TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS
Avenida Aristeu de Andrade nº 377 - Bairro Farol - CEP 57051-090 - Maceió - AL

Termo de Referência - TIC nº 6 / 2020

Termo de Referência - Soluções de Tecnologia da Informação

QUADRO RESUMO

01. Objeto	Registro de preço para eventual aquisição de solução Firewall para o Prédio Sede do TRE/AL, cartórios Eleitorais, unidades e escritórios remotos.
02. Quantidade	160
03. Resumo da Especificação do Objeto	Há a necessidade de se buscar o detalhamento e atendê-lo (Item DETALHAMENTO DO OBJETO (Art. 18, § 3º, III)). Todavia, de forma resumida temos: **Firewalls de Pequeno Porte**; Performance de IPS de 100 Mbps ou superior;; Mínimo de 512MB de memória RAM para maior confiabilidade do sistema. Sistema Operacional do Tipo "Harderizado" não serão aceitos. Apenas os que forem armazenados em memória flash. Fonte de alimentação com operação automática entre 110/220V. Suportar 5 interfaces 10/100/1000 Gbe; Performance de todos os serviços ativos UTM (Gateway Antivírus, Gateway Anti Spyware, IDS, IPS e Filtro de Conteúdo) deverá ser de 50 Mbps ou superior; Garantia de 36 meses;
04. Valor Estimado	Com base no registro de preços do TRE/TO e no Registro de Preços passado deste Regional , temos (R$ 4.350,00 + R$ 4.999,00)/2 e, portanto, preço médio de R$ 4.674,50. A ser confirmado pela SEIC/COMAP Projeção para o exercício 2020: 40 Unidades x R$ 4.674,50,00 = R$ 186.980,00 (destinadas aos cartórios e escritórios remotos, localizados em prédios da Justiça Eleitoal em Alagoas)

	Referência: Estudos Preliminares Item 11
05. Justificativa	Efetivamente, trata-se de ampliação da confiabilidade e da segurança da malha de comunicação de dados entre a Sede do TRE/AL e as zonas eleirorais/escritórios remotos da Justiça Eleitoral em Alagoas. Desta forma, optou-se pela expansão do uso de equipamentos Firewall NG, que suprem as necessidades da solução.
06. Prazo de Entrega	O prazo máximo para o fornecimento das licenças é de 45 (quarenta e cinco) dias corridos após o recebimento da ordem de fornecimento, nota de empenho ou documento equivalente.
07. Adjudicação	(Por Item)
08. Classificação Orçamentária	(A cargo da COFIN). Sugerindo-se material permanente de TI.
09. Local de Entrega	Almoxarifado do Tribunal Regional Eleitoral de Alagoas Av. Menino Marcelo, 7200D, Serraria Maceió – AL CEP 57046-005 Tel.: (82) 3328-1947 Horário: De segunda-feira a quinta-feira das 13 às 19h e sexta-feira das 7h30min Às 13h30min.
10. Unidade Fiscalizadora	SSO/CIE/STI
11. Unidade Gestora	SAD
12. Sanções Administrativas	Vide Item 3.2 Forma de Execução e de Gestão do Contrato (Art. 18, § 3º, III, a) Subitem Penalidades (Art. 18, § 3º, III, a, 11)
13. Prazo de Pagamento	Vide Item 3.2 Forma de Execução e de Gestão do Contrato (Art. 18, § 3º, III, a) Subitem Forma de Pagamento (Art. 18, § 3º, III, a, 7)
14. Estratégia de Recebimento	Vide Item 3.2 Forma de Execução e de Gestão do Contrato (Art. 18, § 3º, III, a) Subitem Recebimento do Objeto:
15. Modalidade e Tipo de Licitação	Vide 2.11 Modalidade, Tipo de Licitação, Critérios de Habilitação e Atendimento aos Requisitos (Art. 18, § 3º, II, j, IV e V)

1. OBJETO (Art. 18, §3º,I):

Registro de preço para eventual aquisição de solução Firewall para o Prédio Sede do TRE/AL, cartórios Eleitorais, unidades e escritórios remotos.

1.1 Definição (Art. 18, §3º, I)

Registro de preço para eventual aquisição de solução Firewall para o Prédio Sede do TRE/AL, cartórios Eleitorais, unidades e escritórios remotos.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO (Art. 18, § 3º, II)

2.1 Motivação (Art. 18, § 3º, II, a)

A contínua evolução na área de tecnologia da informação fornece novas soluções que tornam mais eficientes os meios de comunicação de dados, permitindo, desta maneira, a utilização de novos recursos como forma de aumentar disponibilidade, segurança e performance de tais meios.

Neste sentido, surge a necessidade de fomentar Registro de Preço para aquisição de até 160 (cento e sessenta) Firewalls de pequeno porte, como medida de viabilização a melhoria da segurança, da performance e da confiabilidade dos meios de comunicação que são utilizados pelos cartórios eleitorais e escritórios remotos da Justiça Eleitoral em Alagoas, a acrescer camada adicional de proteção composta por IPS/IDS, filtro de conteúdo, antimalware e antispyware.

Além dos ínúmeros contextos e relatos de invasão de redes disponíveis na literatura ou no registro de noticiário, neste momento de pandemia, COVID-19, com a edição dos mais diversos atos de teletrabalho ou afastamente para realização de trabalhos a partir de casa, a solução pode constituir medida vital para garantir conexões que, se por um lado, garantem o acesso pelos servidores de Sistemas e dados internos da instiuição, garanta, por outro lado, a segurança do maior ativo. maior valor de qualquer instuição: seus dados e informaçõs.

;

- A sugestão de uso de Registro de Preços, da forma como proposta, tem alicerce no Decreto nº 7.892/2013, art. 3º, incisos I, II e IV, assim ponderados:
  - Inciso I: a aquisição de firewalls pode ser frequente, considerando a migração progressiva da rede de dados do atual modelo de contratação - links dedicados, para links ADSL de menor custo;
  - Inciso II: a entrega deve ser sucessiva, de forma a minimizar impactos nos prazos de garantia dos equipamentos, considerando a complexidade de sua efetiva implantação e substituição aos equipamentos anteriores;
  - Inciso IV: não é possível, a priori, ter uma visão clara, da quantidade de equipamentos efetivamente necessários para substituir o atual modelo de conexões dedicadas.

2.2 Objetivos (Art. 18, § 3º, II, b)

A contratação visa, além de promover ações no sentido de elaborar novo instrumento que mantenha um meio para disponibilizar os firewalls demandados, promover as condições para migração do atual modelo de conexões dedicadas (backbone secundário) para um conjunto de menor custo baseado em conexões ADSL, por exemplo e redundânicia de enlaces na forma preconizada pela Resolução CNJ nº 211/2015.

2.3 Benefícios (Art. 18, § 3º, II, c)

- Permitir a criação de malha de comunicação redundante.
- Ampliar a segurança da comunicação e do acesso à Internet das zonas eleitorais
- Permitir a otimização dos enlaces MPLS para uso dos sistemas eleitorais e internos da Justiça Eleitoral
- Acompanhamento centralizado da comunicação das zonas eleitorais;
- Permitir criação de VPNs reguladas e geridas centralizadamente, tais como as demandadas pelo teletrabalho motivado pela pandemia de COVID-19.

2.4 Alinhamento Estratégico (Art. 18, § 3º, II, d)

O alinhamento com o PEI é identificado na visão do recursos de infraestrutura e tecnologia em seus dois aspectos apontados:

1 – Garantir a infraestrutura física apropriadas às atividades administrativas e judiciais e

2 – Garantir a infraestrutura de TI, pois o equipamento fará parte de um conjunto de medidas de salvaguarda e segurança da informação.

Alinhamento com os Objetivos Estratégicos da Estratégia Nacional de TIC do Poder Judiciário nos seguintes aspectos:

1. Prover infraestrutura de TIC apropriada às atividades judiciais e administrativas; e
2. Aprimorar a segurança da informação.

Alinhamento com os Objetivos Estratégicos de TIC da Justiça Eleitoral de Alagoas – 2017/2022 nos seguintes aspectos:

1. Viabilizar serviços e soluções de TIC; e
2. Aprimorar a segurança da informação.

2.5 Referência aos Estudos Preliminares (Art. 18, § 3º, II, e)

Este Termo de Referência foi elaborado considerando o Documento de Oficialização de Demanda (DOD) encaminhado pela Secretaria de Tecnologia da Informação (STI) e os Estudos Preliminares constantes do Processo SEI nº 0001030-68.2020.6.02.8000.

2.6 Relação entre a Demanda Prevista e a Contratada (Art. 18, §3º, II, f)

É pretendida a aquisiçao de forma concomite e progressiva à contratação de enlaces em banda larga para os cartórios eleitorais.

2.7 Análise de Mercado de TIC (Art. 18, § 3º, II, g)

Verifica-se que os bens e serviços pretendidos poderão ser fornecidos por diferentes empresas no mercado de TIC.

Considerando o Item 7 dos Estudos Preliminares, não se vislumbrou alternativa que não o presente Registro de Preços.

2.8 Natureza do Objeto (Art. 18, § 3º, II, h)

Os bens e serviços a serem contratados possuem características comuns e usuais encontradas atualmente no mercado de TIC, cujos padrões de desempenho e de qualidade podem ser objetivamente definidos neste Termo de Referência.

O objeto desta contratação tem como escopo a obtenção de produto específico em período determinado, portanto não se caracteriza como serviço de natureza continuada.

2.9 Parcelamento e Adjudicação do Objeto (Art. 18, § 3º, II, i)

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

Adjudicação será por item.

2.10 Vigência

Será, na forma dos normativos vigentes, o tempo máximo do Registro de Preços.

A vigência da ata será de 12 (doze) meses, contados a partir de sua assinatura.

A utilização do sistema de Registro de Preços visa, primordialmente, a redução de número de licitações para o mesmo objeto, porquanto se concentra em um único procedimento a possibilidade de realizar diversas aquisições recorrentes e necessárias, via ordens de fornecimento, durante o lapso temporal de sua vigência, em face de os preços permanecerem à disposição da Administração.

2.11 Modalidade, Tipo de Licitação, Critérios de Habilitação e Atendimento aos Requisitos (Art. 18, § 3º, II, j, IV e V)

A aquisição pretendida deverá ser realizada por meio de licitação do tipo Pregão Eletrônico, como é de praxe neste Regional, salvo entendimento superior contrário.

A sugestão da equipe de planejamento, por se tratar de fornecimento de equipamento, é pela contratação por licitação via pregão. Por conta de possibilidade de contingenciamento orçamentário indicamos a modalidade de registro de preços.

O DECRETO Nº 7.174, DE 12 DE MAIO DE 2010 que regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União deve ser aplicado nesta aquisição por se tratar de bem de informática.

A ressalva que a equipe aponta é em relação ao artigo 3º, item II que versa sobre a necessidade de exigências, na fase de habilitação, de certificações emitidas por instituições públicas ou privadas credenciadas pelo Instituto Nacional de Metrologia, Normalização e Qualidade Industrial (Inmetro), que atestem, conforme regulamentação específica, a adequação à segurança para o usuário e instalações, compatibilidade eletromagnética e consumo de energia.

Tal exigência inviabiliza e restringe a competição deste certame, vez que a certificação para este tipo de produto, segundo o próprio INMETRO, é voluntária, conforme Portaria Inmetro n.º 170 de 10/04/2012.

(fonte:http://www.inmetro.gov.br/legislacao/rtac/pdf/RTAC001808.pdf).

pretendida deverá ser realizada por meio de licitação do tipo Pregão Eletrônico, como é de praxe neste Regional, salvo entendimento superior contrário.

A sugestão da equipe de planejamento, por se tratar de fornecimento de equipamento, é pela contratação por licitação via pregão. Por conta de possibilidade de contingenciamento orçamentário indicamos a modalidade de registro de preços.

O DECRETO Nº 7.174, DE 12 DE MAIO DE 2010 que regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União deve ser aplicado nesta aquisição por se tratar de bem de informática.

A ressalva que a equipe aponta é em relação ao artigo 3º, item II que versa sobre a necessidade de exigências, na fase de habilitação, de certificações emitidas por instituições públicas ou privadas credenciadas pelo Instituto Nacional de Metrologia, Normalização e Qualidade Industrial (Inmetro), que atestem, conforme regulamentação específica, a adequação à segurança para o usuário e instalações, compatibilidade eletromagnética e consumo de energia.

Tal exigência inviabiliza e restringe a competição deste certame, vez que a certificação para este tipo de produto, segundo o próprio INMETRO, é voluntária, conforme Portaria Inmetro n.º 170 de 10/04/2012.

(fonte:http://www.inmetro.gov.br/legislacao/rtac/pdf/RTAC001808.pdf).

2.12 Adequação do Ambiente (Art. 18, § 3º, II, k)

Para utilização do objeto pretendido é necessário dispor de infraestrutura física para a instalação de firewalls, situação essa já existente no âmbito do TRE/AL, salvo o surgimento de demanda muito particular e além da previsibilidade.

2.13 Conformidade Técnica e Legal (Art. 18, § 3º, II, l)

1. **CONFORMIDADE**

1. O Fabricante deve comprovar participação no MAPP da Microsoft;
2. A tecnologia deve possuir pelo menos uma certificação da ICSA Labs, ICSA Firewall ou Antivirus;
3. O fabricante da solução deverá ser avaliado pela NSS Labs (Network Security Services) no desempenho do Next Generation Firewall Comparative Analysis mais recente, estando no "Security Value Map" acima de 90% (noventa por cento) da avaliação de segurança efetiva.
4. No momento da entrega dos equipamentos a proponente vencedora deverá fornecer declaração do(s) fabricante(s), em papel timbrado com firma reconhecida, dos produtos ofertados, declarando que a proponente possui credenciamento do mesmo para a implantação e suporte técnico de seus produtos;

2. **COMPATIBILIDADE**
   1. É exigida total compatibilidade do equipamento ofertado com a plataforma de gerenciamento e de relatórios Sonicwall Global Managment Systems (GMS), em pleno uso por este Tribunal;
   2. Caso a licitante não cote produto da marca Sonicwall, deverá apresentar declaração da mesma que indique que o produto ofertado tem total compatibilidade com o Sonicwall GMS.

2.14 Obrigações do Contratante (Art. 18, § 3º, II, m)

1. Efetuar o pagamento à Contratada, após o recebimento definitivo;

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;

3. Manter arquivo, junto ao processo administrativo ao qual está vinculado o presente termo, toda a documentação referente ao mesmo;

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

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

2.15 Obrigações da Contratada (Art. 18, § 3º, II, m)

As obrigações abaixo são aplicáveis ao objeto a ser contratado.

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;
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;
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;
4. Comunicar formal e imediatamente ao Gestor ou Responsável Técnico da Administração sobre mudanças nos dados para contato com a Central de Atendimento;
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;
6. 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;
7. 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. Comunicar ao Gestor ou Responsável Técnico, formal e imediatamente, todas as ocorrências anormais e/ou que possam comprometer a execução do objeto;

9. 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;
10. Cumprir e garantir que seus profissionais estejam cientes, aderentes e obedeçam rigorosamente às normas e aos procedimentos estabelecidos na Política de Segurança da Informação do TRE/AL;
11. Responsabilizar-se pela conservação dos ambientes onde desempenhe as atividades necessárias para prestar a garantia on-site.
12. 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.

DETALHAMENTO DO OBJETO (Art. 18, § 3º, III)

3.1 Descrição do Objeto

Especificações do Item 01

Firewalls de Pequeno Porte

1. **CARACTERISTICAS GERAIS**
    1. Os produtos de hardware ofertados devem ser novos, nunca terem sido utilizados e não terem sido descontinuados, ou seja, devem constar na linha atual de comercialização e suporte do fabricante;
    2. Todos os componentes de hardware da solução deverão ser de um único fabricante ou em regime de OEM não sendo permitida a integração de itens não homologados (ex.: memórias, disco rígido, unidades óptica) de terceiros que venha a ocasionar perda parcial ou total da garantia ou qualquer ônus financeiro adicional durante a vigência da garantia;
    3. Todas as partes e peças necessárias para operacionalização e compatibilização do conjunto deverão ser fornecidas pelo fornecedor/fabricante;
    4. O fabricante dos equipamentos deverá prover em seu site da internet todas as atualizações de drivers e softwares opcionais que por ventura acompanhem os mesmos, essas devem ser disponibilizadas em suas versões mais recentes no intuito de que os equipamentos estejam sempre atualizados com as versões mais recentes de softwares e drivers para os mesmos;
    5. Todos os equipamentos ofertados devem do mesmo fabricante e modelo;
    6. As especificações técnicas apresentadas neste documento são mínimas, sendo aceitos equipamentos com características superiores;
    7. É obrigatória a comprovação técnica de todas as características exigidas para os equipamentos e softwares aqui solicitados, independente da descrição da proposta do fornecedor, através de documentos que sejam de domínio público cuja origem seja exclusivamente do fabricante dos produtos, como catálogos, manuais, ficha de especificação técnica, informações obtidas em sites oficiais do fabricante através da internet, indicando as respectivas URL (Uniform Resource Locator). A simples repetição das especificações do termo de referência sem a devida comprovação acarretará na desclassificação da empresa proponente;
    8. A solução deverá utilizar a tecnologia de firewall Stateful Packet Inspection com Deep Packet Inspection (suportar a inspeção da área de dados do pacote) para filtragem de tráfego IP.
    9. Os produtos ofertados deverão vir acompanhados de todos os cabos e acessórios necessários à completa instalação e operação dos mesmos;
    10. Os produtos ofertados deverão vir acompanhados de documentação impressa ou em mídia DVD/CD ou via download, em idioma português ou inglês, contendo orientações para configuração e operação do produto fornecido;
    11. O prazo de entrega dos produtos (hardware e software) deverá ser de, no máximo, 60 (sessenta) dias corridos após o recebimento da nota de empenho;
    12. Em appliance formato desktop , com possibilidade de instalação em kit de montagem em rack de 19”.
    13. Não serão permitidas soluções baseadas em sistemas operacionais abertos como Free BSD, Debian ou mesmo Linux.
    14. O equipamento deverá ser baseado em hardware desenvolvido com está finalidade, ou seja, de um firewall não sendo baseado em plataforma X86 ou equivalente.
    15. Mínimo de 512MB de memória RAM para maior confiabilidade do sistema.
    16. Sistema Operacional do Tipo “Harderizado” não serão aceitos. Apenas os que forem armazenados em memória flash.

17. Fonte de alimentação com operação automática entre 110/220V.
18. Suportar 5 interfaces 10/100/1000 Gbe. Todas operando em modo autosense e em modo half/full duplex, com inversão automática de polaridade configuráveis pelo administrador do firewall para atendendo os segmentos de segurança e rede para:
    1. Segmento WAN , ou externo.
    2. Segmento WAN, secundário com possibilidade de ativação de recurso para redundância de WAN com balanceamento de carga e WAN Failover por aplicação. O equipamento deverá suportar no mínimo balanceamento de 4 links utilizando diferentes métricas pré-definidas pelo sistema.
    3. Segmento LAN ou rede interna.
    4. Segmento LAN ou rede interna podendo ser configurado como DMZ (Zona desmilitarizada)
    5. Segmento LAN ou rede interna ou Porta de sincronismo para funcionamento em alta disponibilidade
    6. Segmento ou Zona dedicada para controle de dispositivos Wireless dedicado com controle e configuração destes dispositivos.
19. Performance de Firewall SPI (Stateful Packet Inspection) igual ou superior a 300 Mbps.
20. Performance para inspeção de Anti-Malware integrado no mesmo appliance: 50 Mbps ou superior
21. Não serão permitidas soluções baseadas em redirecionamento de tráfego para dispositivos externos ao appliance para analise de arquivos ou pacotes de dados. A atualização das assinaturas deverá ocorrer de forma automática sem há necessidade de intervenção humana.
22. A solução de Gateway Antivírus deverá suportar analise de pelo menos os protocolos, CIFS, NETBIOS, HTTP, FTP, IMAP, SMTP e POP3.
23. Performance de IPS de 100 Mbps ou superior
24. Não serão permitidas soluções baseadas em redirecionamento de tráfego para dispositivos externos ao appliance para analise de arquivos ou pacotes de dados.
25. A atualização das assinaturas deverá ocorrer de forma automática sem há necessidade de intervenção humana.
26. Performance de todos os serviços ativos UTM (Gateway Antivírus, Gateway Anti Spyware, IDS, IPS e Filtro de Conteúdo) deverá ser de 50 Mbps ou superior. Caso o fornecedor não possa comprovar este item em documentações públicas, o mesmo poderá comprovado através de testes em bancada com gerador de pacotes.
27. Os Throughputs devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, o fornecedor será considerado inabilitados. Todos os custos oriundos do teste de bancada serão por conta do fornecedor;
28. Capacidade mínima de conexões suportadas em modo firewall deverá ser de no mínimo ou superior 10.000 Mil conexões.
29. Capacidade mínima de conexões suportadas em modo DPI (analise produnda de pacotes com os serviços IPS, Anti-Malware (Anti-Virus e Anti-Spyware) deverá ser de no mínimo ou superior a 10.000 Mil de conexões.
30. Suportar no mínimo 1.800 novas conexões por segundo.
31. Suportar no mínimo 25 interfaces de vlan (802.1q) suportando a definição de seus endereços IP através da interface gráfica;
32. O equipamento deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL onde o mesmo deverá ser descriptografado de forma transparente a aplicação, verificado possíveis ameaças e então re-criptografado enviado juntamente ao seu destino caso este não contenha ame ameaças ou vulnerabilidades. Sua performance mínima para esta funcionalidade deverá ser de 15 Mbps.
33. Performance de VPN IPSEC (3DES & AES 256) deverá ser de 100 Mbps ou superior.

2. **FUNCIONALIDADES DE FIREWALL**
    1. Possibilitar o controle do tráfego para os protocolos TCP, UDP, ICMP e serviços como FTP, DNS, P2P entre outros, baseados nos endereços de origem e destino;
    2. Possibilitar o controle sobre aplicações de forma granular com criação de políticas sobre o fluxo de dados de entrada, saída ou ambos e;
    3. Devem ser aplicados por usuário e por grupo;
    4. Associado sua ação políticas de horários e dias da semana;
    5. Podem ser associados a endereçamento IP baseados em sub-redes;
    6. Permitindo a restrição de arquivos por sua extensão e bloqueio de anexos através de protocolos SMTP e POP3 baseado em seus nomes ou tipos mime.
    7. Permitir a filtragem de e-mails pelo seu conteúdo, através da definição de palavras-chave e a sua forma de pesquisa;
    8. Prover matriz de horários que possibilite o bloqueio de serviços com granularidade baseada em hora, minutos, dia, dias da semana, mês e ano que a ação deverá ser tomada.
    9. O appliance deve permitir a utilização de políticas de segurança associadas as políticas Anti Malware, IPS/IDS e filtro de Conteúdo em diferentes segmentos e diferentes combinações podendo ser aplicadas inclusive em sub-interfaces estruturadas em Vlans, por sua vez associadas a diferentes zonas de seguranças.
    10. Possuir flexibilidade para liberar aplicações da inspeção profunda de pacotes, ou seja, excluir a aplicação da checagem de recursos como Anti Malwares, IPS entre outros.

11. Possibilitar o controle do tráfego para os protocolos GRE, H323 Full v1-5, suporte a tecnologia a gatekeeper, SIP e IGMP baseados nos endereços origem e destino da comunicação,
12. Controle e gerenciamento de banda para a tecnologia VoIP sobre diferentes segmentos de rede/segurança com inspeção profunda de segurança sobre este serviço.
13. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deve se originar;
14. Prover mecanismos de proteção contra ataques baseados em “DNS Rebinding” protegendo contra códigos embutidos em páginas Web com base em JavaScript, Flash e base Java com “malwares”. O recurso deverá prevenir ataques e analises aos seguintes endereços:
    1. Node-local address 127.0.0.1
    2. Link-local address 169.254.0.0/24
    3. Multicast address 224.0.0.0/24
    4. Host que pertence há alguma das sub-nets conectadas a: LAN, DMZ ou WLAN.
    5. Prover servidor DHCP Interno suportando múltiplos escopos de endereçamento para a mesma interface e a funcionalidade de DHCP Relay;
    6. Prover a capacidade de encaminhamento de pacotes UDPs multicast/broadcast entre diferentes interfaces e zonas de segurança como como IP Helper suportando os protocolos e portas:
    7. Time service—UDP porta 37
    8. DNS—UDP porta 53
    9. DHCP—UDP portas 67 e 68
    10. Net-Bios DNS—UDP porta 137
    11. Net-Bios Datagram—UDP porta 138
    12. Wake On LAN—UDP porta 7 e 9
    13. mDNS—UDP porta 5353
15. Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, Real Áudio, Real Vídeo, SIP, RTSP e H323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro;
16. Implementar mecanismo de sincronismo de horário através do protocolo NTP. Para tanto o appliance deve realizar a pesquisa em pelo menos 03 servidores NTP distintos, com a configuração do tempo do intervalo de pesquisa;
17. Prover mecanismo de conversão de endereços (NAT), de forma a possibilitar que uma rede com endereços reservados acesse a Internet a partir de um único endereço IP e possibilitar também um mapeamento 1-1 de forma a permitir com que servidores internos com endereços reservados sejam acessados externamente através de endereços válidos;
18. Permitir, sobre o recurso de NAT, o balanceamento interno de servidores e suas aplicações sem a necessidade de inserção de um equipamento como switches de que atuam entre as camadas 4 (quatro) e 7 (sete) do modelo ISO/OSI.
19. Possuir mecanismo que permita que a conversão de endereços (NAT) seja feita de forma dependente do destino de uma comunicação, possibilitando que uma máquina, ou grupo de máquinas, tenham seus endereços convertidos para endereços diferentes de acordo com o endereço destino;
20. Possuir mecanismo que permita conversão de portas (PAT);
21. Possuir gerenciamento de tráfego de entrada ou saida, por serviços, endereços IP e regra de firewall, permitindo definir banda mínima garantida e máxima permitida em porcentagem (%) para cada regra definida.
22. Possuir controle de número máximo de sessões TCP, previnindo a exaustão de recursos do appliance e permitindo a definição de um percentual do número total de sessões disponíveis que podem ser utilizadas para uma determinada conexão definida por regra de acesso.
23. Implementar 802.1p e classe de serviços CoS (Class of Service) de DSCP (Differentiated Services Code Points);
24. Permitir remarcação de pacotes utilizando TOS e/ou DSCP;
25. Possuir roteamento RIP, OSPF e BGP, com configuração pela interface gráfica;
26. Possuir suporte ao protocolo SNMP versões 2 e 3;
27. Possui suporte a log via syslog;
28. Possuir mecanismo para possibilitar a aplicação de correções e atualizações para o firewall remotamente através da interface gráfica;
29. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall.
30. Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em um dado momento;
31. Permitir a visualização de estatísticas do uso de CPU do appliance o através da interface gráfica remota em tempo real;

3. **PREVENÇÃO DE INTRUSÃO**
    1. Possuir Mecanismo de IPS / IDS, com suporte a pelo menos 3.000 assinaturas de ataques completamente integrados ao Firewall;
    2. O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;
    3. Possuir tecnologia de detecção baseada em assinatura;
    4. Possuir capacidade de remontagem de pacotes para identificação de ataques;
    5. Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque. Exemplo: agrupar todas as assinaturas relacionadas à webserver para que seja usado para proteção específica de Servidores Web;
    6. 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.
    7. Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos sem intervenção do administrador
    8. Reconhecimento de padrões;
    9. Análise de protocolos;
    10. Detecção de anomalias;
    11. Detecção de ataques de RPC (Remote procedure call);
    12. Proteção contra ataques DNS (Domain Name System);
    13. Proteção contra ataques de ICMP (Internet Control Message Protocol);
    14. Suportar reconhecimento de ataques de DDoS, reconnaissance, exploits e evasion;
4. **FILTRO DE CONTEÚDO**
    1. Possuir base contendo no mínimo 20 milhões de sites internet web já registrados e classificados com atualização automática;
    2. Suporte a filtragem para, no mínimo, 56 categorias e com, pelo menos, as seguintes categorias: violência, nudismo, roupas intimas/banho, pornografia, armas, ódio / racismo, cultos / ocultismo,drogas / drogas ilegais, crimes / comportamento ilegal, educação sexual, jogos, álcool / tabagismo, conteúdo adulto, conteúdo questionável, artes e entretenimento, bancos / e-trading, chat, negócios e economia, tecnologia de computadores e Internet, e-mail pessoal, jogos de azar , hacking, humor, busca de empregos, newsgroups, encontros pessoais, restaurantes / jantar, portais de busca, shopping e portais de compras, MP3, download de software, viagens e WEB hosting;
    3. Capacidade de submissão de novos sites através de portal web ou suporte do Fabricante;
    4. Implementar filtro de conteúdo transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes.
    5. O administrador poderá adicionar filtros por palavra-chave de modo específico;
    6. A política de Filtros de conteúdo deverá ser baseada em horário do dia e dia da semana.
    7. Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente para o controle das políticas de Filtro de Conteúdo sem a necessidade de uma nova autenticação.
    8. Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas, assim como, lista negra;
    9. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
    10. Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem;
    11. Deverá permitir o bloqueio Web através de senha pré configura pelo administrador
    12. Deverá permitir criar política de confirmação de acesso
    13. Deverá bloquear sites embarcados dentro outro sites como por exemplo translate.google.com.br
    14. Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança interna;
    15. Permitir a criação de pelo menos 5 categorias personalizadas;
    16. 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, activeX através de base de URL própria atualizável;
5. **CONTROLE DE APLICAÇÕES**
    1. Deverá reconhecer no mínimo 1.500 aplicações;
    2. Capacidade para realizar filtragens/inspeções dentro de portas TCP conhecidas por exemplo porta 80 http, buscando por aplicações que potencialmente expõe o ambiente como: P2P, Kazaa, Morpheus, BitTorrent ou messengers
    3. Controlar o uso dos serviços de Instant Messengers como MSN, YAHOO, Google Talk, ICQ, de acordo com o perfil de cada usuário ou grupo de usuários, de modo a definir, para cada perfil, se ele pode ou não realizar download e/ou upload de arquivos, limitar as extensões dos arquivos que podem ser enviados/recebidos e permissões e bloqueio de sua utilização baseados em horários pré-determinados pelo administrador será obrigatório para este item.

4. Deverá controlar software FreeProxy tais como ToR, Ultrasurf, Freegate,etc.
5. Deverá permitir a criação de regras para acesso/bloqueio por subrede de origem e destino;
6. Funcionalidade de Controle de Banda (QoS)
7. 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 e gerência de congestionamento;
8. Limitar individualmente a banda utilizada por aplicação
9. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
10. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;
11. Deverá controlar (limitar) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;
12. Deverá controlar (limitar) individualmente a banda utilizada por subrede de origem e destino;
13. Deverá controlar (limitar) individualmente a banda utilizada por endereço IP de origem e destino.

6. **VPN**
   1. Suportar no mínimo 10 túneis VPN IPSEC do tipo site-to-site já licenciadas.
   2. Suportar no mínimo 1 túneis VPN IPSEC do tipo client-to-site já licenciadas podendo suportar no futuro, baseado na aquisição de licenciamento, 5 túneis.
   3. Suportar no mínimo 1 conexões clientes do tipo SSL sem custo e 10 licenças/conexões futuras baseadas em licenciamento adicional.
   4. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.
   5. Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por Pré-Shared Key, Certificados digitais e XAUTH client authentication;
   6. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário;
   7. Permitir que seja criado politicas de roteamentos estáticos utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego sendo este visto pela regra de roteamento, como uma interface simples de rede para encaminhamento do tráfego.
   8. Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet;
7. **AUTENTICAÇÃO**
   1. Permitir a utilização de LDAP, AD e RADIUS;
   2. Permitir o cadastro manual dos usuários e grupos diretamente na interface de gerencia remota do Firewall, caso onde se dispensa um autenticador remoto para o mesmo;
   3. Permitir a integração com qualquer autoridade certificadora emissora de certificados X509 que seguir o padrão de PKI descrito na RFC 2459, inclusive verificando as CRLs emitidas periodicamente pelas autoridades, que devem ser obtidas automaticamente pelo firewall via protocolos HTTP e LDAP;
   4. Permitir o controle de acesso por usuário, para plataformas Windows Me, NT, 2000, 2000, XP, Windows 7 , Windows 8 e Windows 10 de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado;
   5. Permitir a restrição de atribuição de perfil de acesso a usuário ou grupo independente ao endereço IP da máquina que o usuário esteja utilizando.
   6. Suportar recurso de autenticação única para todo o ambiente de rede, ou seja, utilizando a plataforma de autenticação atual que pode ser de LDAP ou AD; o perfil de cada usuário deverá ser obtido automaticamente através de regras no Firewall DPI (Deep Packet Inspection) sem a necessidade de uma nova autenticação como por exemplo, para os serviços de navegação a Internet atuando assim de forma toda transparente ao usuário. Serviços como HTTP, HTTPS devem apenas consultar uma base de dados de usuários e grupos de servidores 2008/2012 com AD;
8. **ADMINISTRAÇÃO**
   1. Suportar no mínimo 250 usuários autenticados com serviços ativos e identificados passando por este dispositivo de segurança em um único dispositivo de segurança. Políticas baseadas por grupos de usuários deverão ser suportadas por este dispositivo. Está comprovação poderá ser exigida em testes sobe o ambiente de produção com o fornecimento do produto para comprovação deste e demais itens.
   2. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o firewall, cada um responsável por determinadas tarefas da administração;
   3. Fornecer gerência remota, com interface gráfica nativa;
   4. Fornecer interface gráfica para no mínimo 3 usuários;
   5. A interface gráfica deverá possuir assistentes para facilitar a configuração inicial e a realização das tarefas mais comuns na administração do firewall, incluindo a configuração de VPN IPSECs, NAT, perfis de acesso e regras de filtragem;

6. Possuir mecanismo que permita a realização de cópias de segurança (backups) e sua posterior restauração remotamente, através da interface gráfica, sem necessidade de se reinicializar o sistema;
7. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall e a remoção de qualquer uma destas sessões ou conexões;
8. Permitir a visualização de estatísticas do uso de CPU, memória da máquina onde o firewall está rodando e tráfego de rede em todas as interfaces do Firewall através da interface gráfica remota, em tempo real e em forma tabular e gráfica;
9. Permitir a conexão simultânea de vários administradores, sendo um deles com poderes de alteração de configurações e os demais apenas de visualização das mesmas. Permitir que o segundo ao se conectar possa enviar uma mensagem ao primeiro através da interface de administração.
10. Possibilitar o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo;
11. Possuir interface orientada a linha de comando para a administração do firewall a partir do console ou conexão SSH sendo está múltiplas sessões simultâneas.
12. Possuir mecanismo que permita inspecionar o tráfego de rede em tempo real (sniffer) via interface gráfica, podendo opcionalmente exportar os dados visualizados para arquivo formato PCAP e permitindo a filtragem dos pacotes por protocolo, endereço IP origem e/ou destino e porta IP origem e/ou destino, usando uma linguagem textual;
13. Permitir a visualização do tráfego de rede em tempo real tanto nas interfaces de rede do Firewall quando nos pontos internos do mesmo: anterior e posterior à filtragem de pacotes, onde o efeito do NAT (tradução de endereços) é eliminado;
14. Possuir sistema de respostas automáticas que possibilite alertar imediatamente o administrador através de e-mails, janelas de alerta na interface gráfica, execução de programas e envio de Traps SNMP;

9. **RELATÓRIO**
    1. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas.
    2. Possibilitar a geração de pelo menos os seguintes tipos de relatório com cruzamento de informações, mostrados em formato HTML: máquinas acessadas X serviços bloqueados, usuários X URLs acessadas, usuários X categorias Web bloqueadas (em caso de utilização de um filtro de conteúdo Web);
    3. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (em caso de existência de um filtro de conteúdo Web), maiores emissores e receptores de e-mail;
    4. Permitir o envio dos relatórios, através de email para usuários prédefinidos;
    5. Possuir relatórios prédefinidos na solução e permitir a criação de relatórios customizados;
    6. Possibilitar a geração dos relatórios sob demanda e através de agendamento diário, semanal e mensal. No caso de agendamento, os relatórios deverão ser publicados de forma automática
    7. Disponibilizar download dos relatórios gerados;
10. **GARANTIA, SUPORTE E LICENCIAMENTO**
    1. O licenciamento para todos os serviços de Next Generation Firewall deverá ser de 36 meses.
    2. A garantia deverá ser de 36 meses.
    3. Deve contemplar suporte do Fabricante pelo período vigente, com no mínimo, as seguintes características:
        1. O suporte do fabricante deve ter um sistema de abertura de chamados para acompanhamento – funcionando 24 horas por dia e 7 dias por semana
        2. Deve assegurar a utilização de novas versões de software da solução sem ônus a Licitante, sempre que esta estiver disponível a qualquer cliente
        3. Deve permitir o acesso à base de conhecimento da solução.
11. **CONFORMIDADE**
    1. O Fabricante deve comprovar participação no MAPP da Microsoft;
    2. A tecnologia deve possuir pelo menos uma certificação da ICSA Labs, ICSA Firewall ou Antivirus;
    3. O fabricante da solução deverá ser avaliado pela NSS Labs (Network Security Services) no desempenho do Next Generation Firewall Comparative Analysis mais recente, estando no “Security Value Map” acima de 90% (noventa por cento) da avaliação de segurança efetiva.
    4. No momento da entrega dos equipamentos a proponente vencedora deverá fornecer declaração do(s) fabricante(s), em papel timbrado com firma reconhecida, dos produtos ofertados, declarando que a proponente possui credenciamento do mesmo para a implantação e suporte técnico de seus produtos;
12. **COMPATIBILIDADE**

1. É exigida total compatibilidade do equipamento ofertado com a plataforma de gerenciamento e de relatórios Sonicwall Global Managment Systems (GMS), em pleno uso por este Tribunal;
2. Caso a licitante não cote produto da marca Sonicwall, deverá apresentar declaração da mesma que indique que o produto ofertado tem total compatibilidade com o Sonicwall GMS.

3.2 Forma de Execução e de Gestão do Contrato (Art. 18, § 3º, III, a)

A execução do objeto pressupõe a existência dos seguintes papéis e responsabilidades (Art. 18, § 3º, III, a, 1):

1. Patrocinador da Contratação: é o titular da área demandante, responsável por representar os interesses do órgão no contexto da Contratação, pela aprovação da necessidade e, por fim, pela negociação das ações necessárias para que os objetivos sejam alcançados;
2. Gestor do Contrato (art. 3º, IV, da Resolução TRE/AL nº 15.787/2017): servidor designado para coordenar e comandar o processo da fiscalização da execução contratual. Na forma do Art. 17 da mesma Resolução, o gestor do contrato responsabiliza-se pela condução da gestão e fiscalização do contrato, nos termos do Art. 67, da Lei nº 8.666/93.
3. Fiscal do Contrato (art. 3º, VI, da Resolução TRE/AL nº 15.787/2017): servidor designado para auxiliar o gestor do contrato quanto à fiscalização do objeto do contrato. Neste sentido, indicado pela respectiva autoridade competente para fiscalizar o Contrato quanto aos aspectos técnicos da solução.

Dinâmica da Execução (Art. 18, § 3º, III, a, 2):

1. Os equipamentos deverão ser entregues no Almoxarifado do TRE/AL, nos quantitativos indicados no pedido de fornecimento;
2. A garantia dos equipamentos deve obedecer o detalhamento técnico feito e terá seu tempo contado por cada fornecimento individualmente;
3. Entende-se como garantia aquela prestada pelo próprio fabricante ou por rede credenciada pelo fabricante do(s) referido(s) equipamento(s);
4. O pagamento será realizado individualmente para cada nota fiscal apresentada, após emissão do aceite definitivo pela unidade competente do TRE/AL;
5. Os equipamentos deverão ser novos, não recondicionados, de primeiro uso e não deverão conter marcas, amassados, arranhões ou outros problemas e, ainda, serem entregues em pleno estado de funcionamento;
6. Os equipamentos deverão atender rigorosamente a todas as especificações técnicas contidas neste Termo de Referência e em seus Anexos;
7. Os equipamentos deverão vir acompanhados de todos os acessórios necessários para o seu pleno estado de funcionamento, como cabos, drivers, mídias e outros, os quais só serão recebidos juntamente com os respectivos equipamentos. Este item se aplica tanto para a entrega dos equipamentos quanto para substituições durante o período de garantia;
8. Ao TRE é reservado o direito de efetuar conexões dos equipamentos a outros, bem como adicionar demais acessórios compatíveis tecnicamente, sem que isso constitua motivo para a Contratada se desobrigar da garantia, desde que tal fato não implique danos materiais ou técnicos aos equipamentos e acessórios, hipótese que deverá ser devidamente comprovada;
9. Ao TRE/AL é reservado o direito de efetuar diligência, a qualquer tempo, quanto aos documentos exigidos neste Termo de Referência e em seus Anexos.

Recebimento do Objeto:

1. O Tribunal designará Comissão para realizar o recebimento provisório, que só será emitido se os equipamentos estiverem de acordo com as especificações técnicas;
2. Após a entrega, os equipamentos serão submetidos à avaliação e homologação pelos responsáveis técnicos do Tribunal;
3. O exame para comprovação das características técnicas consistirá em avaliações e testes não-destrutivos, por amostragem realizados em duas etapas:
    a. Primeira: inspeção visual de todos os equipamentos entregues;
    b. Segunda: testes funcionais de configuração e desempenho, em, no mínimo, 10% (dez por cento) e não menos do que 01 (um) dos equipamentos recebidos. O Tribunal poderá, a seu critério, executar os testes nos demais equipamentos, dentro de um critério de razoabilidade, podendo chegar a 100% dos quantitativos, mas dentro de um prazo máximo de 30 (trinta) dias corridos e contados de cada lote de equipamentos.
4. As especificações serão avaliadas também por meio de documentos técnicos que acompanham os equipamentos, informações fornecidas pela Contratada e disponível no sítio do fabricante.
5. A comissão do Tribunal deverá, após a comprovação do perfeito funcionamento dos equipamentos e adequação às especificações técnicas, emitir e assinar o Termo de Recebimento Definitivo.

Instrumentos Formais de Solicitação do(s) Bens e/ou Serviço(s) (Art. 18, § 3º, III, a, 3):

1. A Ordem de Fornecimento será o instrumento formal de solicitação dos bens pertencentes ao escopo desta contratação.

Forma de Pagamento (Art. 18, § 3º, III, a, 7)

1. O pagamento será efetuado mediante crédito em conta-corrente do Fornecedor, por ordem bancária, no prazo disposto nos artigos 5º, § 3º, ou 40, XIV, "a", da Lei n. 8.666/93, conforme o caso, quando mantidas as mesmas condições iniciais de habilitação e cumpridos os seguintes requisitos:
    a. Apresentação de nota fiscal de acordo com a legislação vigente à época da emissão (nota fiscaleletrônica, se for o caso), acompanhada da Certidão Negativa de Débito – CND, comprovando regularidade com o INSS; do Certificado de Regularidade do FGTS – CRF, comprovando regularidade com o FGTS; da Certidão Conjunta Negativa de Débitos Relativos a Tributos Federais e à Dívida Ativa da União, expedida pela Secretaria da Receita Federal; e da Certidão Negativa de Débitos Trabalhistas – CNDT, emitida pela Justiça do Trabalho; e da prova de regularidade para com as Fazendas Estadual e Municipal do domicílio ou sede do Fornecedor; e
    b. Inexistência de fato impeditivo para o qual tenha concorrido o Fornecedor.
2. Nenhum pagamento será efetuado à Contratada enquanto pendente de liquidação qualquer obrigação. Esse fato não será gerador de direito a reajustamento de preços ou a atualização monetária.

Direitos de Propriedade Intelectual (Art. 18, § 3º, III, a, 9):

1. Esse requisito não se aplica ao contexto desta contratação, uma vez que o objeto se refere ao fornecimento de equipamentos, cujos direitos autorais do fabricante são resguardados por legislação nacional e internacional.

Penalidades (Art. 18, § 3º, III, a, 11):

1. Com fundamento no artigo 7º da Lei nº 10.520/2002 e, subsidiariamente, nos artigos 86 e 87 da Lei 8.666/1993, a Contratada ficará sujeita, assegurada prévia e ampla defesa, às seguintes penalidades:
    a. Advertência:
        i. A Contratada será notificada formalmente em caso de descumprimento de obrigação contratual e terá que apresentar as devidas justificativas em um prazo de até 5 (cinco) dias úteis após o recebimento da notificação; e
        ii. Caso não haja manifestação dentro desse prazo ou se entenda serem improcedentes as justificativas apresentadas, a Contratada será advertida;
    b. Multa de:
        i. 0,5% por dia, sobre o valor constante da Ordem de Fornecimento, no caso de atraso injustificado na entrega dos equipamentos, limitada a incidência a 20 (vinte) dias corridos;
            1. No caso de atraso injustificado na entrega dos equipamentos por prazo superior a 20 (vinte) dias corridos, com a aceitação pela Administração, será aplicada a multa de 5% sobre o valor da Ordem de Fornecimento; e
            2. No caso de atraso injustificado na entrega dos equipamentos por prazo superior a 20 (vinte) dias corridos, com a não aceitação pela Administração, será aplicada a penalidade 10% sobre o valor da Ordem de Fornecimento, no caso de inexecução total da obrigação, podendo haver, ainda, o cancelamento do registro de preços do Fornecedor;
        ii. 0,5% por dia, sobre o valor do equipamento, no caso de atraso injustificado na solução do chamado de garantia, limitada a incidência 30 (trinta) dias corridos;
            1. No caso de atraso injustificado na solução do chamado de garantia por prazo superior a 30 (trinta) dias corridos, aplica-se adicionalmente, a multa de 1% sobre o valor da Ordem de Fornecimento; e
            2. A multa por atraso relacionada ao item anterior será auferida por Ordem de Fornecimento e aplicada somente uma única vez a cada mês, independente da quantidade de equipamentos sem solução.
        iii. 5% sobre o valor constante da Ordem de Fornecimento, no caso de inexecução parcial da obrigação assumida;
        iv. 10% sobre o valor da Ordem de Fornecimento, no caso de inexecução total da obrigação, podendo haver, ainda, o cancelamento do registro de preços do Fornecedor;

v. 5% sobre o valor global estimado da Ata de Ata de Registro de Preços, na hipótese de recusa em assinar a Ata ou o instrumento do contrato, ou retirar a Ordem de Fornecimento.

c. Impedimento de licitar e contratar com a União e descredenciamento do SICAF pelo prazo de até 5 (cinco) anos, sem prejuízo das demais penalidades legais; e

d. Declaração de inidoneidade para licitar ou contratar com a Administração Pública.

2. O cometimento reiterado de atrasos injustificados dos prazos previstos para entrega/solução do chamado de garantia dos equipamentos poderá resultar no cancelamento do registro de preços com a Contratada.
3. As sanções previstas nos itens "1.a", “1.c” e “1.d” do item 1 poderão ser aplicadas, cumulativamente ou não, à pena de multa.
4. O valor da multa, aplicada após o regular processo administrativo, será descontado de pagamentos eventualmente devidos à contratada ou cobrado judicialmente;
5. Excepcionalmente, ad cautelam, a Administração poderá efetuar a retenção do valor presumido da multa, antes da instauração do regular procedimento administrativo.

.

4. Requisitos Técnicos (Art. 18, § 3º, IV)

Garantia mínima de 03 (três) anos.

Estar comprovadamente ainda em produção.

Conformidade com o presente Termo de Referência.

5. Modelos (templates) propostos a serem utilizados na contratação (Art. 18, § 3º, III, V)

Proc. SEI Principal nº XXXXXXXXX

Pregão Eletrônico nº XX/YYYY – TRE/AL

Ata de Registro de Preços TRE/AL nº XX/YYYY

Fornecedor: AAAAAAAAAAA. - CNPJ 00.000.000/0000-00

ORDEM DE FORNECIMENTO Nº XXX/20YY – STI

Solicito, com base na Ata de Registro de Preços relativa ao Pregão Eletrônico suprarreferido, celebrada entre este Tribunal e essa Empresa, o fornecimento abaixo discriminado:

Item da Ata	Descrição	Qtd. Solicitada	Valor Unitário (R$)	Valor Total (R$)

			TOTAL:	

Recursos Orçamentários: As despesas decorrentes da prestação dos serviços pretendido serão cobertas com recursos de MATERIAL PERMANENTE DE TI.

Prazo de Entrega: No máximo de XX (XXXXXXX) dias corridos após o recebimento da autorização de fornecimento, nota de empenho ou instrumento formal e equivalente, conforme contrato.

Valor Total: R$ XX.XXX,XX (XXXXXX reais e XXXXXXXa centavos).

RESUMO DE STATUS DA ATA

QUANTITATIVO TOTAL REGISTRADO:	
Quantitativo executado via Ordem de Fornecimento nº 001/20YY	
Quantitativo executado via Ordem de Fornecimento nº 002/20YY	
SALDO ATA:	

Gestor da Ata - Portaria TRE/AL nº XX/XXXX

Maceió, 03 de abril de 2020.

Documento assinado eletronicamente por **DANIEL MACÊDO DE CARVALHO SOUTO**, **Coordenador**, em 03/04/2020, às 15:55, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tre-al.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0679224** e o código CRC **F9F3D885**.