelo ilícito tipificado no art. 184, VI da Lei estadual nº 9.433/05, sendo facultado à Comissão de Licitação ou ao pregoeiro, conforme o caso, proceder à convocação das licitantes remanescentes, na ordem de classificação, ou revogar a licitação.

CAPÍTULO V - A
DA FORMAÇÃO DO CADASTRO DE RESERVA, NO SISTEMA DE REGISTRO DE PREÇOS

53-A. Tratando-se de licitação para registro de preços, serão incluídos na respectiva ata, na forma de anexo, os licitantes que aceitarem cotar os bens ou serviços com preços iguais aos do licitante vencedor, observada a sequência da classificação do certame.
53-A.1 A inclusão a que se refere este item tem por objetivo a formação de cadastro de reserva no caso de impossibilidade de atendimento pelo primeiro colocado da ata.
53-A.2 O responsável pela licitação facultará às licitantes que desejem integrar o cadastro de reserva a apresentação de amostras ou demonstração de compatibilidade e a realização da habilitação, como condição para que seus preços sejam registrados, para o que será adotado, no que couber, os mesmos ritos e prazos definidos neste Título.

53-A.2.1 Na hipótese de licitação por lotes, o patrimônio líquido exigível será calculado em função da soma de tantos quantos forem os lotes em que a licitante tenha manifestado interesse, até que seja atingido o limite da capacidade econômico-financeira, sendo vedada a escolha, pela licitante, dos lotes para os quais deseja a habilitação.
53-A.3 A formalização do cadastro de reserva far-se-á mediante a juntada da ata de realização da sessão pública da licitação que contenha a informação dos licitantes que aceitaram praticar os mesmos preços ofertados pelo vencedor do certame.
53-A.4 Não poderão compor o cadastro de reserva as propostas que não tenham sido classificadas e cujos licitantes não tenham sido habilitados.
53-A.5 Se houver mais de um licitante na situação de que trata este item, a formação do cadastro de reserva deverá obedecer a sequência da classificação do certame.
53-A.6 Nas licitações para registro de preços realizadas sob a modalidade pregão, além das licitantes que aceitarem cotar os bens ou serviços com preços iguais ao da licitante vencedora, será admitida a inclusão, no anexo da ata a que se refere este item, das licitantes cujos preços, ao final da etapa de lances, estejam compatíveis com os preços correntes no mercado ou fixados pela Administração Pública Estadual ou por órgão oficial competente ou constantes da tabela de preços referenciais, e que tenham manifestado interesse em integrar o cadastro de reserva nesta condição **[NOTA: §6º do art. 16 do Decreto nº 19.252/19]**
53-A.7 As licitações para registro de preços destinadas à aquisição de bens e serviços comuns da área da saúde a que se refere a Lei Federal nº 10.191, de 14 de fevereiro de 2001, observarão, na modalidade pregão, o disposto no art. 2-A daquele diploma. **[NOTA: conforme §7º do art. 16 do Decreto nº 19.252/19]**
53-A.8 Para as licitantes beneficiárias do regime diferenciado da Lei complementar nº 123/06, que manifestarem interesse em integrar o cadastro de reserva e cuja habilitação tenha sido procedida com a ressalva de existência de restrição fiscal e/ou trabalhista, será assegurado o prazo de 5 (cinco) dias úteis para a regularização da documentação, pagamento ou parcelamento do débito e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa, computando-se o termo inicial da data da convocação para substituição do fornecedor originário.

CAPÍTULO VI
DA HOMOLOGAÇÃO E ADJUDICAÇÃO

54. Decididos os recursos e constatada a regularidade dos atos procedimentais, a autoridade superior fará a adjudicação do objeto ao licitante vencedor e homologará a licitação. **[NOTA: art. 34, caput, do Decreto nº 19.896/20]**
55. Na ausência de recurso ou quando a decisão que o ensejou tenha sido reconsiderada, caberá ao pregoeiro adjudicar o objeto, encaminhar o processo devidamente instruído à autoridade superior e propor a homologação. **[NOTA: art. 34, parágrafo único, do Decreto nº 19.896/20]**
56. A homologação e a adjudicação do objeto desta licitação não implicará direito à contratação.

TÍTULO V
DAS IMPUGNAÇÕES E DOS PEDIDOS DE ESCLARECIMENTOS

CAPÍTULO I
DAS IMPUGNAÇÕES

57. Qualquer pessoa poderá impugnar os termos do edital do pregão até 03 (três) dias úteis anteriores à data fixada para abertura da sessão pública. **[NOTA: art. 13 do Decreto nº 19.896/20]**
57.1 A impugnação não possui efeito suspensivo e caberá ao pregoeiro decidir no prazo de 02 (dois) dias úteis, contado da data de recebimento da impugnação. **[NOTA: art. 13, §1º, do Decreto nº 19.896/20]**
57.2 A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro nos autos do processo de licitação. **[NOTA: art. 13, §2º, do Decreto nº 19.896/20]**
57.3 O pregoeiro poderá solicitar a manifestação dos setores técnicos, a fim de subsidiar a decisão quanto às impugnações, promovendo a oitiva, quando necessário, do órgão legal de assessoramento jurídico. **[NOTA: art. 13, §3º, do Decreto nº 19.896/20]**
57.4 Se reconhecida a procedência das impugnações, as modificações do edital serão divulgadas pelo mesmo instrumento de publicação utilizado para divulgação do texto original e o prazo inicialmente estabelecido será reaberto, exceto se, inquestionavelmente, a alteração não afetar a formulação das propostas, resguardado o tratamento isonômico aos licitantes. **[NOTA: art. 15 do Decreto nº 19.896/20]**

CAPÍTULO II
DOS PEDIDOS DE ESCLARECIMENTOS

58. Os pedidos de esclarecimentos referentes ao processo licitatório deverão ser enviados ao pregoeiro até 03 (três) dias úteis anteriores da data fixada para a realização da sessão pública do pregão. **[NOTA: art. 14 do Decreto nº 19.896/20]**

58.1 O pregoeiro responderá aos pedidos de esclarecimentos no prazo de 02 (dois) dias úteis, contado da data de recebimento do pedido, e suas respostas vincularão os participantes e a Administração Pública Estadual. **[NOTA: art. 14, §1º, do Decreto nº 19.896/20]**
58.2 O pregoeiro poderá solicitar a manifestação dos setores técnicos, a fim de subsidiar a decisão quanto aos pedidos de esclarecimentos, promovendo a oitiva, quando necessário, do órgão legal de assessoramento jurídico. **[NOTA: art. 14, §2º, do Decreto nº 19.896/20]**
58.3. Se na resposta aos pedidos de esclarecimentos verificar-se a necessidade de modificações do edital, estas serão divulgadas pelo mesmo instrumento de publicação utilizado para divulgação do texto original e o prazo inicialmente estabelecido será reaberto, exceto se, inquestionavelmente, a alteração não afetar a formulação das propostas, resguardado o tratamento isonômico aos licitantes. **[NOTA: art. 15 do Decreto nº 19.896/20]**

TÍTULO VI
DAS DISPOSIÇÕES FINAIS

59. A qualquer tempo, antes da data fixada para apresentação das propostas, poderá o responsável pela licitação, se necessário, modificar este instrumento, hipótese em que deverá proceder à divulgação, reabrindo-se o prazo inicialmente estabelecido, exceto quando, inquestionavelmente, a alteração não afetar a formulação das propostas.
59.1 As modificações do edital serão divulgadas pelo mesmo instrumento de publicação utilizado para divulgação do texto original e o prazo inicialmente estabelecido será reaberto, exceto se, inquestionavelmente, a alteração não afetar a formulação das propostas, resguardado o tratamento isonômico aos licitantes. **[NOTA: art. 15 do Decreto nº 19.896/20]**
60. O pregoeiro poderá em qualquer fase da licitação, suspender os trabalhos, procedendo ao registro da suspensão e a convocação para a continuidade dos mesmos, bem como promover diligências destinadas a esclarecer ou a complementar a instrução do processo licitatório, desde que não implique em inclusão de documento ou informação que deveria constar originariamente da proposta.
61. O pregoeiro poderá, no julgamento da habilitação e das propostas, sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível aos licitantes, e lhes atribuirá validade e eficácia para fins de habilitação e classificação. **[NOTA: art. 31, caput, do Decreto nº 19.898/20]**
61.1 Havendo necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento de que trata este item, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, 24 (vinte e quatro) horas de antecedência, e a ocorrência será registrada em ata. **[NOTA: art. 31, §1º, do Decreto nº 19.898/20]**
61.2 Quando todas as propostas forem desclassificadas ou todos os licitantes forem inabilitados, o pregoeiro poderá, caso se esta funcionalidade estiver disponível no sistema, suspender o pregão e estabelecer uma nova data, com prazo não superior a 03 (três) dias úteis, para o recebimento de nova proposta ou nova documentação, após sanadas as causas que motivaram a desclassificação ou inabilitação. **[NOTA: art. 31, §2º, do Decreto nº 19.898/20]**
62. O pregoeiro poderá, a qualquer tempo, negociar com o proponente da melhor oferta aceitável, visando obter preço menor.
63. Os participantes da licitação têm direito público subjetivo à fiel observância do procedimento estabelecido neste Decreto e qualquer interessado poderá acompanhar o seu desenvolvimento. **[NOTA: art. 39, §2º, do Decreto nº 19.898/20]**
64. A instrução do processo licitatório poderá ser realizada por meio de sistema eletrônico, cujos documentos, constantes dos arquivos e registros digitais, serão válidos para todos os efeitos legais. **[NOTA: art. 39, §1º, do Decreto nº 19.898/20]**
64.1 Os atos do procedimento do pregão eletrônico serão disponibilizados para acesso livre, nos termos da legislação pertinente, ressalvados os documentos sigilosos, apenas enquanto perdurar esta condição. **[NOTA: art. 39, §3º, do Decreto nº 19.898/20]**
64.2 Os arquivos e os registros digitais relativos ao pregão eletrônico serão documentados no processo respectivo com vistas à aferição de sua regularidade pelos agentes de controle, nos termos da legislação pertinente. **[NOTA: art. 39, §4º, do Decreto nº 19.898/20]**
65. Os casos omissos serão dirimidos pelo pregoeiro, com observância da legislação em vigor.

TÍTULO VII
DA REVOGAÇÃO E ANULAÇÃO

66. A licitação poderá ser revogada ou anulada nos termos do art. 122 da Lei estadual nº 9.433/05.

TÍTULO VIII
DA CONTRATAÇÃO
CAPÍTULO I
DA FASE PRÉ-CONTRATUAL
Seção I-A
Da Ata de Registro de Preços, no Sistema de Registro de Preços

66-A. Tratando-se de licitação para registro de preços, homologado o resultado da licitação, o fornecedor mais bem classificado será convocado para assinar a ata de registro de preços, no prazo definido no PREÂMBULO deste edital, podendo o prazo ser prorrogado uma vez, por igual período, quando solicitado pelo fornecedor e desde que ocorra motivo justificado aceito pela Administração Pública Estadual.
66-A.1 A recusa injustificada do fornecedor classificado a assinar a ata, dentro do prazo de validade da proposta, ensejará a aplicação das penalidades legalmente estabelecidas, especialmente, nos termos do inciso IV do art. 33, da Lei estadual nº 9.433/05, a aplicação de multa prevista no art. 192, inciso I, c/c art. 19, parágrafo único do Decreto estadual nº 13.967/12 e a suspensão temporária do direito de participar de licitação e impedimento de contratar com a Administração, nos termos do art. 184, inciso VI, combinado com o art. 194 Lei estadual nº 9.433/05.
66-A.2 Equipara-se à recusa prevista no item 67.1 artigo a circunstância do adjudicatário do registro de preços deixar de manter as condições de habilitação exigidas na licitação, ou, por qualquer meio, dar causa à impossibilidade de subscrição da ata.
66-A.3 É facultado à Administração Pública estadual, quando o convocado não assinar a ata de registro de preços no prazo e condições estabelecidos, convocar os licitantes remanescentes, constantes do cadastro de reserva, na ordem de classificação. **[NOTA: art. 16 do Decreto nº 19.252/19]**
66-A.4 A assinatura da ata de registro de preços implicará compromisso de fornecimento nas condições estabelecidas.
66-A.5 A ata de registro de preços obedecerá as condições da minuta constante deste instrumento convocatório.
66-A.6 A critério da Administração, a assinatura da ata de registro de preços se dará por meio do Sistema Eletrônico de Informações - SEI, caso em que a licitante deverá providenciar o cadastramento de seu representante legal ou procurador no endereço eletrônico www.defensoria.ba.def.br.
66-A.6.1 A recusa da adjudicatária em obter o credenciamento ou a subscrever eletronicamente a ata de registro de preços implicará na decadência ao direito de contratação, sem prejuízo das sanções previstas na legislação específica.

Seção I
Da verificação da manutenção das condições de habilitação

67. Como condição para celebração do contrato, a licitante vencedora deverá fazer prova da manutenção de todas as condições de habilitação, o que também poderá ser aferido, se disponível, mediante consulta ao Registro Cadastral ou a sites oficiais.

Seção II
Da minuta de contrato

68. A contratação com a licitante vencedora obedecerá as condições da minuta de contrato constante do instrumento convocatório, facultada a substituição, a critério da Administração, por instrumento equivalente, desde que presentes as condições do art. 132 da Lei estadual nº 9.433/05.
69. Considerar-se-ão literalmente transcritas no instrumento equivalente todas as cláusulas e condições previstas na minuta de contrato constante do convocatório.

CAPÍTULO II
DA ASSINATURA DO CONTRATO
Seção I
Da Convocação

70. O adjudicatário será convocado a assinar o termo de contrato, ou instrumento equivalente, se for o caso, no prazo fixado no edital, na forma dos §§3º e 4º do art. 124 da Lei estadual nº 9.433/05, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas no inciso I do art. 192 e no art. 194 da Lei estadual nº 9.433/05, podendo solicitar sua prorrogação por igual período, por motivo justo e aceito pela Administração.
70.1 A assinatura do contrato, ou instrumento equivalente, se for o caso, deverá ser realizada pelo representante legal da empresa ou mandatário com poderes expressos.
70.2 No sistema de registro de preços, a recusa injustificada do fornecedor em subscrever o termo de contrato ou instrumento equivalente ensejará a aplicação das penalidades legalmente estabelecidas. **[NOTA: conforme §1º do art. 25 do Decreto nº 19.252/19]**

70.2.1 Equipara-se à recusa prevista a circunstância de o fornecedor deixar de manter as condições de habilitação exigidas na licitação, ou, por qualquer meio, dar causa à impossibilidade de subscrição do contrato. **[NOTA: conforme §2º do art. 25 do Decreto nº 19.252/19]**
70.2.2 O disposto neste item também se aplica aos integrantes do cadastro de reserva, que, convocados na forma do *caput* deste item, não honrem o compromisso assumido, sem justificativa ou com justificativa recusada pela Administração. **[NOTA: conforme §3º do art. 25 do Decreto nº 19.252/19]**
71. A critério da Administração, a assinatura do contrato ou do instrumento equivalente se dará por meio do Sistema Eletrônico de Informações – SEI-DPE, caso em que a licitante deverá providenciar o cadastramento de seu representante legal ou procurador no endereço eletrônico www.defensoria.ba.def.br.
71.1 A recusa da adjudicatária em se cadastrar ou a subscrever eletronicamente o contrato ou instrumento equivalente implicará na decadência da contratação e à sujeição às sanções cominadas na legislação.

Seção II
Da impossibilidade de contratação

72. Na contratação delegada, se a licitante vencedora, convocada dentro do prazo de validade de sua proposta, não celebrar o contrato, é facultado ao pregoeiro examinar e verificar a aceitabilidade das propostas subseqüentes, na ordem de classificação, bem como o atendimento das condições de habilitação, adotando os procedimentos imediatamente posteriores ao encerramento da etapa de lances, sem prejuízo da aplicação das sanções previstas na legislação pertinente. **[NOTA: art. 119, parágrafo único e art. 36, caput, do Decreto nº 19.896/20.**
72.1 Na licitação para registro de preços, quando o convocado não assinar o contrato no prazo e condições estabelecidos, é facultado à Administração Pública convocar os licitantes remanescentes, constantes do cadastro de reserva, na ordem de classificação. **[NOTA: art. 16 do Decreto nº 19.252/19]**

CAPÍTULO III
DOS PRAZOS DE DURAÇÃO

73. A vigência contratual observará o prazo estabelecido na minuta de contrato constante do instrumento convocatório, sendo vedada a fixação de prazo de vigência indeterminado.

CAPÍTULO IV
DAS GARANTIAS
74. As garantias contratuais, quando exigidas, deverão recair sobre uma das modalidades previstas na lei, observadas as disposições da minuta de contrato constante do instrumento convocatório.

CAPÍTULO V
DO REAJUSTAMENTO E DA REVISÃO DA PROPOSTA

75. O reajustamento dos preços contratuais observará os índices específicos ou setoriais mais adequados à natureza da obra, compra ou serviço, conforme definido na minuta de contrato constante do instrumento convocatório.
75.1. Os preços poderão ser revistos nas hipóteses previstas na Lei estadual nº 9.433/05, observados os parâmetros definidos na minuta de contrato constante do instrumento convocatório.

CAPÍTULO VI
DAS ALTERAÇÕES CONTRATUAIS

76. O contrato poderá ser alterado, mediante justificação expressa, nas hipóteses previstas na Lei estadual nº 9.433/05.
77. Os atos de prorrogação, suspensão ou rescisão dos contratos administrativos sujeitar-se-ão às formalidades exigidas para a validade do contrato originário.
78. Independem de termo contratual aditivo, podendo ser registrado por simples apostila: a) a simples alteração na indicação dos recursos orçamentários ou adicionais custeadores da despesa, sem modificação dos respectivos valores; b) o reajustamento de preços previsto no edital e no contrato; c) as atualizações, compensações ou apenações financeiras decorrentes das condições de pagamento dos mesmos constantes.

CAPÍTULO VII
DA EXECUÇÃO E FISCALIZAÇÃO DO OBJETO CONTRATUAL

79. A execução e a fiscalização do objeto contratual obedecerão as disposições previstas na minuta de contrato constante do instrumento convocatório, ficando esclarecido que a ação ou omissão, total ou parcial da fiscalização não eximirá a Contratada da total responsabilidade pelas obrigações assumidas.

CAPÍTULO VIII
DO RECEBIMENTO DO OBJETO CONTRATUAL

80. O recebimento do objeto contratual obedecerá as disposições previstas na minuta de contrato constante do instrumento convocatório.

CAPÍTULO IX
DA INEXECUÇÃO E DA RESCISÃO

81. A inexecução total ou parcial do contrato ensejará a sua rescisão, com as conseqüências contratuais e as previstas na Lei estadual nº 9.433/05, observados os parâmetros definidos na minuta de contrato constante do instrumento convocatório.

TÍTULO IX
DAS PENALIDADES

82. Constituem ilícitos administrativos as condutas previstas nos arts. 184, 185 e 199 da Lei estadual nº 9.433/05, sujeitando-se os infratores às cominações legais, especialmente as definidas no art. 186 do mesmo diploma, garantida a prévia e ampla defesa em processo administrativo.
82.1 A Critério da Administração, nos termos do art. 8º, IV c/c art. 89 e art. 95 da Lei nº 12.290, de 20 de abril de 2011, as notificações e intimações de atos dos processos administrativos poderão ser realizadas através do endereço eletrônico fornecido pela licitante no cadastro do Sistema Eletrônico de Informações – SEI.
83. Para a aplicação das penalidades serão levados em conta a natureza e a gravidade da falta, os prejuízos dela advindos para a Administração Pública e a reincidência na prática do ato, observando-se os critérios de dosimetria estabelecidos pelo Decreto estadual nº 13.967/12.

CAPÍTULO I
DA DECLARAÇÃO DE INIDONEIDADE

84. Serão punidos com a pena de declaração de inidoneidade para licitar e contratar com a Administração, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a autoridade competente para aplicar a punição, os que incorram nos ilícitos previstos nos incisos I a V do art. 184, nos incisos II, III e V do art. 185 e no art. 199 da Lei estadual nº 9.433/05.

CAPÍTULO II
DA SUSPENSÃO TEMPORÁRIA

85. Serão punidos com a pena de suspensão temporária do direito de cadastrar e licitar e impedimento de contratar com a Administração os que incorram nos ilícitos previstos nos incisos VI e VII do art. 184 e nos incisos I, IV, VI e VII do art. 185 da Lei estadual nº 9.433/05.

CAPÍTULO III
DA ADVERTÊNCIA VERBAL

86. Será advertido verbalmente a licitante cuja conduta vise perturbar o bom andamento da sessão, podendo o responsável pela licitação determinar a sua retirada do recinto, caso persista na conduta faltosa.

CAPÍTULO IV
DO DESCREDENCIAMENTO DO SISTEMA DE REGISTRO CADASTRAL

87. A licitante ou contratada será descredenciada do Sistema de Registro Cadastral quando, em razão da ocorrência das faltas previstas na Lei estadual nº 9.433/05, deixar de satisfazer as exigências relativas à habilitação jurídica, qualificação técnica, qualificação econômico-financeira, ou regularidade fiscal e trabalhista exigidas para cadastramento.

CAPÍTULO V
DA MULTA

88. A recusa à assinatura do contrato, pelo adjudicatário, no prazo fixado no instrumento convocatório, ensejará a aplicação da pena de multa de mora no percentual de 10% (dez por cento) incidente sobre o valor global do contrato, sem prejuízo das demais sanções previstas na Lei estadual nº 9.433/05.

88.1 No sistema de registro de preços, recusando-se o adjudicatário a subscrever ata, a multa será de 5% (cinco por cento) e incidirá sobre o valor correspondente ao objeto que lhe foi adjudicado
88.2 Equipara-se à recusa prevista no item 88.1 a circunstância de o adjudicatário do registro de preços deixar de manter, durante todo o período de validade do registro, as condições de habilitação exigidas na licitação, caso em que a multa de 5% (cinco por cento) será aplicada sobre a diferença entre o valor global do objeto adjudicado e o valor da parte do fornecimento ou do serviço já realizado.
89. A inexecução contratual, inclusive por atraso injustificado na execução do contrato, sujeitará o contratado à multa de mora, na forma prevista na minuta de contrato constante do instrumento convocatório, que será graduada de acordo com a gravidade da infração, observado o disposto na Lei estadual nº 9.433/05 e no Decreto estadual nº 13.967/12.

TÍTULO X
DO FORO

90. Para quaisquer questões judiciais oriundas do presente edital, prevalecerá o Foro da Comarca de Salvador, Estado da Bahia, com exclusão de qualquer outro, por mais privilegiado que seja.