PODER JUDICIÁRIO DE ALAGOAS

ANEXO VIII
TERMO DE REFERÊNCIA

Controle de revisão		
Data da revisão	Executor	Atualização
25/10/2016	DIATI	Criação
28/11/2016	DIATI	Otimização
01/02/2017	DIATI	Adição do tópico “Topologia da Solução”; otimização das especificações comuns a todos os lotes; adição de requisitos da qualificação técnica.

1. OBJETO:

O objeto deste projeto básico é estabelecer requisitos mínimos visando **registro de preço** para contratação de empresas especializadas na prestação de serviço de LINKS DE ACESSO A INTERNET SIMÉTRICOS, incluindo instalação, configuração, manutenção periódica e serviços de segurança, de acordo com as especificações, quantitativos e observações constantes neste Termo de Referência.

2. JUSTIFICATIVA:

Atualmente o Poder Judiciário de Alagoas possui um link de 100Mb/s que canaliza toda demanda de upload e download da Egrégia Corte ao backbone da internet. É uma contratação realizada no ano de 2012 e tem seu encerramento previsto para agosto de 2017, de maneira que esse fato cria a necessidade, mais do que prioritária, de que se realize nova contratação, mediante procedimento licitatório, para manutenção deste serviço. Esta nova aquisição foi planejada com o foco em atender às novas necessidades do Poder Judiciário, tanto no aspecto de capacidade quanto no de segurança.

Relatórios recentes, providos por ferramentas de monitoramento, evidenciam a necessidade de expansão do link de dados, visto que a taxa de transmissão da contratação vigente está atingindo picos de consumo que ultrapassam limites prudenciais. A progressiva virtualização processual – que atualmente abrange 100% do Estado de Alagoas – somada a recentes e onerosos serviços, do ponto de vista da comunicação de dados, como a videoconferência, confirma uma tendência natural de se recorrer à tecnologia para ofertar uma prestação jurisdicional cada vez mais célere e efetiva. Essas inovações levarão ao previsível e iminente cenário de gradativo esgotamento da banda disponível para download e upload nos próximos meses, causando expressivos gargalos que limitarão serviços importantes do tribunal, sobretudo aos sistemas judiciais. Logo, é essencial que se promova uma nova aquisição de serviço de acesso à internet mais veloz e com recursos de contingência capazes de minimizar os problemas decorrentes de falhas pontuais do serviço contratado.

Os requisitos propostos neste termo de referência estão alinhados com os objetivos de nivelamento de infraestrutura elencados na Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (resolução 211/2015 do CNJ), a qual estabelece diretrizes de nivelamento que devem ser observadas nas contratações de Tecnologia da Informação, e com as diretrizes traçadas no Planejamento Estratégico de TIC 2015-2020 do Poder Judiciário Alagoano. Ambos propõem uma

infraestrutura de comunicação de dados com a internet prestada por 2 provedores distintos, totalizando uma largura de banda que permita o atingimento de 80% de consumo máximo.

É importante destacar, ainda, que a opção por adotar tecnologia anti DDoS em conjunto com o link de internet proporcionará ao Tribunal proteção contra ataques distribuídos de negação de serviço (distributed denial of service). Esse tipo de ataque, conforme amplamente noticiado no segmento, tem crescido de maneira exponencial no Brasil, trazendo graves prejuízos à atividade econômica e à prestação de serviços públicos. Tribunais estaduais, como o de Sergipe[1] e o do Rio de Janeiro[2], já experimentaram significativos períodos de indisponibilidade dos seus serviços de comunicação de dados ofertados à sociedade em decorrência de ação de hackers.

A Internet exerce papel preponderante para que o Tribunal de Justiça do Estado de Alagoas consiga satisfazer, com efetividade, sua missão institucional fornecendo diversos serviços. Vários destes, além de críticos, necessitam de conexões que garantam a alta disponibilidade, pois devem estar em funcionamento permanentemente, durante as 24 (vinte e quatro) horas do dia, 7 (sete) dias da semana, vez que falhas em sua operação impactam diretamente no cumprimento da missão constitucional incumbida a esta corte.

3. ESPECIFICAÇÕES E QUANTIDADES:

3.1. Lotes

3.1.1. LOTE 1

Serviço de ACESSO À INTERNET dedicado e simétrico por meio de infraestrutura física segura redundante, incluindo serviço de segurança perimetral, a ser instalado no datacenter do Tribunal de Justiça do Estado de Alagoas, e proteção contra DoS e DDoS.

PRESTADOR 1			
ITEM	**ESPECIFICAÇÃO**	**UNID.**	**QUANTIDADE**
1	ACESSO À INTERNET dedicado e simétrico, com previsão de velocidade de **300 Mbps,** incluindo instalação, configuração, manutenção periódica.	Mensal	12
2	Serviço de proteção DDoS	Mensal	12
3	Serviço de segurança perimetral	Mensal	12

3.1.2. LOTE 2

Serviço de ACESSO À INTERNET contingencial, dedicado e simétrico, incluindo proteção contra DoS e DDoS.

[1] SUMARES, Paulo. **Anonymous tira sites de Sergipe do ar em protesto contra bloqueio do WhatsApp**. Disponível em: < https://goo.gl/ydFRnc>. Acesso em: 21 nov. 2016.

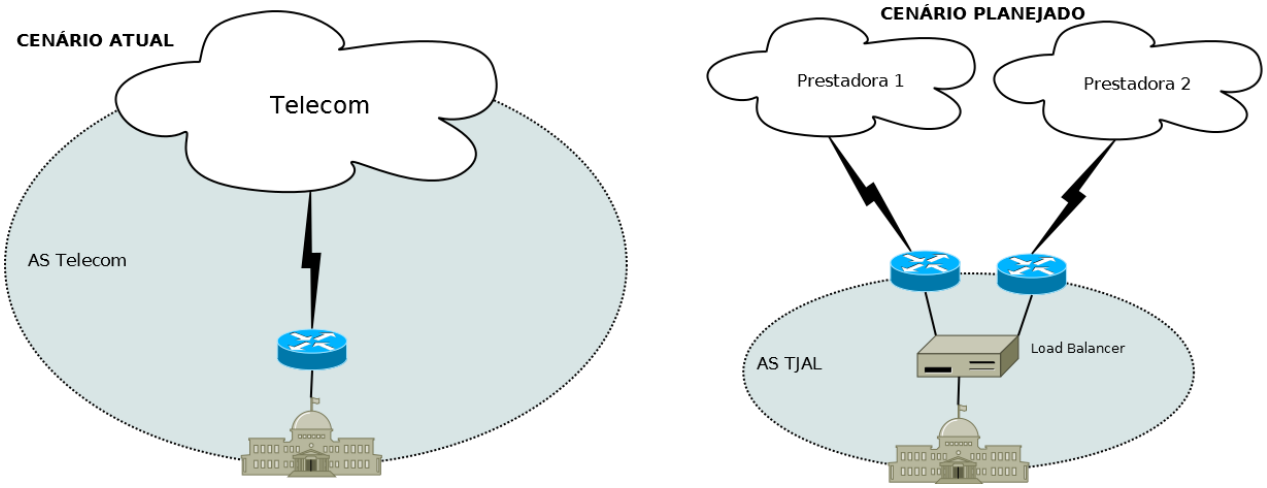
[2] EXAME. **Hackers derrubam página do TJ-RJ após bloqueio do WhatsApp**. Disponível em: <https://goo.gl/aBmzT5>. Acesso em: 21 nov. 2016

PRESTADOR À 2			
ITEM	**ESPECIFICAÇÃO**	**UNID.**	**QUANTIDADE**
1	ACESSO À INTERNET contingencial,	Mensal	
	dedicado e simétrico, com previsão de velocidade de **150 Mbps,** incluindo instalação, configuração, manutenção periódica.		12
2	Serviço de proteção DDoS	Mensal	12

3.1.3. Para o Lote 01 e Lote 02, a Licitante vencedora no Lote 01 não poderá ser a vencedora no Lote 02 e vice-versa.

3.1.4. Os serviços dos Lotes 01 e 02 terão vigência contratual de 12 (doze) meses, prorrogáveis até 60 (sessenta).

3.2. Topologia da solução



3.2.1. Haverá 2 links, fornecidos por prestadoras distintas, que serão convergidos em um appliance concentrador que será responsável pelo recurso de balanceamento de carga e failover. O vencedor do LOTE 1, principal, e o vencedor do LOTE 2, secundário, poderão, conforme necessidade da CONTRATANTE, iniciarem a prestação do serviço em momentos diferentes. Sendo assim, além dos demais componentes necessários para a sustentação do serviço de acesso à internet, o fornecimento e instalação do appliance estará a cargo da PRESTADORA 2.

3.2.2. O appliance concentrador deverá possuir os seguintes requisitos mínimos:

3.2.2.1. Deve otimizar largura de banda de internet.

3.2.2.2. Deve otimizar roteamento para priorizar tráfegos de aplicativos de missão crítica.

3.2.2.3. Deve permitir failover e failback automático de links WAN para segurar continuidade de fluxo de tráfego.

3.2.2.4. Multi-homing para melhorar tempos de resposta e disponibilidade para requisições de entrada.
3.2.2.5. Suporte a múltiplos algoritmos de balanceamento de carga:
3.2.2.5.1. Algoritmo fixo;
3.2.2.5.2. Round-robin;
3.2.2.5.3. Baseado em aplicação;
3.2.2.5.4. Baseado em conexões;
3.2.2.5.5. Baseado em tráfego;
3.2.2.5.6. Baseado em FQDN;
3.2.2.6. Suporte a multi-homing:
3.2.2.6.1. Wan Load Balancing e Fault Tolerance;
3.2.2.6.2. Domínios mútiplos;
3.2.2.6.3. DNS relay;
3.2.2.6.4. Suporte a IPv6;
3.2.2.6.5. IPv4/IPv6 authoritative DNS/DNSSEC
3.2.2.7. Gerenciamento de largura de banda:
3.2.2.7.1. Largura de banda mínima e máxima;
3.2.2.7.2. Por prioridade;
3.2.2.7.3. Por Ip de origem e de destino e aplicação;
3.2.2.7.4. Por agendamento.
3.2.2.8. Deve oferecer suporte aos protocolos de roteamento RIP V1/2 e OSPF.
3.2.2.9. Deve oferecer suporte a PPPoE/DHCP.
3.2.2.10. Deve oferecer suporte a 802.1q VLAN.
3.2.2.11. Deve oferecer suporte a NAT mode / Routing mode.
3.2.2.12. Médotos de Gerenciamento:
3.2.2.12.1. Web Admin (SSL);
3.2.2.12.2. Console (RJ45, RS232 ou SSH);
3.2.2.12.3. SNMP;
3.2.2.12.4. Gerenciamento centralizado para múltiplos dispositivos.
3.2.2.13. Deve suportar um throughput compatível com a totalidade da largura de banda contrata, considerando os 2 lotes.
3.2.2.14. Deve possuir alimentação redundante (Dual power supply).
3.2.2.15. Deve suportar no mínimo 2.000.000 de conexões concorrentes.
3.2.2.16. Deve suportar no mínimo 180.000 conexões por segundo.
3.2.2.17. Deve possuir fonte de alimentação com entrada 110/220 volts AC, com comutação automática de tensão;

3.3. Especificações e exigências comuns a todos os lotes

3.3.1. Deverá ser disponibilizado acesso IP permanente que possibilite a interligação do ambiente da CONTRATANTE à rede mundial de computadores, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, composto de um canal direto com a Internet de uso ilimitado, em conformidade com os prazos definidos no Acordo de Nível de Serviço;

3.3.2. A solução deverá contemplar meios de acessos redundantes, utilizando fibra óptica com encaminhamentos físicos distintos, entre o Datacenter da CONTRATANTE e a estação de distribuição do backbone da rede da CONTRATADA;

3.3.3. Para aceitação do fornecimento, é exigido que os enlaces de fibra óptica redundante sejam fornecidos por encaminhamentos distintos fim a fim, ou seja, desde a estação de distribuição da LICITANTE cada fibra óptica do enlace redundante deve seguir caminhos distintos, por ruas e rotas distintas, chegando até a entrada de Telecom do CONTRATANTE por caminhos distintos,
onde haverá o encontro das fibras ópticas para entrada até o DG de Telecom da CONTRATANTE. Esta garantia deverá ser analisada pela equipe técnica da CONTRATANTE através de fornecimento de projeto de encaminhamentos fornecido pela LICITANTE, como parte das exigências para Qualificação Técnica;

3.3.4. Deverão ser fornecidos, pelo menos, 2 (dois) enlaces de acesso redundantes entre si, em fibra ótica, devendo cada um dos circuitos de comunicação utilizar tecnologia determinística com taxa de transferência que atenda integralmente à velocidade contratada, evitando-se deste modo, a instalação de vários links com taxas de transferências inferiores ao solicitado para se obter a velocidade contratada;

3.3.5. Deverá fornecer cada um dos canais com transmissão full duplex e taxa simétrica, isto é, a mesma capacidade de transmissão para o tráfego de entrada e de saída, simultaneamente;

3.3.6. Na implantação por dupla abordagem a CONTRATADA proverá equipamento automático de chaveamento e os enlaces devem operar em modo ativo todo o tempo;

3.3.7. A CONTRATADA deverá configurar e implantar os canais de comunicação, que interligarão a Unidade da CONTRATANTE à Internet, contemplando todos os insumos necessários à sua plena operacionalização, tais como:

3.3.7.1. circuito de acesso, que interliga a Unidade da CONTRATANTE à Internet;
3.3.7.2. porta de entrada no backbone da CONTRATADA;
3.3.7.3. roteador;
3.3.7.4. equipamento de acesso (modem, SDH, switch, etc.)

3.3.8. O roteador de acesso que compõe os links redundantes da CONTRATADA a ser instalado na infraestrutura da CONTRATANTE deverá possuir no mínimo 02 portas no padrão ethernet 1000 Base-T e deverá permitir sua fixação em rack padrão 19”, devendo vir acompanhado de todos os acessórios originais do fabricante para tal fixação;

3.3.9. Caso seja necessário o fornecimento de modem, o equipamento deverá permitir sua fixação em rack padrão 19”, devendo vir acompanhado de todos os acessórios originais do fabricante para tal fixação;

3.3.10. A taxa de transmissão deverá sempre estar disponível na totalidade do fluxo contratado. A CONTRATADA não poderá, de forma alguma, bloquear, limitar ou filtrar o tráfego de entrada ou de saída dos links contratados, não sendo admitido nenhum tipo de restrição seja por serviço, tipo de arquivo ou protocolo;

3.3.11. A CONTRATADA deve possuir conexões ao backbone nacional e internacional (Europeu e/ou da América do Norte) de no mínimo 15 (quinze) vezes maior que a inicialmente contratada;

3.3.12. Deverá ser fornecido consultas, conforme necessidade da CONTRATANTE, ou acesso via Telnet, SSH ou WEB (http ou https) a um sistema conhecido por “looking-glass” ou outro equivalente, de modo que seja possível consultas de rotas, “as-paths”, neighbors BGP, flaps e dampenings, e

conectividade (ping e traceroute), possuindo informações internas da rede da CONTRATADA e recursos de filtros por expressões regulares;

3.3.13. Tribunal de Justiça do Estado de Alagoas será a CONTRATANTE e gestora técnica dos serviços contratados;

3.3.14. Todo fornecimento e instalação dos materiais e equipamentos necessários à prestação dos serviços pela CONTRATADA, não poderá acarretar ônus adicional à CONTRATANTE, devendo todo o custo de implantação agregar o valor da proposta. Logo, deverão estar inclusos na solução todos os recursos de conectividade, tais como: modems, conversores, roteadores, e outros correlatos, bem como a infraestrutura para instalação dos equipamentos de transmissão necessária à prestação dos serviços;

3.3.15. Os equipamentos fornecidos deverão ser capazes de atender INTEGRALMENTE aos requisitos de qualidade e velocidade do link de comunicação de dados contratado;

3.3.16. Os roteadores integrantes do “Backbone” da prestadora de serviços e os roteadores instalados no Datacenter da CONTRATANTE deverão possuir capacidade de suportar o tráfego com banda completamente ocupada, sem que os limites de 70% de utilização da memória e 70% de utilização da CPU sejam excedidos;

3.3.17. Os recursos de hardware e software dos equipamentos envolvidos devem ser atualizados tecnologicamente, sem ônus para à CONTRATANTE, durante a vigência do contrato;

3.3.18. Sempre que houver lançamento de nova versão estável de sistema operacional e ou firmware que faça correções de segurança dos equipamentos fornecidos, a CONTRATADA deverá providenciar as devidas atualizações com prévia aprovação da CONTRATANTE, sem ônus adicional;

3.3.19. Os equipamentos a serem instalados na infraestrutura da CONTRANTANTE deverão ser acomodados em racks fechados, fornecidos pela CONTRATANTE;

3.3.20. Os equipamentos relacionados com a solução deverão ser instalados e mantidos operacionais, com todos os seus acessórios e documentações;

3.3.21. Os equipamentos devem possuir fonte de alimentação com entrada 110/220 volts AC e com a frequência de 60 Hz, com comutação automática de tensão;

3.3.22. Os roteadores instalados na infraestrutura da CONTRATANTE deverão estar configurados para permitir a configuração remota somente através de SSH v2, ficando por conta da CONTRATADA o fornecimento de todos os recursos necessários à configuração remota;

3.3.23. Todos os links e equipamentos fornecidos pela CONTRATADA, nas suas condições de fabricação, operação, manutenção, configuração, funcionamento, alimentação e instalação, deverão obedecer rigorosamente às normas e recomendações em vigor, elaboradas por órgãos oficiais competentes ou entidades autônomas reconhecidas na área – ABNT (Associação Brasileira de Normas Técnicas) e ANATEL (Agência Nacional de Telecomunicações), e entidades de padrões reconhecidas internacionalmente – ITU-T (International Telecommunication Union), ISO (International Standardization Organization), IEEE (Institute of Electrical and Electronics Engineers), EIA/TIA (Electronics Industry Alliance and Telecommunication Industry Association);

3.3.24. A CONTRATADA deverá fornecer à CONTRATANTE as senhas de acesso, via porta de console e via SSHv2, para cada um dos roteadores instalados, com privilégios somente para operações de leitura – (read only) para os comandos “ping”, “routing” e “trace”. Também deverá ser fornecido

acesso somente de leitura às estatísticas de SNMP (comunidade de leitura ou usuário/senha), além de configurar os roteadores para gerar logs (Syslog – RFC 3164) e/ou traps SNMP para um ou mais endereços IPs a serem definidos pela CONTRATANTE;

3.3.25. Deve ser configurado o envio de mensagens NetFlow ou sFlow para equipamento indicado pela CONTRATANTE;

3.3.26. A rede de energia elétrica, o sistema de aterramento, condicionamento de ar e segurança física dos equipamentos serão de responsabilidade da CONTRATANTE;

3.3.27. A entrega de cada um dos links objeto deste Termo deverá ser através de porta RJ-45 Ethernet (padrão IEEE 802.3 e derivados) e/ou conexão ótica (preferencialmente);

3.3.28. Todos os circuitos e serviços deverão receber uma identificação única, a ser utilizada tanto pela CONTRATANTE como pela CONTRATADA. A nomenclatura a ser utilizada na identificação de cada circuito deverá refletir cada unidade da CONTRATANTE;

3.3.29. Todo conjunto de materiais e equipamentos fornecidos pela CONTRATADA, deverão ser novos e sem uso prévio, e atender as normas do Código de Defesa do Consumidor, não podendo ser reciclados ou recondicionados e nem de fabricação artesanal;

3.3.30. Deverá dispor de reserva técnica de componentes sobressalentes suficientes, caso haja necessidade de substituição;

3.3.31. Os materiais a serem utilizados na instalação deverão ser de qualidade e propriedades físicas que melhor se adaptem às condições a que estarão sujeitos, assim como a instalação em ambientes internos (indoor) ou externos (outdoor), deverão seguir rigorosamente as práticas de engenharia e Normas Técnicas pertinentes e em vigor no Brasil;

3.3.32. Todo e qualquer equipamento, acessório ou interface, ainda que não mencionados neste documento, porém, necessário à composição da solução ou necessário ao atendimento de qualquer funcionalidade ou configuração requerida neste Termo de Referência, deverá estar incluído na solução proposta, sem implicação de ônus adicionais para a CONTRATANTE;

3.3.33. os equipamentos que se mostrarem necessários deverão ser fornecidos pela CONTRATADA, em regime de comodato;

3.3.34. A CONTRATADA deverá flexibilizar alocação do IP (Internet Protocol) de modo que, durante o curso da contratação, a CONTRATADA poderá fornecer endereços IPV4 com máscara /24 e endereços IPV6, sendo válidos e contíguos para a Internet (conforme definido na RFC1918), ou poderá fazer portabilidade dos IPs públicos da CONTRATANTE, a depender do tempo que transcorrerá desde o pedido à implantação do AS (Autonomous System) do Tribunal de Justiça de Alagoas, que ficará a cargo da CONTRATANTE.

3.3.35. A CONTRATADA deve ser capaz de prover trânsito para o AS que a CONTRATANTE possuir, com suporte ao protocolo BGP 4 e ASN de 32 bits;

3.3.36. A CONTRATADA deve estar apta a fazer anúncio de rotas do AS que a CONTRATANTE possuir para os backbones nacionais e internacionais;

3.3.37. A CONTRATADA deve possuir política de roteamento que permita trânsito nacional e internacional para o AS que o CONTRATANTE possuir;

3.3.38. A CONTRATADA deverá atender às solicitações de alterações nos parâmetros de roteamento BGP das rotas do AS da CONTRATANTE tais como “local preference” feitas pelos técnicos da CONTRATANTE e devidamente validadas pelos técnicos da CONTRATADA;

3.3.39. O Autonomous System que a CONTRATANTE possuir não poderá ser usado, em nenhuma hipótese, como trânsito para tráfego não diretamente direcionado para a rede da CONTRATANTE, ou seja, o link contratado não deverá ser rota válida para nenhum tráfego do AS de cada provedor, mas apenas o tráfego direcionado a CONTRATANTE pode ser encaminhado a eles;

3.3.40. O AS do provedor deve suportar communities originais e estendidas do BGP, de forma a ser possível para o AS da CONTRATANTE transmitir informações avançadas de tráfego e rotas, e que estas informações sejam respeitadas pelos AS que receberem tais informações, devendo a CONTRATANTE ter o direito de customizar communities com os AS aos quais estará ligado, de forma que tenha controle do modo em que as informações de roteamento serão tratadas nos AS’s vizinhos.

4. SEGURANÇA

4.1. Serviço de segurança perimetral (ganhador do lote 1)

4.1.1. Deverão ser fornecidos equipamentos NGFW do tipo “appliance” e do mesmo fabricante, a fim de viabilizar a compatibilidade e o gerenciamento centralizado dos mesmos.

4.1.2. O hardware, o sistema operacional e os serviços de segurança devem ser desenvolvidos pelo mesmo fabricante, a fim de promover maior compatibilidade dos elementos e otimização de desempenho;

4.1.3. Deve possuir avaliação na NSS Labs para Next Generation Firewall (NGFW) com no mínimo 2 (dois) anos publicados, confirmando uma taxa de bloqueio de ataques (“efetividade de segurança”) superior ou igual à 90% (noventa por cento);

4.1.4. Deve possuir certificação ICSA Firewall;

4.1.5. Deve oferecer além do serviço de firewall, no mínimo, os seguintes serviços de segurança:

4.1.5.1. Sistema de Prevenção de Intrusão (Intrusion Prevention System - IPS);
4.1.5.2. Rede Privada Virtual (Virtual Private Network - VPN);
4.1.5.3. Web Gateway (Anti-Malware, Antivírus, AntiPhishing, Controle de Acesso Web para HTTP/HTTPS e FTP);
4.1.5.4. Controle de Aplicação (Application Control);

4.1.6. Deve possuir inspeção de estados, ou seja, registrar em memória o estado de cada conexão aprovada pelo mesmo, para permitir que ele possa comparar um pacote com o histórico da conexão a qual o mesmo pertence e decidir se o mesmo é válido ou não (stateful inspection/inspeção de estados);

4.1.7. Deve possibilitar a configuração de um intervalo de tempo (timeout) para cada serviço, permitindo eliminar a tabela de estados conexões que estejam ociosas, reduzindo assim o consumo de memória;

4.1.8. Caso a licença do produto venha a expirar por qualquer motivo, todas as funcionalidades essenciais para a continuidade do serviço deverão permanecer habilitadas, ou seja, não será admitida a desativação dos serviços e do seu gerenciamento;

4.1.9. A dispositivo deve dar ao administrador a possibilidade de realizar atualizações de software (patches) e firmware de forma manual e automática;

4.1.10. O dispositivo deve integrar-se com pelo menos o serviço de diretório Active Directory da Microsoft;

4.1.11. Deve suportar DHCP cliente, Relay e Servidor;

4.1.12. Deve suportar PPPoE;

4.1.13. Deve incluir suporte ao protocolo IPv6 nos modos: Ipv6-only, dual stack e tunneling;

4.1.14. Deve ser capaz de trabalhar como agente Sflow.

4.1.15. Deve incluir suporte a OPSF v3;

4.1.16. Deve incluir suporte a IGMP v2 e v3;

4.1.17. Deve incluir suporte a gerenciamento SNMP v1, v2 e v3;

4.1.18. Deve incluir suporte a envio de traps SNMP;

4.1.19. Deve permitir o ajuste de data e hora por meio de NTP;

4.1.20. Suportar a configuração de qualidade de serviço (QoS);

4.1.21. Deve permitir o envio de eventos de log em diferentes níveis (log level) para um servidor de Syslog;

4.1.22. Permitir o armazenamento dos logs localmente, devendo disponibilizar ferramentas que permitam limitar o tamanho da base, fazer backup e extração dos mesmos;

4.1.23. Deve suportar jumbo frames;

4.1.24. As regras de controle de acesso devem possuir como critério para a classificação de um pacote os seguintes campos: IP origem, IP destino, serviço, aplicação e usuário;

4.1.25. As regras de controle de acesso devem permitir utilizar também como critério para a origem de uma conexão um grupo, usuário, ou qualquer combinação destes, através de integração com a base de dados do Microsoft AD;

4.1.26. Deverá ser possível criar regra com tempo determinado para efetividade, de modo que, após o tempo definido, a regra passe a não mais ser avaliada pelo firewall;

4.1.27. Deve permitir definir para cada regra se a mesma irá ou não gerar um log de evento;

4.1.28. Deve compreender o mecanismo de funcionamento dos seguintes protocolos de Voz sobre IP: suportando H323 (incluindo h.245), SIP e MGCP, permitindo assim um controle mais rigoroso dos mesmos;

4.1.29. Deve compreender o mecanismo de funcionamento dos seguintes protocolos de vídeo (streaming): RTP e RTCP;

4.1.30. Deve permitir a criação de regras de firewall por área geográfica (país);

4.1.31. Deve permitir criar regras de alteração de endereço IP (NAT - Network Address Translation) mapeando toda uma faixa de endereços para outra (N para N), toda uma rede para um único IP (N para 1) ou um único IP para outro (1 para 1);

4.1.32. Deve permitir criar regras de alteração de portas TCP ou UDP (PAT - Port Address Translation);

4.1.33. Deve permitir através da combinação de NAT e PAT mapear um único IP válido da faixa de endereços disponível (fornecida pelo provedor) para servidores distintos (com IPs reais diferentes) e que implementem serviços em portas distintas (ex: 200.1.1.1-HTTP vai para a máquina A e 200.1.1.1-FTP vai para a máquina B);

4.1.34. Deve oferecer proteção contra IP spoofing.

4.1.35. GERENCIAMENTO E RELATÓRIOS

4.1.35.1. Deve possuir interface gráfica que permita o fácil gerenciamento de todos os serviços de segurança exigidos para os dispositivos de Firewall de Próxima Geração (NGFW) neste documento;

4.1.35.2. Caso o acesso à interface gráfica aconteça via navegador web (browser), deve ser compatível com os navegadores Internet Explorer, Mozilla Firefox e Google Chrome e permitir acesso criptografado via HTTPs;

4.1.35.3. Caso o acesso à interface gráfica exija a instalação de um software, o mesmo deve ser suportado na plataforma Windows (2003 Server, Vista 32/64 bits, 2008 Server 32/64 bits e Windows 7 32/64 bits) e permitir comunicação criptografada com o dispositivo;

4.1.35.4. A interface deve possuir um dashboard que permita personalizar as telas que contenham as informações mais relevantes para o administrador;

4.1.35.5. A interface deve oferecer ferramentas que viabilizem a inspeção e diagnósticos de problemas (Troubleshoot);

4.1.35.6. A interface deve possibilitar o uso de objetos para representar os componentes da rede (servidores, estações, subredes, roteadores, protocolos, etc.) na criação das regras que definem a política de segurança;

4.1.35.7. A interface deve possuir ferramenta que permita fazer um backup programado de todas as configurações do dispositivo;

4.1.35.8. A interface deverá possuir mecanismos que a tornem mais amigável ao administrador, incluindo, mas não limitado a: facilidade ao se arrastar, soltar e copiar uma regra, clonar um objeto e editar objetos dentro da própria regra;

4.1.35.9. A interface deve permitir a criação de filtros para a visualização das regras, baseados em origem, destino e/ou serviço, de modo a esconder as regras que não satisfaçam os critérios do filtro e deixem visíveis apenas as regras que se encaixaram nos critérios do mesmo; podendose combinar os mesmos usando a lógica AND (E), OR (OU) ou NOT e coringas (contains, greater than or equal, less than equal – operações TCL). Isto torna mais fácil a visualização e, consequentemente, a administração;

4.1.35.10. A interface deve permitir a definição de um nome para cada regra e/ou acrescentar um comentário, facilitando assim a identificação e compreensão do propósito da regra de segurança;

4.1.35.11. A interface deve mostrar claramente as alterações realizadas pelos administradores após a última instalação das regras, apontando claramente as diferenças da política de segurança antes e após as alterações;

4.1.35.12. A interface deve possibilitar a visualização dos logs de eventos gerados pelo sistema e serviços de segurança que estiverem ativos no dispositivo;

4.1.35.13. A interface deve permitir a criação de filtros para o log de eventos de modo a deixar visíveis apenas os logs relativos aos interesses do administrador;

4.1.35.14. A interface deve ser capaz de exibir quais aplicações, IP's de origem ou destino e usuários que mais consomem banda;

4.1.35.15. A interface gráfica deve fornecer estatísticas sobre as origens que mais geraram conexões, os destinos mais acessados, os serviços/aplicações e regras mais utilizadas;

4.1.35.16. A interface deve possibilitar a visualização em tempo real de parâmetros de performance do dispositivo para, no mínimo, utilização da memória, processamento e disco rígido;

4.1.35.17. A interface deve permitir a visualização em tempo real de todos os clientes conectados via VPN, informando o nome do usuário, seu endereço IP real, a data e hora em que foi feita a conexão e o tipo do cliente (SSL, IPSEC, etc.);

4.1.35.18. A interface deve permitir visualização em tempo real de todos os túneis de VPN IPSEC site para site, identificando os peers e o estado do túnel;

4.1.35.19. Deve permitir acesso remoto seguro à linha de comando por meio do protocolo SSH versão 2;

4.1.35.20. Deve permitir que qualquer alteração nas configurações do dispositivo e também a visualização dos logs, possa acontecer tanto por meio da interface gráfica como via linha de comando;

4.1.35.21. A interface deve possibilitar a geração de relatórios por período (Data, ultimo mês, ultima semana, ultimo ano) para os principais serviços de segurança suportados pelo dispositivo;

4.1.35.22. O administrador deve ter a opção de personalizar qualquer um dos relatórios fornecidos pela ferramenta, adaptando-o às suas necessidades;

4.1.35.23. A interface deve permitir gerar relatórios nos formatos HTML, XML, CSV ou PDF;

4.1.35.24. A interface deve incluir a opção de envio de relatório automático por e-mail, podendo ser programada segundo calendário definido pelo administrador;

4.1.35.25. Devem estar disponíveis, no mínimo, os seguintes tipos de relatórios de tráfego de rede:

- Usuários mais ativos;
- Serviços/aplicações mais ativos;
- IP's de origens e destinos mais ativos;
- Serviços/aplicações mais utilizados e suas fontes;
- Serviços/aplicações mais utilizados e seus destinos;
- IP's de origens internas e externas mais bloqueadas;
- IP's de destinos internos e externos mais bloqueados;
- Serviços/aplicações mais bloqueados;

4.1.35.26. Devem estar disponíveis relatórios para o tráfego de VPN, no mínimo, dos seguintes tipos:

- Serviços mais comuns; Origens mais comuns;
- Destinos mais comuns.

4.1.35.27. Deve ser possível filtrar a informação a ser apresentada no relatório com base na origem, destino, serviço ou usuário da conexão;

4.1.36. AUTENTICAÇÃO

4.1.36.1. Deve ser possível filtrar a informação a ser apresentada no relatório com base na origem, destino, serviço ou usuário da conexão;

4.1.36.2. Para administração do dispositivo, deve ser permitida a criação de múltiplos usuários;

4.1.36.3. Deve suportar perfis de administração distintos, de modo que se possam ter administradores com direitos de acesso diferenciados, incluindo pelo menos os seguintes perfis: read/write, read only, gerenciamento de usuários (com exceção de administradores) e visualização de logs;

4.1.36.4. Deve possibilitar a autenticação por meio de um captive portal personalizável pelo administrador;
4.1.36.5. Deve suportar autenticação via Radius, TACACS+, LDAP, base local e Microsoft Active Directory;
4.1.36.6. Deve permitir que em caso de falha na comunicação, por qualquer motivo, do dispositivo com o servidor que contém a base de usuários, seja possível utilizar uma conta de Administrador local como medida de contingência;
4.1.36.7. O login e logout, assim como as alterações feitas por qualquer administrador devem ficar registrados em log para efeito de auditoria;

4.1.37. RECURSO DE ALTA DISPONIBILIDADE

4.1.37.1. Deve permitir o uso de dispositivos em cluster, podendo implementar assim redundância (ativo/passivo) e balanceamento de carga (ativo/ativo), devendo, portanto, vir acompanhado de todas as licenças de software e hardware adequadas;
4.1.37.2. No caso de indisponibilidade de um dos equipamentos do cluster, o outro deverá assumir automaticamente todas as funcionalidades sem causar indisponibilidade dos serviços;
4.1.37.3. A mudança de status de um membro do cluster deve gerar alerta com possibilidade de se utilizar trap snmp;
4.1.37.4. Deve ser assegurando que os equipamentos sejam dotados de mecanismos de replicação em que qualquer alteração realizada em um dos equipamentos seja replicada para outros;
4.1.37.5. O conteúdo da tabela de estados de cada membro do Cluster deve ser compartilhado com os demais membros (sincronismo de tabelas de estado), de modo a permitir que, em caso de falha de um componente do Cluster, as conexões aprovadas pelo mesmo possam continuar ativas em outro membro;
4.1.37.6. Deve permitir a definição de quais interfaces do equipamento serão compartilhadas, quais serão apenas monitoradas e quais são irrelevantes para o funcionamento do cluster;

4.1.38. VPN

4.1.38.1. Deve permitir a criação de túneis entre redes (site para site) e entre clientes e redes (cliente para site);
4.1.38.2. Deve utilizar os protocolos padrão de mercado: IKE e IPSEC;
4.1.38.3. Deve incluir suporte a IKEv1 e IKEv2;
4.1.38.4. Deve possuir proteção contra-ataques de negação de serviço no IKE;
4.1.38.5. Deve suportar os seguintes protocolos de criptografia de dados: 3DES, AES (128 e 256 bits);
4.1.38.6. Deve suportar os protocolos de integridade de dados MD5, SHA1, SHA-256 e SHA-512;
4.1.38.7. Deve suportar pelo menos os seguintes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit) para IKE fases I e II;
4.1.38.8. Deve permitir definir a frequência de troca de chaves tanto na fase 1 quanto na fase 2 do IKE;
4.1.38.9. Deve permitir encapsular os pacotes IPSEC em UDP (NAT Traversal);
4.1.38.10. Deve permitir definir quais conexões (origem, destino e serviço) serão criptografadas;
4.1.38.11. Na autenticação de túneis site para site deve permitir o uso de Certificados Digitais e Senhas (Pre Shared Secret);
4.1.38.12. Na autenticação de túneis cliente para site deve permitir o uso de Certificados Digitais, tokens RSA, LDAP, RADIUS e TACACS;
4.1.38.13. Deve suportar a criação de regras personalizadas na VPN cliente para site, permitindo que grupos de usuários distintos tenham acesso restrito a equipamentos e serviços diferentes na rede protegida pelo firewall;

4.1.38.14. Deve incluir suporte para VPN site para site nas seguinte topologias: Full Meshed (todos para todos), Estrela (escritórios remotos para site central), "Hub and Spoke" (site remoto através de site central para outro site remoto);

4.1.38.15. Deve possuir recurso que permita forçar o roteamento de todo o tráfego do cliente VPN através do túnel criado, de modo a possibilitar que o firewall central tenha visibilidade e possa controlar todo o tráfego do cliente;

4.1.38.16. Deve possuir recurso de DHCP na VPN, fornecendo ao cliente endereço IP e demais parâmetros que o administrador julgar relevantes (DNS, Wins, etc..) e que serão usados pelo cliente em toda a comunicação através do túnel criado;

4.1.38.17. Deve ser capaz de importar Certificados externos de parceiros;

4.1.38.18. Deve incluir a capacidade de confiar em CAs externas;

4.1.38.19. Deve suportar VPNs baseadas em rotas, aonde uma conexão VPN IPSEC Site-to-Site é vista pelo Sistema Operacional como uma interface de rede do tipo ponto-a-ponto, permitindo assim a ativação do protocolo de roteamento OSPF nestas interfaces;

4.1.38.20. Deve permitir desabilitar NAT dentro da VPN site-to-site;

4.1.38.21. Deve permitir desativar o controle de acesso do firewall para o tráfego entre sites remotos interligados por uma VPN.

4.1.39. IPS

4.1.39.1. O modo suspensão (By pass) quando o firewall atingir condições severas de carga (Heavy Load) deve ser opcional;

4.1.39.2. Deve suportar gerenciamento em modo “Failover” e em “Cluster”;

4.1.39.3. Deve suportar modo de inspeção “stateful”;

4.1.39.4. Deve suportar modo “inline” e modo “promiscuos”;

4.1.39.5. Deve suportar atualizações de assinaturas automáticas e manuais;

4.1.39.6. Deve suportar inspeção de tráfego SSL;

4.1.39.7. Deve suportar modo de detecção e proteção contra, no mínimo, as seguintes ameaças:

- SYN (SYN Attack);
- Varredura de portas (Port Scan Attack);
- Web Scraping
- JSON Parser Attack
- HTTP Request Smuggling
- Trojan, backdoor e spyware
- Detecção de evasão
- LDAP injection

4.1.40. CONTROLE DE APLICAÇÃO

4.1.40.1. Deverá contar com ferramentas que permitam administrar o tráfego de aplicações, permitindo o acesso autorizado e o bloqueio das não autorizadas através de capacidade de análise baseada em camada 7 do modelo OSI.

4.1.40.2. Deverá ser possível aplicar a análise de camada 7 em todas as políticas suportadas pelo equipamento, ou seja, se o equipamento suportar a criação de 2.500 (duas mil e quinhentas) políticas, deverá ser possível aplicar este recurso em todas, bem como criar assinaturas para aplicações customizadas;

4.1.40.3. Deverá identificar as aplicações, independente das portas e protocolos, assim como técnicas de evasão utilizadas;

4.1.40.4. As funções de controle de aplicações, não podem impossibilitar a ativação de outras funcionalidades de segurança, tais como:

4.1.40.4.1. IPS;

4.1.40.4.2. Antivírus;

4.1.40.4.3. Anti-malware;

4.1.40.4.4. Controle de tipos de arquivos (por extensão e assinaturas);

4.1.40.5. Deve possibilitar o controle das aplicações por, no mínimo, das seguintes formas:

4.1.40.5.1. Aplicação;

4.1.40.5.2. Categorias;

4.1.40.5.3. Risco;

4.1.40.5.4. IP/Range de IP's/Redes;

4.1.40.5.5. Usuários;

4.1.40.6. Diferentes grupos de usuários;

4.1.40.7. Deve possibilitar a integração com base externa de "Active Directory" e LDAP, para criação de políticas. Possibilitando a criação de regras utilizando:

4.1.40.7.1. Usuários;

4.1.40.7.2. Grupo de usuários;

4.1.40.7.3. Endereço IP;

4.1.40.7.4. Endereço de Rede;

4.1.40.7.5. Combinação das opções acima.

4.1.40.8. Deve possibilitar a customização de aplicações, categorias e grupos que não estão na base de aplicações, para utilização na criação de políticas;

4.1.40.9. Deve possibilitar a utilização de no mínimo 2 ações nas regras de controle: Bloquear e Monitorar;

4.1.40.10. Deve ter um mecanismo configurável de bypass onde o administrador consegue definir grupos específicos de usuários que estão autorizados a ignorar as regras de filtragem de aplicações para um período de tempo específico;

4.1.40.11. Deve permitir a verificação de regras por intervalo de tempo e/ou período (data e horário de início e fim de validade);

4.1.40.12. Deve fornecer um mecanismo para limitar o uso de aplicativos baseados em consumo de banda tanto para upload quanto download;

4.1.41. REDUNDÂNCIA DE LINK INTERNET

4.1.41.1. O dispositivo deve permitir configurar redundância de link de acesso a Internet utilizando-se circuitos de provedores diferentes e, consequentemente, faixas de endereços IP diferentes;

4.1.41.2. Deve incluir suporte a agregação de links, permitindo tratar um conjunto de links físicos como um único link lógico;

4.1.41.3. Para a seleção do link para o qual o pacote será destinado deve suportar o uso dos mecanismos active/standby, Round-Robin e 802.3ad, permitindo ao administrador escolher qual o mais apropriado a seu ambiente;

4.1.41.4. O firewall deve poder verificar a disponibilidade do link através de testes de conectividade com destinos configuráveis pelo administrador;

4.1.41.5. O firewall deverá fazer NAT do tráfego de saída utilizando o endereço IP do provedor do link selecionado, independente do modelo de redundância escolhido;

4.1.42. WEB GATEWAY (ANTI-MALWARE, ANTIVÍRUS, ANTIPHISHING, CONTROLE DE ACESSO WEB PARA HTTP/HTTPS E FTP)

4.1.42.1. Deve possuir sistema de Filtragem de URL ativado para pesquisas locais, bem como consultar banco de dados na nuvem para URL´s desconhecidas.

4.1.42.2. Possuir verificação contra códigos maliciosos como vírus, worms, trojans, phishing, spyware e applets e activeX maliciosos, sem a necessidade de um agente (agentless) ou software adicional;

4.1.42.3. Permitir criar políticas de permissão baseado no perfil do usuário ou grupo, range ou endereço IP, permitindo uma navegação mais segura;

4.1.42.4. Permitir a utilização da ferramenta em modo Transparent Bridge;

4.1.42.5. Desejável possuir suporte ao protocolo ICAP (Internet Content Adaptation Protocol);

4.1.42.6. Integrar-se às seguintes soluções de diretório de usuários: Microsoft Active Directory e OpenLDAP;

4.1.42.7. Realizar a verificação somente em arquivos passíveis de códigos maliciosos, permitindo assim um melhor desempenho;

4.1.42.8. A ferramenta deve realizar o escaneamento em tempo real das URL's a fim de identificar ameaças, identificando-as o seu bloqueio deve ser realizado automaticamente;

4.1.42.9. Atualização automática das vacinas de forma incremental e da versão do software;

4.1.42.10. Utilizar OCSP (Online Certificate Status) e possuir base local para inclusão de certificados confiáveis;

4.1.42.11. Possuir banco de dados de URL categorizados em, no mínimo, 60 categorias e tomar as seguintes ações para o acesso a estas categorias: permitir, bloquear, monitorar e alertar. Este banco de dados deve estar hospedado em um servidor externo (nuvem) e localmente, disponibilizado e assegurado pelo fabricante para que se tenha uma atualização mais rápida das categorias, não sendo necessária a consulta, na nuvem, para cada URL;

4.1.42.12. Possibilidade de permissão de acesso websites definidos nas categorias em períodos prédeterminados;

4.1.42.13. Possuir a funcionalidade de criação de categorias customizadas pelo o administrador da ferramenta;

4.1.42.14. Possuir a funcionalidade de liberar ou bloquear URL`s categorizadas ou não;

4.1.42.15. Possuir integração com Safe Search do Google e do Yahoo;

4.1.42.16. Deverá ser possível customizar as páginas de bloqueio apresentadas aos usuários;

4.1.42.17. Possuir recurso para permitir / bloquear conexões Peer-to-Peer (BitTorrent, Gnutella, eDonkey e etc);

4.1.42.18. Possuir capacidade de analisar o conteúdo de páginas que possam apresentar conteúdo malicioso e, automaticamente, bloqueá-las. Este recurso deverá estar integrado às funções de análise de malware e spyware do equipamento;

4.1.42.19. Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada deve possuir capacidade para detecção de Malwares não conhecidos (dia Zero);

4.1.42.20. O dispositivo deve ser capaz de enviar arquivos suspeitos de forma automática para análise "In Cloud" ou para dispositivo local, onde o arquivo será executado e simulado em ambiente controlado (Sandbox);

4.1.42.21. Possibilitar a pré-definição de políticas para determinar quais tipos de arquivos deverão ser enviados para análise;

4.1.42.22. Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para detecção da ameaças não conhecidas;
4.1.42.23. Deve suportar a monitoração de arquivos trafegados na internet (HTTP, FTP, HTTP, SMTP) como também arquivos trafegados internamente nos servidores de arquivos usando SMB;

4.1.43. DETALHAMENTO DO APPLIANCE FIREWALL NEXT-GENERATION

4.1.43.1. Quantidade: 2 unidades em alta disponibilidade;
4.1.43.2. Deve ser licenciado para um número ilimitado de usuários e endereços IP;
4.1.43.3. Deve ocupar no máximo 1RU;
4.1.43.4. Deve possuir pelo menos 8 interfaces 10/100/1000Mbps Base-T (RJ-45);
4.1.43.5. Deverá possuir interface para gerenciamento por console;
4.1.43.6. Possuir alimentação elétrica AC 100-240V, 50-60Hz;
4.1.43.7. Cada equipamento deverá suportar padrão de tomada do tipo NBR 14136;
4.1.43.8. Deve suportar operação em ambientes com temperaturas entre 0 e 40 graus Celsius;
4.1.43.9. Deve suportar operação em ambientes com umidade relativa do ar entre 20% e 90%;
4.1.43.10. Deve permitir a configuração de até 1024 VLANs;
4.1.43.11. Cada equipamento deverá oferecer um throughput de no mínimo de 10 Gbps para firewall (1518/512/64);
4.1.43.12. Cada equipamento deverá oferecer um throughput de no mínimo 1,5 Gbps para NGFW
4.1.43.13. Cada equipamento deverá oferecer um throughput de no mínimo de 350 Mbps para VPN (siteto-site e cliente-to-site);
4.1.43.14. Cada equipamento deverá oferecer um throughput de no mínimo de 3 Gbps de IPS;
4.1.43.15. Deve possuir no mínimo 4000 licenças do tipo “cliente-to-site” IPSEC e SSL e 100 licenças do tipo “site-to-site”;
4.1.43.16. Deve suportar pelo menos 5 Milhões de sessões concorrentes;
4.1.43.17. Deve suportar o estabelecimento de pelo menos 200 Mil novas conexões por segundo;

4.1.44. SERVIÇOS DE GERENCIAMENTO PARA FIREWALL NEXT-GENERATION

4.1.44.1. Prover serviços de gerenciamento centralizado para os firewall Next-Generation através de SOC (Security Operation Center) localizado no Brasil
4.1.44.2. Atendimento através de e-mail e ligação 0800 na língua portuguesa em regime 24x7x365
4.1.44.3. A solução de gerenciamento deve dar ao administrador a possibilidade de realizar atualizações de software (patches) e firmware de todos os dispositivos de segurança de forma manual e automática;
4.1.44.4. Deve incluir suporte a gerenciamento SNMP v1, v2 e v3;
4.1.44.5. Deve incluir suporte a envio de traps SNMP;
4.1.44.6. Deve permitir o ajuste de data e hora por meio de NTP;
4.1.44.7. Deve permitir o envio de eventos de log em diferentes níveis (log level) para um servidor de Syslog;
4.1.44.8. Permitir o recebimento e armazenamento dos logs localmente de todos os dispositivos de segurança, devendo disponibilizar ferramentas que permitam limitar o tamanho da base, fazer backup e extração dos mesmos;
4.1.44.9. Deve ser capaz de atualizar e gerenciar de forma centralizada, no mínimo, os seguintes conteúdos de segurança:
- Assinaturas de Antivirus;
- Assinaturas de IPS;

- Políticas de Web Gateway;
- Políticas de Regras de Firewall;
- Políticas de Controle de Aplicação;
- Criar, implantar e monitorar VPN's;
- Políticas de filtro Web;

4.1.44.10. Manter armazenamento de logs dos últimos 365 dias corridos

4.1.44.11. Prover administração e gerenciamento em regime 24x7

4.1.44.12. Suportar número ilimitado de solicitações de troca de regras no mês

4.1.44.13. Estabelecer SLA para troca de regras com pelo menos 2 horas para atendimento e limite de 4 horas para aplicação

4.1.44.14. Prover upgrade de software e firmware durante a vigência do contrato

4.1.44.15. Estabelecer suporte técnico do fabricante para solucionar qualquer problema relacionado ao appliance ou software

4.1.44.16. Prover relatórios customizados ao CONTRATANTE quando solicitado, relativos aos serviços de monitoramento e segurança fornecidos pelo NGFW, tais como: usuários mais ativos, serviços/aplicações mais ativos, IP's de origens e destinos mais ativos, dentre outros;

4.2. Serviço de proteção de negação de serviço distribuído (Distributed Denial of Service-DDoS)

4.2.1. CARACTERÍSTICAS GERAIS

4.2.1.1. Capacidade de criar e analisar a reputação de endereços IP, possuindo base de informações própria, gerada durante a filtragem de ataques, e interligada com os principais centros mundiais de avaliação de reputação de endereços IP.

4.2.1.2. Suportar mitigação automática de ataques, utilizando múltiplas técnicas como White Lists, Black Lists, limitação de taxa, técnicas desafio-resposta, descarte de pacotes mal formados, técnicas de mitigação de ataques aos protocolos HTTP e DNS, bloqueio por localização geográfica de endereços IP, dentre outras.

4.2.1.3. Prover informações de origem de ataque dos países, ranges de IP's e características do tipo de ataque.

4.2.1.4. Serviço de atualização de assinaturas de ataques das soluções de detecção e mitigação

4.2.1.5. Capacidade de detectar e mitigar todos e quaisquer ataques que façam o uso não autorizado de recursos de rede, tanto para IPv4 como para IPv6, incluindo, mas não se restringindo aos seguintes:

4.2.1.5.1. Ataques de inundação (Bandwidth Flood), incluindo Flood de UDP e ICMP;

4.2.1.5.2. Ataques à pilha TCP, incluindo mal uso das Flags TCP, ataques de RST e FIN, SYN Flood e TCP Idle Resets;

4.2.1.5.3. Realizar autenticação de conexão TCP, quando do recebimento de pacotes syn;

4.2.1.5.4. Limitar o número de conexões TCP simultâneas de um mesmo host;

4.2.1.5.5. Ataques que utilizam Fragmentação de pacotes, incluindo pacotes IP, TCP e UDP;

4.2.1.5.6. Ataques de Botnets, Worms e ataques que utilizam falsificação de endereços IP origem (IP Spoofing);

4.2.1.5.7. Ataques denominados de "Comand-and-Control", Point of Sale Malware, Remote Access Trojans RAT's via feed atualizado diariamente;

4.2.1.5.8. Ataques à camada de aplicação, incluindo protocolos HTTP e DNS Volumetricos;

4.2.1.5.9. Bloqueio de query de DNS, resposta de query de DNS baseado em domínio pré-cadastrado para autenticação e checagem de flag de recursão DNS;

4.2.1.5.10. DNS BlackList;

4.2.1.5.11. RegEx para registros específicos ou “flags de recursão.

4.2.1.6. Possuir mecanismos de quando bloquear um ataque por expressão regular DNS, selecionar se bloqueia apenas o ataque ou o host temporariamente

4.2.1.7. Autenticação em query DNS por requisição em TCP

4.2.1.8. Autenticação em JavaScript e Redirect para HTTP

4.2.1.9. Adicionar expressão regular de “payload” em black-list

4.2.1.10. Prevenir que hosts válidos sejam adicionados a black-list por engano

4.2.1.11. Capacidade de interagir automaticamente ou manualmente com solução “on-premisse” (appliance) localizado in-site no datacenter do cliente; No caso, o appliance quando detectar um ataque DDoS pode automaticamente ou manualmente (conforme SLA) requisitar mitigação na nuvem, para apenas o tráfego atacado, e não todo o tráfego do datacenter.

4.2.1.12. A sinalização entre datacenter e nuvem deve ser capaz de ocorrer em qualquer protocolo protegido (TCP/UDP/ICMP/DNS/HTTP), podendo ser ativada por qualquer uma das contramedidas acima.

4.2.1.13. Manter lista dinâmica de endereços IP bloqueados, retirando dessa lista os endereços que não enviarem mais requisições maliciosas após um período de tempo considerado seguro

4.2.1.14. As soluções de detecção e mitigação devem possuir serviço de atualização de assinaturas de ataques.

4.2.1.15. A mitigação de ataques deve ser baseada em arquitetura na qual há o desvio de tráfego suspeito comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento.

4.2.2. CARACTERÍSTICAS DA INFRAESTRUTURA DE SUPORTE ANTI-DDOS

4.2.2.1. Possuir conexão com Centro Operacional de Segurança (ou SOC – Security Operations Center) no Brasil, com equipe especializada em monitoramento, detecção e mitigação de ataques, com opção de atendimento através de telefone 0800, correio eletrônico, em idioma português brasileiro, durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual.

4.2.2.2. Possuir conexão com no mínimo 1 centro de limpeza nacional com capacidade de mitigação de 10Gbps e 3 centros de limpeza internacional com capacidade de mitigação de 30Gbps.

4.2.2.3. Evitar saturação da banda de Internet em caso de ataques de negação de serviço (Distributed Denial of Service – DDoS) com capacidade de mitigar 10 Gbps.

4.2.2.4. Caso o volume de tráfego do ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS devem ser tomadas contramedidas tais como aquelas que permitam o bloqueio seletivo por blocos de IP de origem no AS pelo qual o ataque esteja ocorrendo, utilizando técnicas como Remote Triggered Black Hole.

4.2.2.5. As funcionalidades de monitoramento, detecção e mitigação de ataques são mantidas em operação ininterrupta durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual.

4.2.2.6. O bloqueio de ataques DOS e DDOS não são realizados por ACLs em roteadores de borda.

4.2.2.7. Deve disponibilizar um portal onde a contratante tem acesso online aos tipos de ataques sofridos e o tamanho destes ataques categorizados por severidade (Ex: baixo, Médio, Alto).

4.2.2.8. A mitigação dos ataques é realizada dentro do Brasil, sem encaminhamento do tráfego para limpeza fora do território brasileiro.

4.2.2.9. Em momentos de ataques DOS e DDOS, todo trafego limpo é reinjetado na infraestrutura da contratante através de túneis GRE (Generic Routing Encapsulation), configurado entre a plataforma de DOS e DDOS da contratada e o CPE do contratante.

4.3. Transferência de conhecimento

4.3.1. A CONTRATADA deverá capacitar a equipe de gerência de infraestrutura da CONTRATANTE, para que a torne apta a utilizar de forma eficiente e eficaz os equipamentos de segurança e monitoramento fornecidos;

4.3.2. O treinamento versará sobre a operação e configuração da solução para 10 pessoas da equipe técnica do TJ-AL, ministrado por um instrutor certificado pelo fabricante, nas instalações da CONTRATANTE e com todos os equipamentos também por ela fornecidos.

4.3.3. O treinamento deverá ser sem custo adicional ao preço formulado em sua proposta, incluindo material didático oficial.

5. DA VISTORIA TÉCNICA

5.1. A empresa interessada em compor o certame licitatório poderá realizar, mediante agendamento, através do seu responsável técnico devidamente credenciado, vistoria da infraestrutura do órgão em período que compreende da publicação do edital até 48 (quarenta e oito) horas úteis antes da realização do certame do presente objeto.

5.2. Destinada ao licitante que deseje verificar in loco as características físicas do prédio, os locais de instalação dos equipamentos intermediários, a verificação da infraestrutura no DATACENTER, objetivando colher todas as informações e impressões da LICITANTE quanto ao espaço físico que irá trabalhar, para que não haja erro de dimensionamento dos recursos nem quaisquer alegações futuras.

5.3. A vistoria será realizada no Data Center do Tribunal de Justiça do Estado de Alagoas, localizado no Anexo Administrativo I, situado à Praça Marechal Deodoro, Maceió-AL;

5.4. Sendo tal visita opcional, não será emitido certificado de comparecimento e também serão ignoradas alegações de prejuízos para composição das propostas comerciais, por desconhecimento das instalações físicas onde deverá ser instalado o circuito.

6. REQUISITOS DE ATIVAÇÃO DOS SERVIÇOS

6.1. A passagem dos cabos necessários para ativação dos circuitos, desde o ambiente externo até ao local de instalação dos equipamentos de comunicação de cada localidade é de responsabilidade da CONTRATADA;

6.2. Os equipamentos necessários para a implantação do serviço de comunicação de dados contratados deverão ser instalados nas dependências da CONTRATANTE;

6.3. A CONTRATADA deverá executar os serviços de instalação física, configurações e testes necessários à operação dos equipamentos;

6.4. Após a assinatura do contrato, a CONTRATADA deverá disponibilizar, no prazo máximo de 10 (quinze) dias corridos, um projeto técnico e um plano de trabalho, contendo, no mínimo: a) Topologia detalhada;

b) Plano de Execução;

c) Cronograma de atividades;

d) Responsáveis técnicos pelas atividades;

e) Plano de Testes;

f) Roteiro de testes para verificação da operação dos serviços;

g) Plano de monitoramento do serviço;

h) Plano de continuidade para eventuais riscos e falhas no serviço;

6.5. Após a entrega do Plano de Trabalho, a CONTRATANTE terá até 10 (dez) dias corridos para avaliar e aprovar o referido documento;

6.6. Caso o Plano de Trabalho seja rejeitado pela CONTRATANTE, a CONTRATADA terá o prazo de até 5 (cinco) dias corridos para efetuar as correções;

6.7. Deverá haver agendamento da data de instalação das conexões à internet nas localidades conjuntamente com a equipe técnica da CONTRATANTE, de maneira que haja o acompanhamento das instalações pelo Fiscal do Contrato e de forma a interferir o mínimo possível nos trabalhos normais da localidade;

6.8. A instalação física, configuração dos equipamentos e ativação dos serviços será realizada em dia e horário definido pela CONTRATANTE, podendo ser realizados em sábados, domingos e feriados, caso a CONTRATANTE julgue necessário, sem nenhum ônus adicional;

7. DO PRAZO DE EXECUÇÃO

7.1. Para todos os lotes, o prazo máximo de instalação dos equipamentos e dos acessos à Internet e início da prestação dos serviços contratados será de até 30 dias corridos, contados a partir da aprovação do plano de trabalho.

8. DOS TESTES E ACEITE DOS SERVIÇOS

8.1. Para efeito de aferição contínua da qualidade do serviço prestado, o objeto contratado será avaliado tanto na fase de instalação e ativação inicial do serviço quanto periodicamente, através de aceites mensais.

8.2. Na fase de instalação e ativação inicial do serviço, o aceite se dará:

8.2.1. Provisoriamente

8.2.1.1. Após a ativação dos serviços, a CONTRATADA realizará os testes necessários, em conjunto com a equipe técnica da CONTRATANTE, de forma a verificar se os serviços estão em conformidade com as especificações deste Termo de Referência, no prazo de 10 dias úteis;

8.2.1.2. Os testes compreenderão, no mínimo:

a) aferição da velocidade do link instalado, tanto para download como para upload;

b) constatação da adequação do circuito instalado aos requisitos de qualidade descritos nas especificações técnicas (Banda Disponível, Latência - RTT - e Perda de Pacotes);

c) avaliação da qualidade dos serviços de instalação realizados (passagem de cabos lógicos e elétricos, acomodação de equipamentos, entre outros);

d) avaliação da qualidade, eficiência e presteza do serviço de atendimento a chamados de manutenção, bem como, da disponibilidade e urbanidade dos funcionários prepostos da empresa contratada;

e) avaliação do desempenho do circuito no acesso a sites comumente utilizados pela contratante;

f) avaliação do desempenho do circuito no acesso ao Datacenter do TJ-AL, via VPN.

8.2.1.3. A CONTRATADA deverá disponibilizar meios de aferir a velocidade dos links instalados, não eximindo o CONTRATANTE de usufruir de meios próprios para ratificar a aferição das velocidades contratadas;

8.2.2. Definitivamente

8.2.2.1. Havendo cumprimento integral das condições expressas neste Termo de Referência, o CONTRATANTE formalizará o aceite definitivo da ativação do objeto.

8.2.2.2. O aceite definitivo dar-se-á mediante a emissão do Termo de Recebimento Definitivo (TRD) assinado pelas partes.

8.3. Mensalmente, para os serviços de conectividade com a Internet bem como os serviços de antiDDoS, o recebimento se dará:

8.3.1. **provisoriamente**, até o quinto dia útil de cada mês, pelo órgão recebedor do objeto, para efeito de posterior verificação da conformidade das especificações, sendo que nessa oportunidade deverão ser entregues:

8.3.1.1. Relatório mensal analítico, elaborado pela CONTRATADA, contendo, no mínimo:

a) Relação de chamados de manutenção abertos no mês anterior

b) Tempo de indisponibilidade por chamado;

c) Horário de abertura e encerramento por chamado;

d) Tempo total de falhas, apuração mensal de indisponibilidade e dos Acordos de Nível de Serviço.

8.3.1.2. Relatório mensal de ocorrências de ataques DDoS ocorridos no mês anterior, elaborado pela CONTRATADA com seus próprios registros e anotações.

8.3.2. **definitivamente**, pelo gestor responsável pela fiscalização do ajuste ou, nos casos em que se enquadrarem no §8º do art. 15 da Lei nº 8.666/93, por comissão designada pela Diretora-Geral, no prazo máximo de 5 (cinco) dias, contados da data do recebimento provisório, mediante termo circunstanciado, após:

a) Verificação de conformidade da prestação em relação às especificações estabelecidas e exigências constantes no Contrato, Edital e seus anexos;

b) Verificação e confronto do Relatório mensal de chamados de manutenção abertos no mês com os registros da Ferramenta de Monitoração da Rede Local do TJAL e do Sistema de Registro de Ocorrências da Rede Local do TJAL;

c) Verificação do atendimento pela CONTRATADA dos níveis de serviço exigidos por intermédio da análise de relatório mensal emitido pelo Sistema de Registro de Ocorrências da Rede Local do TJAL além de gráfico colhido na Ferramenta de Monitoração da Rede Local do TJAL com o indicativo de disponibilidade dos links mantidos pelo contrato em questão, confrontando as informações com as condições estabelecidas no Acordo de Nível de Serviço (ANS);

8.4. Os relatórios aos quais se referem o caput são essenciais para a liberação do pagamento da fatura, ficando, por conseguinte, adiado todo o pagamento até a apresentação dos relatórios e o aceite do Tribunal.

8.5. Os serviços considerados em desconformidade serão rejeitados na sua totalidade, ou em parte, devendo a empresa contratada providenciar as devidas correções na maior brevidade possível.

8.6. Enquanto os serviços não forem aceitos na sua totalidade, continuará a transcorrer o prazo de entrega, não sendo devido à empresa contratada pagamentos de qualquer espécie.

8.7. A prestação do serviço será considerada iniciada somente após o ACEITE DEFINITIVO por parte da equipe técnica responsável da CONTRATANTE. Portanto, o início do período de faturamento se dará no primeiro dia após o aceite da totalidade dos serviços entregues.

8.8. O ACEITE DEFINITIVO não isenta a CONTRATADA das responsabilidades sobre o pleno funcionamento de todas as facilidades e vantagens oferecidas, estendendo-se a necessidade de teste destas facilidades ao longo da prestação dos serviços;

9. GERENCIAMENTO PRÓ-ATIVO E ASSISTÊNCIA TÉCNICA

9.1. Caberá ao fornecedor vencedor, juntamente com a equipe técnica do Tribunal, gerenciar de forma pró-ativa a Conexão IP Internet CONTRATADA, em regime de 24x7, garantindo os níveis de serviço contratados fim-a-fim, tempo de retardo de ida e volta, percentual de pacotes com erros, percentual de descarte de pacotes, disponibilidade, desempenho da rede CONTRATADA e os demais indicadores de Acordo de Nível de Serviço (ANS).

9.2. A CONTRATADA deve efetuar manutenção corretiva assim que for detectado algum mau funcionamento de enlaces e equipamentos, ou problemas em instalações feitas, de forma que voltem a funcionar perfeitamente;

9.3. A CONTRATADA deve realizar o serviço de manutenção no local de instalação do equipamento sempre que possível. Caso seja necessário remover o equipamento, a CONTRATADA deve providenciar a

substituição do equipamento por outro idêntico ou superior, em perfeito funcionamento, para então retirar o equipamento com defeito e encaminhá-lo para a manutenção;

9.4. Todos os custos acarretados tanto pela troca de materiais/acessórios (transporte, instalação, e etc.) quanto pela realização de ajustes nas instalações (transporte, alimentação, e etc.) serão de responsabilidade da CONTRATADA.

9.5. A CONTRATADA deverá oferecer suporte técnico em regime de 24x7x365 (vinte e quatro horas por sete dias na semana, por trezentos e sessenta e cinco dias no ano), com serviço de atendimento telefônico gratuito tipo 0800 para a área de Maceió, com atendimento às chamadas na língua portuguesa.

9.6. Quando da solicitação de atendimento, a CONTRATADA fornecerá à CONTRATANTE, o número do respectivo chamado técnico;

9.7. A Central de Atendimento Especializado da CONTRATADA deverá manter um sistema de registro, acompanhamento dos chamados e esclarecimentos de dúvidas, compreendendo desde o registro de abertura até a resolução do fato motivador do chamado e permitindo, inclusive, o acesso a essas informações pela CONTRATANTE;

9.8. Qualquer abertura de chamado técnico somente poderá ser encerrada com o consentimento expresso de algum preposto da CONTRATANTE. No encerramento do chamado técnico, a CONTRATADA deverá registrar o nome do preposto da CONTRATANTE, responsável pela autorização de encerramento do chamado técnico;

9.9. Os tempos de recuperação serão computados a partir do recebimento da solicitação de reparo pela central de atendimento da CONTRATADA até a comunicação do término desse reparo à CONTRATANTE;

9.10. Quando não for possível a abertura de chamado na Central de Atendimento da CONTRATADA, a indisponibilidade será considerada a partir da efetiva interrupção registrada pelos sistemas da CONTRATANTE e/ou CONTRATADA;

10. ACORDO DE NIVEL DE SERVIÇO (ANS)

10.1. O acordo de nível de serviço (ANS) visa garantir que os serviços contratados sejam prestados pela CONTRATADA em grau mínimo de eficiência e qualidade exigido pela CONTRATANTE;

10.2. A CONTRATADA será responsável pelo cumprimento e medição dos índices estabelecidos neste item que serão auditados pela CONTRATANTE durante todo o prazo de vigência do contrato, e que poderão ser revistos, a qualquer tempo, com vistas à melhoria ou ajustes na qualidade dos serviços prestados;

10.3. As inoperâncias e/ou indisponibilidades dos serviços, no todo ou em parte, que não sejam de responsabilidade da CONTRATANTE, bem como insuficiência no alcance dos níveis mínimos de satisfação dos requisitos técnicos, representados por indicadores, devem gerar descontos na fatura proporcionais ao tempo de desconformidade;

10.4. DA DISPONIBILIDADE MENSAL DO SERVIÇO

10.4.1. A disponibilidade operacional mensal mínima é definida como a relação entre o tempo em que o sistema apresenta as características técnicas e operacionais especificadas e o tempo total considerado;

10.4.2. Deve ser assegurada disponibilidade operacional mensal mínima de 99,7%;

10.4.3. O serviço deverá estar disponível 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, todos os dias do ano. Desta maneira a CONTRATADA deverá estabelecer estrutura de operação para este nível de serviço;

10.4.4. No cálculo da disponibilidade serão consideradas todas as interrupções do serviço, exceto as programadas pelo CONTRATANTE ou pela CONTRATADA;

10.4.5. A disponibilidade do serviço indicará o percentual de tempo, durante o período de 01 (um) mês de operação, em que o serviço permanece em condições normais de funcionamento;

10.4.6. O serviço será considerado indisponível a partir do início de uma interrupção registrada no centro de atendimento/supervisão da CONTRATADA ou a partir da comunicação de interrupção, feita pela CONTRATANTE, até o restabelecimento do serviço às condições normais de operação e a respectiva informação à CONTRATANTE;

10.4.7. Serão excluídas desta contagem as interrupções programadas para manutenção, desde que seja feita comunicação à CONTRATANTE com pelo menos 05 (cinco) dias úteis de antecedência e que a interrupção seja programada para ser executada das 19h00 às 05h00;

10.4.8. Serão excluídas dessa contagem as interrupções causadas por falta de energia elétrica nas localidades que ocasione o desligamento dos equipamentos instalados na CONTRATANTE, hipótese que será investigada pela equipe da CONTRATANTE;

10.4.9. Caso haja interrupções não programadas nos serviços, a CONTRATADA fica sujeita a descontos na fatura mensal, aplicados no mês imediatamente subsequente ao mês no qual ocorreram os fatos que originaram os descontos.

10.5. PRAZOS GERAIS PARA ATENDIMENTO E REPARO

10.5.1.1. Na ocorrência de inoperância dos circuitos, o prazo máximo para reparo/restabelecimento deverá obedecer a classificação de severidade e o prazo máximo de reparo, conforme tabelas abaixo:

CLASSIFICAÇÃO DOS NÍVEIS DE SEVERIDADE DOS CHAMADOS	
NÍVEIS	**DESCRIÇÃO**
1-CRÍTICO	Serviços totalmente indisponíveis. Sem conectividade total. Falha em equipamentos da CONTRATADA que torne indisponível a conexão. Impacto a múltiplos usuários. Falha em link que afete operações críticas da CONTRATANTE.
2-URGENTE	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta da conexão. Falha intermitente que torne o acesso insatisfatório. Lentidão ou velocidade abaixo do contratado. Impacto moderado. Operação normal afetada, mas sem interrupção.

3-NORMAL	Serviços disponíveis com ocorrência de alarmes e avisos, consulta sobre problemas, dúvidas gerais. Manutenção e monitoramento de eventos de falhas ou de avisos relatados pelo cliente. Pequeno impacto a um ou mais usuários. A correção pode ser feita de forma agendada.

TABELA DE PRAZOS DE ATENDIMENTO E REPARO PARA OS LOTES 1 e 2				
MODALIDADE	PRAZOS	Níveis de severidade		
		1-CRÍTICO	**2-URGENTE**	**3-NORMAL**
Atendimento local, e-mail, web ou telefone	Término do atendimento	2 horas	4 horas	8 horas

10.5.1.2. Deverá ser considerado a contagem do tempo de atendimento de forma ininterrupta e contínua;

10.5.1.3. Deverá ser considerado horas corridas no prazo de atendimento;

10.5.1.4. Entende-se por reparo/restabelecimento do funcionamento, a série de procedimentos destinados a recolocar os serviços em seu perfeito estado de uso, compreendendo inclusive, substituição de equipamentos, ajustes e reparos;

10.5.1.5. Os níveis de severidade elencados servem como referência ao prazo máximo tolerado pelo Tribunal para os respectivos níveis, podendo haver sansões contratuais pelo desrespeito aos limites de tempo estabelecidos. Não há impedimento quanto a aplicação cumulativa de descontos ocasionados pelo não cumprimento dos indicadores de aferição de ANS.

10.5.2. MÉTODOS E INDICADORES DE AFERIÇÃO DO ANS

10.5.2.1. A aferição das metas estipuladas no Acordo de Nível de Serviço deverá obedecer aos indicadores abaixo, sem que isso isente a CONTRATADA de cumprir todas as demais exigências deste Termo de Referência, as quais também são passíveis de sanção.

10.5.2.2. CONTRATADA deverá disponibilizar, mensalmente, relatório consolidado com todos os indicadores de aferição de ANS, bem como relatórios individualizados para cada indicador.

10.5.2.3. O CONTRATANTE promoverá auditagem das aferições realizadas pela CONTRATADA por meio de ferramentas próprias de monitoramento de rede.

10.5.2.4. Indicador de Disponibilidade de Rede:

INDICADOR DE DISPONIBILIDADE MENSAL	
ITEM	**DESCRIÇÃO**
Finalidade	Garantir o pleno funcionamento de um circuito, em condições normais de operação.
Início de vigência	Data do Termo de Recebimento Definitivo (TRD)
Cálculo	**IDM=[(To-ΣTi)/To]*100** Onde: IDM = índice de disponibilidade mensal do enlace em % To = período de operação (um mês) em minutos. ΣTi = somatório dos tempos de inoperância durante o período de operação (um mês) em minutos.

Limiar de satisfação	**Mínimo de 99,7%**
Sanções	Índice de Disponibilidade Mensal abaixo do contratado = Multa moratória de 2% sobre o valor mensal do circuito a cada 0,1% abaixo do contratado no valor do IDM. Limitada a 10% do valor mensal do circuito. Superado esse limite, será aplicada a sanção estabelecida no item 20 deste TERMO, sem prejuízo à aplicação da multa moratória.
Relatórios de Níveis de Serviço	A CONTRATADA deverá disponibilizar mensalmente à CONTRATANTE, relatórios com IDM apurado diariamente, totalizados e apresentados mensalmente por enlace. Nos relatórios citados deverão ser apresentados (em minutos): o tempo de indisponibilidade, o tempo de interrupções programadas, o tempo de interrupções de responsabilidade do CONTRATANTE. A CONTRATADA deverá disponibilizar, quando demandada pelo CONTRATANTE, relatório detalhando os tempos de falhas (com hora de início e fim da inoperância), minutos excedentes ao prazo máximo para reparo e disponibilidade no período (mês) e motivo(s) da(s) indisponibilidade(s) apurada(s).

10.5.2.5. Indicador de Taxa de Perda de Pacotes

TAXA DE PERDA DE PACOTES (TPP)	
ITEM	**DESCRIÇÃO**
Finalidade	Garantir o mínimo de perda de pacotes nos circuitos contratados.
Periodicidade	Medições diárias e constantes, sobretudo em horários de maior tráfego. Sempre que a CONTRATANTE julgar necessário, poderá ser solicitada a medição do percentual de perda de pacotes fim a fim, através de equipamento de teste especializado, sem prejuízo de medições próprias a serem realizadas pelo Tribunal .
Cálculo	**TPP=[(NPO-NPD)/NPO]*100** Onde: TPP = Taxa de Perda de Pacotes NPO = Nº de pacotes na origem NPD = Nº de pacotes no destino
Limiar de satisfação	**Menor ou igual a 0,5%**
Sanções	TPP maior do que o valor contratado = Multa moratória de 2% sobre o valor mensal do circuito por dia que exceder o limiar de satisfação. Limitada a 10% do valor
	mensal do circuito. Superado esse limite, será aplicada a sanção estabelecida no item 20 deste TERMO, sem prejuízo à aplicação da multa moratória.
Relatórios de Níveis de Serviço	Para aferição destes índices, a CONTRATADA se compromete a prover acesso aos aplicativos de gerência e estatística do enlace, através de usuário e senha e disponibilizar gráfico de perda de pacotes com valor de escala mínimo não superior a 5 (cinco) minutos

10.5.2.6. Indicador de Taxa de Erro de Bit

TAXA DE ERRO DE BIT (TxErr)	
ITEM	**DESCRIÇÃO**

Finalidade	A Taxa de Erro de Bit (TxErr) é definida como a relação entre a quantidade de bits corretamente transmitidos para cada bit transmitido com erro no enlace pertencente a rede de acesso. A taxa de erro de bit deverá ser medida por solicitação do CONTRATANTE.
Início de vigência	Data do Termo de Recebimento Definitivo (TRD)
Periodicidade	Medições diárias e constantes, sobretudo em horários de maior tráfego. Sempre que a CONTRATANTE julgar necessário, poderá ser solicitada a medição da Taxa de Erro de Bit fim a fim, através de equipamento de teste especializado.
Cálculo	**TxErr = BErr / BTot** Onde: TxErr: Taxa de Erro de Bit Berr = Número de bits enviados com erro no período de aferição (5 minutos) BTot = Número total de bits enviados no período de aferição (5 minutos)
Limiar de satisfação	**Taxa de Erro de Bit – BER (bits/s): ≤ 1 x 10^{-7}.**
Sanções	TxErr maior do que o valor contratado = Multa moratória de 2% sobre o valor mensal do circuito por dia que exceder o limiar de satisfação. Limitada a 10% do valor mensal do circuito. Superado esse limite, será aplicada a sanção estabelecida no item 20 deste TERMO, sem prejuízo à aplicação da multa moratória.
Relatórios de Níveis de Serviço	A CONTRATADA deverá disponibilizar, além de relatórios mensais, relatórios em sua ferramenta *web* com os valores das medições realizadas durante o período.

10.5.2.7. Indicador de nível de latência

NÍVEL DE LATÊNCIA	
ITEM	**DESCRIÇÃO**
Finalidade	Garantir que o retardo do circuito contratado esteja dentro de uma margem aceitável.
Instrumento de medição	envio de mensagens ICMP Echo Request, com tamanho de pacote de 64 bytes (incluindo o cabeçalho do pacote IP). Este indicador será aferido a cada intervalo de 5 minutos.
Início de vigência	Data do Termo de Recebimento Definitivo (TRD)
Periodicidade	Medições diárias e constantes, sobretudo em horários de maior tráfego, e Sob demanda, com apresentação de relatório do intervalo solicitado.
Limiar de	**Máximo de 65ms**
satisfação	
Sanções	Multa moratória de 2% sobre o valor mensal do circuito por dia que exceder o limiar de satisfação. Limitada a 10% do valor mensal do circuito. Superado esse limite, será aplicada a sanção estabelecida no item 20.2.1 deste TERMO, sem prejuízo à aplicação da multa moratória.

Relatórios de Níveis de Serviço	A CONTRATADA deverá disponibilizar, além de relatórios mensais, relatórios em sua ferramenta *web* com os valores das medições realizadas durante o período.

10.5.2.8. Indicador de Tempo de Atendimento e Reparo

PRAZOS GERAIS PARA ATENDIMENTO E REPARO (TAR)	
ITEM	**DESCRIÇÃO**
Finalidade	Garantir um intervalo de tempo máximo para reparo/restabelecimento de um circuito inoperante.
Instrumento de medição	Software de Monitoramento de Rede
Início de vigência	Data do Termo de Recebimento Definitivo (TRD)
Cálculo	**TAR (h)**= Somatório do tempo excedido em cada evento no mês.
Sanções	TAR >0 = Multa moratória de 1% sobre o valor mensal do circuito a cada 1 hora. Limitada a 10% do valor mensal do circuito. Superado esse limite, será aplicada a sanção estabelecida no item 20.2.1 deste TERMO, sem prejuízo à aplicação da multa moratória.
Observações	A CONTRATADA deverá disponibilizar mensalmente à CONTRATANTE, relatórios com o Tempo de atendimento e reparo, totalizados e apresentados mensalmente por nível de severidade.

10.5.2.9. Indicador de alerta e mitigação de ataques de negação de serviço

ALERTA E MITIGAÇÃO DE ATAQUES DoS e DDoS	
ITEM	**DESCRIÇÃO**
Finalidade	Garantir um intervalo de tempo máximo para emissão de alerta e mitigação de ataques de negação de serviço.
Início de vigência	Data do Termo de Recebimento Definitivo (TRD)
Limiar de satisfação	**Tempo de emissão de alerta de ataque (EAA**) ≤ 15 min., a contar da detecção da anomalia **Tempo de início de mitigação de ataque (MA)** ≤ 15 min., a contar da emissão do alerta
Cálculo	**TEEAA = Tempo excedido de emissão de alerta de ataque (min.)** **TEMA = tempo excedido de início de mitigação de ataque (min.)** **TEAM = tempo excedido de alerta e mitigação de ataque Dos e DDoS (min.)** **TEAM = TEEAA + TEMA**
Sanções	TEAM>0: Multa de 1% sobre o valor mensal do circuito a cada minuto excedido.
Observações	A CONTRATADA deverá disponibilizar mensalmente à CONTRATANTE relatórios com ocorrências de ataques DDoS ocorridos no mês anterior.

10.5.3. RESUMO DOS LIMITES DE SATISFAÇÃO DO ACORDO DE NÍVEL DE SERVIÇO

Ocorrência	**SLA**

Disponibilidade dos links de dados e Internet	Para todos os lotes: 99,7% Mensal
Perda de Pacotes máxima permitida	Para todos os lotes: ≤0,5%
Taxa de erro de bit	Para todos os lotes: ≤ 1×10^{-7}
Latência máxima permitida	Para todos os lotes: ≤ 65ms
Atendimento e reparo	TAR(h)=0 (Somatório de tempo excedido de atendimento, baseado nos níveis de severidade elencados no item 10.5)
Ataques de negação de serviço distribuído (DDOS)	Tempo de emissão de alerta de ataque (EAA) ≤ 15 min Tempo de início de mitigação de ataque (MA) ≤ 15 min.

11. GERENCIAMENTO DE NÍVEL DE SERVIÇO

11.1. A CONTRATADA deverá disponibilizar um sistema de monitoração “on line”, que apresente gráficos de desempenho em tempo real, que seja acessado via endereço “web” (utilizando protocolo http ou https), com usuário e senha específico, para que os responsáveis da CONTRATANTE possam monitorar a utilização do serviço objeto desse edital, com no mínimo as seguintes informações:

11.1.1. Sobre as características físicas do ponto de acesso:

11.1.1.1. Utilização de banda do ponto de acesso, informando o volume tráfego (em bits e pacotes);
11.1.1.2. O percentual de descarte de pacotes e quadros para o ponto de acesso;
11.1.1.3. Taxa média de ocupação do ponto de acesso;
11.1.1.4. O tempo de retardo de ida e volta entre o ponto de acesso e o backbone da prestadora;
11.1.1.5. Percentual de pacotes com erros do ponto de acesso;
11.1.1.6. Percentual de disponibilidade mensal, considerando sempre o período de faturamento mensal.

11.1.2. Sobre incidentes (indisponibilidade ou degradação do acesso) ocorridos nos circuitos:

11.1.2.1. Dia e hora da ocorrência;
11.1.2.2. Relação de todos os chamados abertos;
11.1.2.3. Duração da ocorrência/falha;
11.1.2.4. Sua causa;
11.1.2.5. Solução dada ao ocorrido;
11.1.2.6. Percentual de disponibilidade no período.

11.2. A CONTRATADA deverá ser capaz de prover envio automático de e-mails e/ou SMS com as informações sobre a evolução dos chamados, para os representantes da equipe técnica do Tribunal. Os dados de envio dos emails/SMS deverão ser conseguidos junto à Diretoria de Tecnologia da Informação deste Tribunal.

12. QUALIFICAÇÃO TÉCNICA

12.1. A vencedora do certame deverá apresentar:

12.1.1. Outorga da Agência Nacional de Telecomunicações – ANATEL, que lhe permita fornecer serviços de transmissão de dados objeto deste Termo. Poderá ser apresentada a cópia do extrato de publicação no DOU do Contrato de Concessão ou Termo de Autorização;

12.1.2. Comprovação de possuir vínculo, na data prevista para assinatura do contrato, profissional de nível superior ou outro devidamente reconhecido pela entidade competente, detentor de atestado de responsabilidade técnica por execução de serviços de características semelhantes, limitadas estas às parcelas de maior relevância e valor significativo do objeto da licitação referentes aos serviços técnicos especializados de implantação, operacionalização, gerenciamento e manutenção de soluções integradas na forma de Redes de Telemática (transmissão de dados);

12.1.3. Declaração contendo o nome e a qualificação técnica do profissional referido no item anterior, acompanhada de um ou mais atestados fornecidos por pessoas jurídicas de direito público ou privado, em nome do profissional, devidamente acompanhados da respectiva Certidão de Acervo Técnico (CAT) emitida pelo CREA, para comprovação dos requisitos solicitados;

12.1.4. Certidão de Registro ou Inscrição dos seus Responsáveis Técnicos para com a entidade profissional competente (CREA);

12.1.5. Atestado(s) de capacidade técnica, expedido(s) por pessoa jurídica de direito publico ou privado, que comprove(m) que a licitante tenha executado, ou esteja executando, satisfatoriamente serviço de Circuito de Internet, objeto desta licitação;

12.1.6. No caso de atestados emitidos por empresa da iniciativa privada, não serão considerados aqueles emitidos por empresa pertencente ao mesmo grupo empresarial da licitante, sua subsidiária, controlada ou controladora e por empresa na qual haja pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da licitante.

12.1.7. Declaração da empresa fornecedora do link de acesso à Internet através do seu backbone IP, informando que a licitante possui interligação direta , através de canais dedicados, a pelo menos 2 (dois) outros AS nacionais e a pelo menos 2 (dois) AS internacionais, sendo que deverá indicar o(s) Circuito(s) de Internet que comprove(m) o(s) registro(s) desse(s) AS(s) em organismo(s) nacional(is) e internacional(is) respectivamente. As bandas de saída entre os AS (nacional e internacional) deverão somar pelo menos 5 (cinco) Gbps;

12.1.8. Comprovação do serviço Anti-DDoS através de apresentação de declaração da empresa fornecedora e cópia de contrato com Scrubbing Center no Brasil onde este comprove:

12.1.8.1. possuir no mínimo 1 centro de limpeza nacional e 3 centros de limpeza internacional com capacidade de ingestão igual ou superior ao descrito no tópico 4.2 (Requisitos técnicos do serviço de Anti-DDOS);

12.1.8.2. possuir aderência a todos os parâmetros técnicos descritos no tópico 4.2.

12.1.9. Para licitante que possua Scrubbing Center no Brasil próprio, apresentar declaração do fabricante da solução Anti-DDoS proposta, comprovando que a solução atende as especificações do Termo de Referência;

12.2. A ARREMATANTE deverá apresentar documentação técnica da solução, descrevendo:

a) diagrama de fornecimento da solução;
b) relação detalhada de equipamentos ativos que serão fornecidos e instalados, indicando marca e modelo de cada equipamento;
c) cronograma detalhado de execução da implantação inicial;
d) projeto de encaminhamentos e implantação inicial do serviço, indicando trajeto da(s) fibra(s) óptica(s) entre o backbone da rede da LICITANTE até o edifício-sede da CONTRATANTE;

12.3. A ARREMATANTE deverá apresentar documentos de especificações técnicas oficiais dos fabricantes que comprovem que os equipamentos da solução fornecida atende integralmente aos requisitos exigidos neste Termo de Referência;

12.4. Todos os documentos acima, fornecidos pela ARREMATANTE, serão analisados pela Equipe Técnica da CONTRATANTE para validação e homologação da solução;

12.5. Será inabilitado o ARREMATANTE que deixar de apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste termo de referência.

13. DA HABILITAÇÃO

13.1. Habilitação Jurídica

a) Registro comercial, no caso de empresa individual;
b) Ato constitutivo (estatuto ou contrato social em vigor), devidamente registrado no órgão competente, em se tratando de sociedades comerciais (empresariais), e, no caso de sociedade por ações, acompanhado de documentos comprobatórios da eleição dos atuais administradores;
c) Decreto de autorização, em se tratando 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.
d) Declaração que comprove a inexistência de vínculo dos membros da contratada com este Tribunal, que evidencie a prática de nepotismo, conforme atesta o artigo 2º, V, e artigo 3º da Resolução 7/2005 e/ou artigo 4º da resolução 156/2012, ambas do CNJ.
e) Declaração de inexistência de fato posterior que impeça a empresa de contratar com a administração, nos moldes do prescrito no artigo 32, § 2º, da Lei nº 8.666/93.
f) Declaração em que ateste cumprir o prescrito no art. 27, V, da Lei n° 8.666/93, declarando não empregar menores trabalhando de modo ilícito.

13.2. Qualificação Econômico-Financeira:

a) Certidão negativa de falência, concordata e recuperação judicial de empresa, expedida pelo Cartório de Distribuição da sede da licitante, expedida nos últimos 30 dias que anteceder a abertura da licitação.

13.3. Regularidade Fiscal:

a) Prova de Inscrição no Cadastro Nacional de Pessoas Jurídicas – CNPJ.
b) Certidão Conjunta Negativa de Débitos Relativos a Tributos Federais e à Dívida Ativa da União, emitida pela Receita Federal;
c) Prova de regularidade para com o Instituto Nacional do Seguro Social (INSS), através da apresentação da Certidão Negativa de Débitos (CND), emitida pelo Instituto Nacional do Seguro Social-INSS e/ou Receita Federal;
d) Prova de regularidade junto ao Fundo de Garantia por Tempo de Serviço, através da apresentação do Certificado de Regularidade do FGTS (CRF), emitido pela Caixa Econômica Federal;
e) Prova de regularidade para com a Fazenda Municipal da sede da empresa, expedidas pelos órgãos competentes.
f) Prova de regularidade dos Débitos Trabalhista, expedidas pelos órgãos competentes.

14. LOCAIS DE PRESTAÇÃO DOS SERVIÇOS

O serviços, objetos dos Lotes 1 e 2, deverão ser prestados na sede do Tribunal de Justiça do Estado de Alagoas, Praça Marechal Deodoro, 319, Centro, Maceió-AL.

15. DA CONFIDENCIALIDADE DA INFORMAÇÃO

15.1. A CONTRATADA deverá manter sigilo em relação aos dados, informações ou documentos que tomar conhecimento em decorrência da prestação dos serviços objeto desta contratação, bem como se submeter às orientações e normas internas de segurança da informação vigentes, devendo orientar seus empregados e/ou prepostos nesse sentido, sob pena de responsabilidade civil, penal e administrativa. O compromisso será oficializado por assinatura de termo de confidencialidade e sigilo emitido pela contratada.

15.2. A CONTRATADA deverá cumprir e atender aos padrões de segurança e controle para acesso e uso das instalações da CONTRATANTE, zelando por sua integridade, preservando o sigilo e a confidencialidade de todos os dados e informações pertinentes aos serviços prestados, de acordo com a legislação vigente que dispõe sobre a categoria dos documentos públicos sigilosos e o acesso a eles.

15.3. A CONTRATADA não deverá acessar ou manipular qualquer informação confiada sem prévia autorização da CONTRATANTE.

16. OBRIGAÇÕES DA CONTRATADA

16.1. Entregar os serviços contratados, em prazo não superior ao máximo estipulado neste edital. Caso o atendimento não seja feito dentro do prazo, a **CONTRATADA** ficará sujeita à multa estabelecida neste edital;

16.2. Manter, durante toda a vigência do contrato, registro dos eventos que porventura tenham provocado interrupções nas portas de comunicação, a fim de justificar a não consideração de períodos de indisponibilidade perante o Tribunal, sempre de acordo com o previsto neste Termo de Referência;

16.3. Cumprir o Acordo de Nível de Serviço (SLA) estabelecido no item 10 deste Termo de Referência;

16.4. Fornecer, sem qualquer ônus adicional à **CONTRATANTE**, quaisquer componentes adicionais de hardware ou software necessários ao perfeito funcionamento dos itens ofertados, mesmo que não constem do contrato;

16.5. Submeter à aprovação deste Tribunal toda e qualquer alteração ocorrida nas especificações, em face de imposições técnicas, de cunho administrativo ou legal;

16.6. Responsabilizar-se por todos os encargos sociais, trabalhistas, previdenciários, fiscais e comerciais, tributos de qualquer espécie que venham a ser devido em decorrência da execução deste instrumento, bem como custos relativos ao deslocamento e estada de seus profissionais, caso existam;

16.7. Responsabilizar-se pelos danos causados diretamente à **CONTRATANTE** ou a terceiros, decorrentes de sua culpa ou dolo, ação ou omissão, quando da execução do contrato, não excluindo ou reduzindo essa responsabilidade à fiscalização ou o acompanhamento realizado pela **CONTRATANTE**.

16.8. Arcar com o pagamento de eventuais multas aplicadas por quaisquer autoridades federais, estaduais e municipais, em consequência de fato a ela imputável e relacionado com este contrato.

16.9. Arcar com todos os prejuízos advindos de perdas e danos. Incluindo despesas judiciais e honorários advocatícios resultantes de ações judiciais, a que a CONTRATANTE for compelida a responder em decorrência desta contratação.

16.10. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas no instrumento convocatório, para a contratação.

16.11. Manter seus funcionários, quando nas dependências da CONTRATANTE, sujeitos às normas internas deste (segurança, disciplina), porém sem qualquer vínculo empregatício com o Órgão.

16.12. Possibilitar a fiscalização deste Tribunal, no tocante à verificação das especificações exigidas neste Termo de Referência, prestando todos os esclarecimentos solicitados e atendendo às reclamações procedentes, caso ocorram;

16.13. Comunicar à **CONTRATANTE**, de imediato e por escrito, qualquer irregularidade verificada durante a execução do contrato, para a adoção das medidas necessárias à sua regularização.

16.14. Manter, durante toda a vigência do contrato, as condições de habilitação consignadas neste termo.

16.15. Indicar um de seus empregados para atuar como preposto, cabendo a ele:

a. Interagir com a CONTRATANTE no que se refere ao contrato;
b. Acompanhar o cumprimento do ANS;
c. Adotar medidas administrativas e técnicas para o cumprimento do ANS;

d. Garantir a veracidade das informações fornecidas à CONTRATANTE;
e. Representar a CONTRATADA junto a CONTRATANTE;

17. PRAZO DO CONTRATO

O período para execução do serviço será de 12 (doze) meses, podendo ser prorrogada conforme artigo 57, II Lei 8.666/93.

18. FISCALIZAÇÃO E GESTÃO DO CONTRATO

- Os serviços serão acompanhados e fiscalizados por servidor do Tribunal especialmente designado pela autoridade competente, que terá seu substituto legal, cabendo-lhes as atribuições e responsabilidades do artigo 67 da Lei nº. 8.666/93, os quais serão auxiliados, ou não, por empresa terceirizada a ser contratada.
- Caberá ao Fiscal do Contrato:
  - Emitir a ordem de serviço do objeto contratual;
  - Verificar a execução do objeto contratual, visando garantir a qualidade desejada; ○ Atestar e encaminhar as notas fiscais ao setor competente para autorizar os pagamentos; ○ Dar imediata ciência aos seus superiores e ao órgão de controle, dos incidentes e ocorrências

  da execução que possam acarretar a imposição de sanções ou a rescisão contratual; ○ Adotar, junto a terceiros, as providências necessárias para a regularidade da execução do

  contrato.
- As decisões e providências que ultrapassarem a competência da fiscalização deverão ser solicitadas pelo fiscal à autoridade competente, para a adoção das medidas que julgar necessárias.
- A fiscalização será exercida pelo Contratante e não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por quaisquer irregularidades, e, na sua ocorrência, não implica co-responsabilidade do Poder Público ou de seus agentes e prepostos. Ao Contratante se reserva o direito de rejeitar a execução do objeto contratual prestado, se em desacordo com os termos do edital.
- Caberá ao Gestor do contrato:
  - Proceder à prorrogação de Contrato junto à Autoridade Competente (ou às instâncias competentes), que deve ser providenciada antes de seu término, reunindo as justificativas competentes;
  - Proceder à comunicação para abertura de nova licitação à área competente, antes de findo o

  estoque de bens e/ou a prestação de serviços e com antecedência razoável; ○ Proceder ao pagamento de Faturas/Notas Fiscais;
  - Proceder à comunicação ao setor competente sobre quaisquer problemas detectados na

  execução contratual, que tenham implicações na atestação; ○ Proceder à Comunicar as irregularidades encontradas: situações que se mostrem

desconformes com o Contrato e com a Lei; ○ Comunicar as irregularidades encontradas: situações que se mostrem desconformes com o

Contrato e com a Lei; ○ Exigir somente o que for previsto no Contrato. Qual quer alteração de condição contratual

deve ser submetida ao superior hierárquico, acompanhada das justificativas pertinentes ○ Cuidar das alterações de interesse da Contratada, que deverão ser por ela formalizadas e

devidamente fundamentadas, principalmente em se tratando de pedido de reequilíbrio econômicofinanceiro ou repactuação. No caso de pedido de prorrogação de prazo, deverá ser comprovado o fato impeditivo da execução, o qual, por sua vez, deverá corresponder àqueles previstos no parágrafo primeiro do artigo 57 da Lei 8.666/93 e alterações; ○ Elaborar ou solicitar justificativa técnica, quando couber, com vistas à alteração unilateral do

Contrato pela Administração;

- ○ Alimentar os sites do Contratante, os sistemas informatizados deste Poder,

responsabilizando-se por tais informações, inclusive sempre quando cobradas/solicitadas; ○ Negociar o Contrato sempre que o mercado assim o exigir e quando da sua prorrogação, nos

termos da Lei; ○ Procurar auxílio junto às áreas competentes em caso de dúvidas técnicas, administrativas ou

jurídicas;

- ○ Documentar nos autos todos os fatos dignos de nota;
- ○ Deflagrar e conduzir os procedimentos de finalização à Contratada, com base nos termos Contratuais, sempre que houver descumprimento de suas cláusulas por culpa da Contratada, acionando as instâncias superiores e/ou os Órgãos Públicos competentes quando o fato exigir.
- ○ A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada,

inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em co-responsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

- ○ O representante da Administração anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

 Fica designado o(a) Servidor(a)_____, lotado(a) no _____, matrícula _____, e em sua ausência, o seu substituto legal, (quando houver) para, nossa ordem, exercerem a gestão/fiscalização do contrato, devendo o mesmo representar este Tribunal perante a contratada e zelar pela boa execução do objeto pactuado, nas atividades de gestão, fiscalização e controle constantes no Ato Normativo nº 025/2010".

19. OBRIGAÇÕES DO CONTRATANTE:

19.1. O CONTRATANTE obriga-se a:

19.1.1. Propiciar todas as facilidades indispensáveis à boa execução do fornecimento dos serviços objeto deste ajuste, inclusive permitir o livre acesso do responsável CONTRATADO às dependências do CONTRATANTE, desde que devidamente identificados;

19.1.2. Atestar a execução do objeto do presente ajuste por meio do gestor de contrato;

19.1.3. Efetuar o pagamento ao CONTRATADO de acordo com as condições de preço e prazos estabelecidos neste termo de referência;

19.1.4. Aplicar as penalidades por descumprimento do contrato;

19.1.5. Fiscalizar para que, durante a vigência do contrato, sejam mantidas as condições de habilitação e qualificação exigidas na licitação.

19.1.6. CONTRATANTE e CONTRATADA deverão manter registros escritos dos chamados de assistência técnica, onde constem sua data e hora, nome do funcionário da CONTRATANTE responsável pela comunicação, nome do empregado da CONTRATADA que a receber e uma descrição resumida do defeito;

19.1.7. O aceite dos serviços prestados será dado pelo fiscal do contrato devendo a CONTRATADA refazer os serviços não aprovados sem quaisquer ônus adicionais para a CONTRATANTE.

20. DAS SANÇÕES ADMINISTRATIVAS

20.1. Pelo descumprimento total ou parcial do objeto deste certame e/ou pelo retardamento na sua execução, a Administração do CONTRATANTE poderá, garantida a prévia defesa da Contratada no prazo de 05 (cinco) dias úteis, aplicar à CONTRATADA as seguintes sanções:

20.1.1. ADVERTÊNCIA - sempre que forem observadas irregularidades de pequena monta para os quais tenha concorrido;

20.1.2. MULTA MORATÓRIA – de 2% (dois por cento) por dia de atraso injustificado sobre o valor total do circuito contratado, até o limite de 20 (vinte) dias, podendo esse valor ser abatido no pagamento a que fizer jus a contratada, ou ainda, quando for o caso, cobrado administrativa ou judicialmente;

20.2. Decorridos 20 (vinte) dias úteis sem que a CONTRATADA tenha iniciada a execução da obrigação assumida, estará caracterizada a inexecução total do contrato, ensejando a sua rescisão unilateral e a aplicação das penalidades previstas em lei e no contrato;

20.2.1. MULTA COMPENSATÓRIA - de 10% (dez por cento) sobre o valor total do contrato, em caso de inexecução total.

20.2.2. Em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida ou sobre o valor mensal do contrato quando não for possível aferir valor proporcional.

20.3. SUSPENSÃO TEMPORÁRIA de participação em licitação e impedimento de contratar com a Administração, por prazo não superior a 02 (dois) anos; e

20.4. DECLARAÇÃO DE INIDONEIDADE para licitar ou contratar com a administração pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o contratado ressarcir a administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base na alínea anterior.

20.5. O Contratante aplicará as demais penalidades previstas nas Leis 10.520/2002 e 8.666/93 e no Decreto nº. 5450/2005, sem prejuízo das responsabilidades penal e civil;

20.6. O licitante que ensejar o retardamento da execução do certame, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo, fizer declaração falsa ou cometer fraude fiscal, garantida o direito prévio da citação e da ampla defesa, ficará impedido de licitar e contratar com a Administração Pública, pelo prazo de até 05 (cinco) anos, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade;

20.7. A recusa injustificada da licitante vencedora em assinar o Contrato, dentro do prazo de 05 (cinco) dias após convocada pelo TJ-AL, caracteriza o descumprimento total da obrigação assumida, sujeitando-a, além da penalidade prevista no subitem 20.1, multa correspondente a 20% (vinte por cento) do valor estimado da contratação;

20.8. Em qualquer situação, será assegurado à CONTRATADA o amplo direito de defesa.

21. DO PAGAMENTO

21.1 Os pagamentos serão efetuados, em moeda corrente nacional, em até 10 (dez) dias úteis após o recebimento definitivo, mediante apresentação da seguinte documentação:

21.1.1 nota fiscal/fatura discriminativa, em via única, devidamente atestada pelo GESTOR DO CONTRATO;

21.1.2 CND – Certidão Negativa de Débitos para com a Previdência Social;

21.1.3 CRF – Certificado de Regularidade de FGTS, expedido pela Caixa Econômica Federal;

21.1.4 Certidão Conjunta Negativa de Débitos Relativos a Tributos Federais, expedida pela Receita Federal do Brasil;

21.1.5 Certidão negativa de débitos trabalhistas, emitido pelo TST – Tribunal Superior do Trabalho;

21.1.6 Prova de regularidade para com a Fazenda Estadual ou Municipal do domicílio ou sede da licitante;

21.2 Considera-se para efeito de pagamento o dia da entrega da O.B. na unidade bancária.

21.3 A apresentação de nota fiscal/fatura com incorreções ou desacompanhada da documentação requerida, implicará a sua devolução à Empresa Contratada para regularização, devendo o prazo de pagamento ser contado a partir da data de sua reapresentação;

21.4 Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido de alguma forma para tanto, fica convencionado que a taxa de compensação financeira devida pelo

Tribunal de Justiça, entre a data de pagamento prevista para o pagamento e o efetivo adimplemento da parcela, será aquela resultante da aplicação da seguinte fórmula: **EM=IxNxVP**

Onde:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento; VP = Valor da parcela a ser paga;

I = Índice de atualização financeira = 0,00016438, assim apurado:

$$I=TX \quad I = \frac{(6/100)}{365} \quad I = 0,00016438$$

TX = Percentual da taxa anual = 6%

21.5 O cumprimento ao disposto na legislação em vigor, Tribunal de Justiça reterá na fonte os tributos pertinentes às áreas federal, estadual, municipal, e previdenciários que incidirem sobre os pagamentos que efetuar a pessoa jurídica, conforme o caso.

21.6 Poderá ser deduzida do valor da Nota Fiscal de Serviços/Fatura, multa imposta pelo Tribunal de Justiça, se for o caso.

22. DA ATA DE REGISTRO DE PREÇOS

22.1. Homologado o resultado da licitação, o Órgão Gerenciador, respeitadas a ordem de classificação e a quantidade de fornecedores a serem registrados, convocará os interessados para assinatura da Ata de Registro de Preços que, após cumpridos os requisitos de publicidade, terá efeito de compromisso de fornecimento nas condições estabelecidas.

22.2. As convocações de que tratam o item anterior deverão ser atendidas no prazo máximo de 05 (cinco) dias úteis, prorrogável apenas 01 (uma) única vez a critério do Gerenciador, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas no subitem 26.1 deste edital.

22.3. A ata de registro de preços firmada com os licitantes fornecedores observará as disposições constantes na minuta, sendo vedado efetuar acréscimos nos quantitativos fixados, inclusive o acréscimo de que trata o § 1º do art. 65 da Lei nº 8.666/93, sendo possível a revisão e o cancelamento dos preços registrados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos serviços ou bens registrados, observadas as disposições dos artigos 16, 17 e 18 do Decreto Estadual nº 29.342/2013.

22.4. Sempre que o licitante vencedor não atender à convocação, nos termos definidos no item 12.2, é facultado à Administração, dentro do prazo e condições estabelecidos, convocar remanescentes, na ordem de classificação, para fazê-lo em igual prazo e nas mesmas condições, ou revogar o item específico respectivo, ou a licitação.

22.5. Ao assinar a Ata de Registro de Preços, a adjudicatária obriga-se a fornecer os bens a ela adjudicados, conforme especificações e condições contidas neste edital, em seus anexos e também na proposta apresentada, prevalecendo, no caso de divergência, as especificações e condições do edital.

23. DA UTILIZAÇÃO DA ATA DE REGISTRO DE PREÇOS POR ÓRGÃOS OU ENTIDADES NÃO PARTICIPANTES

23.1. A Ata de Registro de Preços, durante sua vigência, poderá ser utilizada por qualquer órgão ou entidade da Administração Pública que não tenha participado do certame licitatório, mediante prévia consulta ao órgão gerenciador, desde que devidamente comprovada a vantagem, nos termos do artigo 21 do Decreto Estadual nº 29.342/2013, exceto os órgãos e entidades da Administração Pública Federal, conforme dispõe o Parágrafo único do art. 22 do Decreto Estadual nº 29.342/2013.

23.2. Os órgãos e entidades que não participarem do registro de preços, quando desejarem fazer uso da Ata de Registro de Preços, deverão manifestar seu interesse junto ao órgão gerenciador da Ata, para que este se manifeste sobre a possibilidade de adesão.

23.3. As contratações adicionais a que se refere o artigo 21 do Decreto Estadual nº 29.342/2013, não poderão exceder, por órgão ou entidade, a 100% (cem por cento) dos quantitativos dos itens registrados na Ata de Registro de Preços, limitadas ao quíntuplo do quantitativo de cada item registrados na ata de registro de preços para o órgão gerenciador e órgãos participantes, independente do número de órgãos não participantes que aderirem, nos termos do art.21, § 4º do Decreto Estadual nº 29.342/2013.

24. DAS ALTERAÇÕES NA ATA DE REGISTRO DE PREÇOS

24.1. O preço registrado poderá ser revisto em decorrência de eventual redução daqueles praticados no mercado, ou de fato que eleve o custo dos serviços ou bens registrados, cabendo ao Tribunal (órgão gerenciador) promover as necessárias negociações junto aos fornecedores.

24.2. Quando o preço inicialmente registrado, por motivo superveniente, tornar-se superior ao praticado no mercado, o Contratante deverá:

24.2.1. Convocar o fornecedor visando à negociação para redução de preços e sua adequação ao praticado pelo mercado;

24.2.2. Frustrada a negociação, o fornecedor será liberado do compromisso assumido; e

24.2.3. Convocar os demais fornecedores visando igual oportunidade de negociação.

24.2.4. Quando o preço de mercado tornar-se superior aos preços registrados e o fornecedor, mediante requerimento devidamente comprovado, não puder cumprir o compromisso, o Contratante poderá:

24.2.5. Liberar o fornecedor do compromisso assumido, sem aplicação da penalidade, confirmando a veracidade dos motivos e comprovantes apresentados, e se a comunicação ocorrer antes do pedido de fornecimento; e

24.2.6. Convocar os demais fornecedores visando igual oportunidade de negociação.

24.3. Não havendo êxito nas negociações, o Tribunal (órgão gerenciador) deverá proceder à revogação da Ata de Registro, adotando as medidas cabíveis para obtenção da contratação mais vantajosa.

24.4. A Ata de Registro de Preços poderá gerar contrato a interesse da administração.

25. DO CANCELAMENTO DO REGISTRO DE PREÇOS

25.1. O fornecedor terá seu registro cancelado nas hipóteses previstas na Lei Federal n° 8.666, de 21 de junho de 1993, ou quando:

a. descumprir as condições da Ata de Registro de Preços;
b. não retirar a respectiva nota de empenho ou instrumento equivalente, no prazo estabelecido pela Administração, sem justificativa aceitável;
c. não aceitar reduzir o seu preço registrado, na hipótese de este se tornar superior àqueles praticados no mercado;
d. tiver presentes razões de interesse público;
e. por acordo entre as partes, quando o fornecedor, mediante solicitação por escrito aceita pela Administração, comprovar estar impossibilitado de cumprir as exigências do edital que deu origem ao registro de preços ou de cumprir as cláusulas e condições do compromisso para futura e eventual contratação.

25.2. O cancelamento do registro de preços será feito no processo que lhe deu origem, devendo sua comunicação ser feita, ao fornecedor contratado, por correspondência com recibo de entrega, juntando-se comprovante nos respectivos autos.

25.3. No caso de ser ignorada ou inacessível a sede ou o domicílio do fornecedor, a comunicação será feita por publicação no Diário de Justiça Eletrônico, por uma vez, e afixação no local de costume do órgão gerenciador, considerando-se cancelado o registro na data considerada como de publicação no Diário da Justiça Eletrônico, que respeitará a forma do art. 4º, da Lei Federal nº 11.419, de 19 de dezembro de 2006.

25.4. Em qualquer das hipóteses de cancelamento do registro de preços previstas neste item, é facultada à Administração a aplicação das penalidades.

25.5. O cancelamento de registro nas hipóteses previstas, assegurados o contraditório e a ampla defesa, será formalizado por despacho da autoridade competente do órgão gerenciador.

25.6. O fornecedor poderá solicitar o cancelamento do seu registro de preços na ocorrência de fato superveniente que venha a comprometer a perfeita execução contratual, decorrente de caso fortuito ou de força maior devidamente comprovado.

25.7. A solicitação do fornecedor para cancelamento do preço registrado deverá ser formulada com antecedência mínima de 30 (trinta) dias, facultada à Administração a aplicação das penalidades previstas no instrumento convocatório, assegurada defesa prévia do fornecedor, nos termos da Lei Federal n° 8.666, de 21 de junho de 1993.

26. DA VIGÊNCIA DA ATA DE REGISTRO DE PREÇOS

26.1. A Ata de Registro de Preços vigerá pelo prazo de 12 (doze) meses, a contar da data de sua assinatura.

27. DO REAJUSTE

27.1. É vedado qualquer reajustamento de preços durante o prazo de vigência do registro de preços.

27.2. Fica ressalvada desta vedação a revisão de preços efetuada conforme os artigos 16, 17 e 18 do Decreto Estadual nº 29.342/2013.

28. DAS CONSIDERAÇÕES FINAIS

- O presente vincula-se ao instrumento convocatório e à proposta da Contratada, sendo os casos omissos resolvidos de acordo com a legislação aplicável à espécie.
- A Contratada fica obrigada a manter, durante toda a execução do contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições de habilitação e qualificação exigidas para a contratação.
- Não será permitida a subcontratação do fornecimento objeto do presente ajuste, exceto dos treinamentos técnicos que poderão ser subcontratados de Centro de Treinamentos Autorizados ou dos próprios fabricantes.
- O CNPJ do FUNJURIS é 01.700.776/0001-87.
- Ao contratado poderá ser acrescido ou diminuído o objeto do fornecimento dentro dos limites estabelecidos na lei 8.666/93.

Maceió, 01 de fevereiro de 2017.

Christiano Rossini Martins Costa
Analista Judiciário – Especialidade Análise de Sistemas Integrante
Técnico do Projeto