**ANEXO I DO TERMO DE REFERÊNCIA**

**ESPECIFICAÇÕES TÉCNICAS**

1. **ESPECIFICAÇÕES TÉCNICAS PARA O GRUPO 1**
   1. **DEFINIÇÕES GERAIS**
      1. Serviços de rede de longa distância (WAN) para manter a interligação da Sede do TRT7, localizada em Fortaleza-CE, com suas respectivas unidades remotas (fóruns e varas do trabalho) localizadas no interior do Estado do Ceará, por meio da disponibilização de recursos de conectividade dimensionados para suprir as demandas de tráfego de dados da rede corporativa de comunicação do TRT7 utilizando tecnologia VPN IP/MPLS.
      2. Não fará parte do escopo dos serviços do Grupo 1 qualquer acesso à internet.
      3. O fornecimento mensal de conexão da rede interna da localidade remota à Sede do TRT7, por meio de LINK MPLS, deverá prover conectividade com alta qualidade e performance, por meio de serviço de IP, em modo full duplex de uso ilimitado, isto é, a taxa de transmissão fornecida deverá ser simétrica suportando as mesmas velocidades, tanto na entrada de dados (download) quanto na saída (upload), simultaneamente.
      4. A CONTRATADA deverá instalar os links MPLS com as características e nos endereços especificados abaixo:

| item | banda mínima garantida | tipo de nó | unidade do TRT7 |
| --- | --- | --- | --- |
| 1 | 50 Mbps | NS | **Fórum do Trabalho de Caucaia**  Endereço: Av. Contorno Sul, s/n – Planalto Caucaia  CEP: 61.605-490 Caucaia/CE |
| 2 | 50 Mbps | NS | **Fórum do Trabalho de Maracanaú**  Endereço: Rua Edson Queiroz, N° 480  Bairro: Piratininga  CEP: 61.905-155 Maracanaú/CE |
| 3 | 50 Mbps | NS | **Fórum do Trabalho da Região do Cariri**  Endereço: Rua Rafael Malzoni, 761  Bairro: São José  CEP: 63.024-030 - Juazeiro do Norte - CE |
| 4 | 50 Mbps | NS | **Fórum do Trabalho de Sobral**  Endereço: Av. Lúcia Sabóia, nº 500 - Centro  CEP: 62.320 - 000 - Sobral/CE |
| 5 | 30 Mbps | NS | **Vara do Trabalho de Aracati**  Endereço: Rua Coronel Alexanzito, 503 - Centro  CEP: 62.800-00 Aracati/CE |
| 6 | 30 Mbps | NS | **Vara do Trabalho de Baturité**  Endereço: Rua Major Pedro Catão, nº 450 - Mondego  CEP: 62.760 - 000 Baturité/CE |
| 7 | 30 Mbps | NS | **Vara do Trabalho de Crateús**  Endereço: Rua Hermínio Bezerra, 801  Bairro: Planalto CE-075  CEP: 63.700 - 000 Crateús/CE |
| 8 | 30 Mbps | NS | **Vara do Trabalho de Iguatu**  Endereço: Rua José de Alencar, 1.155 - Bugi  CEP: 63.500 - 000 Iguatu/CE |
| 9 | 30 Mbps | NS | **Vara do Trabalho de Limoeiro do Norte**  Endereço: Rua Cândido Olímpio de Freitas, nº 1.655 - centro  CEP: 62.930 - 000 L. do Norte/CE |
| 10 | 30 Mbps | NS | **Vara do Trabalho de Pacajus**  Endereço: Av. Vice-Prefeito Expedito Chaves Cavalcante S/N – Cruz das Almas  CEP: 62.870-000 Pacajus/CE |
| 11 | 30 Mbps | NS | **Vara do Trabalho de Quixadá**  Endereço: Rua Tenente Cravo, nº 775  Bairro: Campo Velho  CEP: 63.900 - 000 Quixadá/CE |
| 12 | 30 Mbps | NS | **Vara do Trabalho de São Gonçalo do Amarante**  Endereço: Av. Paulo Costa, S/N, bairro Carioca  CEP: São Gonçalo do Amarante/CE |
| 13 | 30 Mbps | NS | **Vara do Trabalho de Tianguá**  Endereço: Rua Manoel da Rocha Teixeira, 1200  Bairro: Nenê Plácido  CEP: 62.327-445 Tianguá/CE |
| 14 | 30 Mbps | NS | **Vara do Trabalho de Eusébio**  Endereço: Rua Dermeval Carneiro, 115, Centro, Eusébio - CE  CEP: 61760-970 |
| 15 | 400 Mbps | NC | **Tribunal Regional do Trabalho da 7ª Região**  **Prédio Anexo 2:** Rua Vicente Leite, 1.281  CEP 60.170-151 |

Quadro 1. Tipos de links MPLS e endereços

* + 1. A redundância de enlaces e de roteadores deverá ser implementada como se segue:

a) Nó Central (NC): Prédio Sede do Tribunal, concentra todos os enlaces do Tribunal, possui SLA Mensal de 99,8%, conectado exclusivamente por dupla abordagem em fibra ótica, com redundância composta por 2 (dois) conjuntos de enlace e equipamentos CPE e PE, com acessos distintos e atendidos por estações terminais independentes. Cada conjunto deve ter capacidade para atender 100% do nível de serviço contratado para o nó e deve ser configurada de forma que, se houver falha em um conjunto, todo o tráfego será transportado através do conjunto remanescente. Caso o Tribunal possua sua estrutura de comunicação de dados distribuída em mais de um prédio, conectados por rede local de alta velocidade, cada enlace e CPE poderá estar em um endereço diferente. É facultado ao Tribunal optar, durante toda a vigência do contrato, pelo Failover ATIVO/STANDBY ou Failover ATIVO-ATIVO, com balanceamento de carga por pacotes ou conexões.

b) Nó Simples (NS): Unidades remotas do TRT7, possui SLA Mensal de 99,2%, conectado exclusivamente por fibra ótica. Não há redundância de enlace e equipamento CPE.

* + 1. Não haverá aquisição de equipamentos por parte do TRT7. Haverá fornecimento dos mesmos pela CONTRATADA, em regime de comodato, através da prestação de serviços de telecomunicações como parte da solução de VPN IP/MPLS;
    2. Não serão contemplados na especificação: racks, no-breaks e cabeamento. Tais infraestruturas são de responsabilidade do TRT7;
    3. No decorrer da vigência do contrato de prestação, poderá eventualmente haver mudança de endereços das unidades do TRT7 relacionadas, assim como adição de novos endereços.
    4. No caso de mudança de endereços, a CONTRATADA deverá arcar com os respectivos custos de alteração da rede WAN.
    5. Por mudança de endereço entende-se a alteração do local físico de instalação do enlace, podendo esta alteração ocorrer entre quaisquer localidades circunscritas na abrangência do TRT7;
  1. **ESPECIFICAÇÕES MÍNIMAS OBRIGATÓRIAS DOS SERVIÇOS**
     1. A CONTRATADA deverá fornecer, dimensionar, disponibilizar, instalar, configurar, monitorar, operar, gerenciar e manter os equipamentos/ recursos que forem necessários (roteadores, modems, estações de gerenciamento, meios de transmissão, cabeamento WAN, acessórios necessários, dentre outros) para o provimento dos serviços conforme solicitados neste documento.
     2. Os equipamentos serão de propriedade da CONTRATADA, que deverá ser responsável pelo suporte técnico dos mesmos, de modo a cumprir a disponibilidade mínima exigida.
     3. A infraestrutura de rede da CONTRATADA (backbones, POPs, equipamentos internos, roteadores CPE, dentre outros) deverá estar sempre atualizada, dimensionada e preparada para suportar a totalidade dos serviços solicitados neste documento, garantindo os níveis de desempenho especificados no mesmo, verificando os valores de demanda de capacidade das conexões listados no **Quadro 1.**
     4. A infraestrutura de rede da CONTRATADA (backbones, POPs, equipamentos internos, roteadores CPE dentre outros) deverá ser redimensionada e preparada para suportar os serviços adicionais solicitados pela CONTRATANTE, garantindo os níveis de desempenho especificados neste documento para todos os serviços, nas seguintes situações:

a) Solicitação, pela CONTRATANTE, de alteração de taxas de transmissão;

b) Solicitação eventual, pela CONTRATANTE, de serviços para um novo endereço não contemplado na relação de endereços listados no **Quadro 1.**

* + 1. O ônus do redimensionamento e da preparação da infraestrutura será da CONTRATADA.
    2. A critério da CONTRATANTE, serão estabelecidos procedimentos de ativação do enlace, incluindo como serão conectados os equipamentos da CONTRATADA e da CONTRATANTE. Estes procedimentos serão anexados ao Projeto Executivo e seu cumprimento será requisito para um enlace ser considerado instalado.
    3. As especificações constantes deste documento consideram que as soluções de telecomunicações a serem contratadas deverão ter alta qualidade, disponibilidade, desempenho, segurança, atualização tecnológica e com suporte a contingência. Para isso, a rede da CONTRATADA deverá seguir as melhores práticas de projeto e implementação, suporte e operação de redes, seguindo os documentos de BCP (Best Current Practice) especificados pelo IETF nas RFCs correspondentes, por exemplo, as RFC 2430 e RFC 3785.
    4. As bandas mínimas garantidas dos links, conforme especificado no **Quadro 1**, deverão, durante a vigência do contrato, estar disponíveis em sua totalidade.
    5. Não há perspectiva de crescimento anual do número de sítios durante a vigência do contrato. Entretanto, a CONTRATADA deverá se comprometer com o atendimento eventual de futuros sítios, a critério da CONTRATANTE, nas mesmas condições técnicas e de preço oferecidos à CONTRATANTE para o objeto deste edital.
    6. A CONTRATANTE poderá solicitar a desativação do serviço prestado a qualquer dos endereços listados no **Quadro 1**.
    7. A rede oferecida deve ser logicamente independente e isolada de qualquer outra rede, em especial do ambiente público da Internet. O mecanismo para implementar o isolamento é o MPLS/VPN. Essa garantia deverá ser implementada fim-a-fim.
    8. A CONTRATADA deverá prestar os serviços de comunicação de dados, por meio de VPN IP/MPLS conforme os seguintes padrões:

a) RFC 1163, A Border Gateway Protocol;

b) RFC 2283, Multiprotocol Extensions for BGP-4;

c) RFC 2547, BGP/MPLS VPNs.

* + 1. A solução da CONTRATADA deverá suportar Qualidade de Serviço (QoS) através da arquitetura DiffServ, incluindo DiffServ sobre MPLS conforme os seguintes padrões:

a) RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers;

b) RFC 2475, An Architecture for Differentiated Services;

c) RFC 2597, Assured Forwarding PHB Group;

d) RFC 2598, An Expedited Forwarding PHB;

e)RFC 3270, Multi-Protocol Label Switching (MPLS) Support of Differentiated Services.

* + 1. A topologia lógica da rede VPN IP/MPLS oferecida deverá ser do tipo *full mesh*.
    2. A rede deve transportar, diferenciar e marcar as seguintes classes de serviço: controle de rede, tempo real - videoconferência, tempo real - voz, dados prioritários, tráfego em rajadas e melhor esforço.
    3. A rede da CONTRATADA deverá estar com a hora de seus elementos de rede ajustados com o relógio do ON (Observatório Nacional) e sincronizados através do protocolo NTP (Network Time Protocol) – RFC1305 ou do protocolo SNTP (Simple Network Time Protocol) versão 4 – RFC2030.
    4. De acordo com as prioridades e níveis de serviço desejados, a Contratada deverá implementar e fornecer, de forma fim-a-fim, classificação e marcação de diferentes níveis de tráfego, sendo mandatória a implementação de, no mínimo, 4 (quatro) delas (controle de rede, tempo real, dados prioritários e melhor esforço). As classes de serviço a serem implementadas são descritas a seguir:

a) Controle de Rede: aplicações de monitoramento e controle da rede, que deverão ser priorizadas acima de todas as outras a fim de garantir a disponibilidade de recursos para as intervenções preventivas ou corretivas que se façam necessárias ao seu correto funcionamento.

b) Tempo Real – Aplicações sensíveis ao retardo (delay) e variações de retardo da rede (jitter), que exigem priorização de pacotes e reserva de banda.

c) Dados Prioritários – Aplicações interativas para o negócio, que exigem entrega garantida e tratamento prioritário.

d) Melhor Esforço – “Best Effort”: Todo tráfego não explicitamente atribuído às classes anteriores deverá ser alocado nesta classe. Sua finalidade é permitir um valor muito baixo de recursos para tráfegos não previstos ou ainda não identificados como tráfegos importantes. Essa classe deverá permitir o fluxo de tráfego, se houver recursos disponíveis na rede, impedindo que esse tráfego afete negativamente as demais classes.

* + 1. Todos os roteadores CPE devem ser dimensionados para operar com carga máxima de CPU e memória de 75%, desde que satisfeita a condição de tráfego igual ou inferior à capacidade da soma dos enlaces WAN calculada a média de no mínimo 5 minutos. Caso seja identificado, durante a execução do contrato, um roteador com uso de CPU ou memória acima destes limites, este deverá ser substituído ou atualizado, sem ônus adicional para a CONTRATANTE.
    2. Todos os roteadores CPE devem ser dimensionados de forma que tenham capacidade de encaminhamento de pacotes IP, em pacotes por segundo, compatíveis com as velocidades dos enlaces WAN conectados.
    3. Para cada sítio conectado, deverá ser garantida a disponibilidade do serviço conforme os níveis estabelecidos na tabela a seguir:

| ACORDO DE NÍVEL DE SERVIÇO E REDUNDÂNCIA | | |
| --- | --- | --- |
| TIPO | NÓ CENTRAL - NC | NÓS SIMPLES - NS |
| SLA MENSAL | 99,8% | 99,2% |
| REDUNDÂNCIA | Dupla abordagem em fibra ótica, composto por dois conjuntos de enlace e CPE, atendido por estações terminais distintas. | Sem dupla abordagem. |

Quadro 2: Níveis de disponibilidade

* + 1. Na ocorrência de falha ou intermitência no funcionamento de um acesso, o segundo deverá assumir automaticamente e proteger o tráfego que era cursado pelo(s) elemento(s) em falha em até 20s, considerada neste prazo inclusive a convergência de rotas;
    2. Após a solução da falha causadora do contingenciamento, o tráfego deverá retornar automaticamente para a situação anterior à falha.
    3. Adicionalmente, os seguintes requisitos de contingência deverão ser atendidos:

a) A solução completa de contingência deverá ser testada pela CONTRATADA periodicamente ao longo da execução do contrato. A periodicidade e o horário da realização dos testes será definida pela CONTRATANTE que, ao seu critério, poderá acompanhar os testes;

b) A CONTRATADA deverá disponibilizar relatório com os resultados dos testes de contingência;

c) A CONTRATANTE poderá solicitar a realização extraordinária dos testes com antecedência mínima de 2 (dois) dias úteis.

* + 1. Quanto aos requisitos de Qualidade de Serviço e de acordo com as prioridades e níveis de serviços requisitados, os diferentes tipos de tráfego que cursarão por meio da rede deverão ser classificados em seis classes de serviços, com as respectivas sugestões de porcentagens de alocação de largura de banda, conforme descrito a seguir:

a) Controle de Rede (1% da largura de banda): aplicações e/ou protocolos de monitoramento e controle da rede como, por exemplo: Telnet, SSH, SNMP, NTP, syslog, TACACS+;

b) Tempo Real (5% da largura de banda): aplicações de voz sensíveis ao retardo (delay) e às variações de retardo (jitter), que exigem priorização de tráfego e reserva de banda;

c) Dados Prioritários (45% da largura de banda): aplicações que necessitam de garantias mínimas de banda e máximas de retardo, pouco tolerante a variações destes parâmetros;

d) Melhor esforço (tráfego não prioritário): todo o restante da largura de banda não priorizada estará disponível para os tipos de tráfego não mencionados anteriormente.

* + 1. A CONTRATADA deverá implantar roteadores com suporte aos padrões e funcionalidades para implementação de Qualidade de Serviço conforme descrito anteriormente.
    2. A CONTRATANTE poderá solicitar, a qualquer momento, a modificação nas configurações das classes de serviço e nos percentuais de banda destinados a cada uma delas.
  1. **REQUISITOS DA INFRAESTRUTURA**
     1. Os locais de instalação possuem alimentação elétrica de 220V, 60 Hz.
     2. A CONTRATADA não será responsável pelo fornecimento de solução de alimentação, proteção elétrica e racks.
     3. A CONTRATADA será responsável pela interligação da rede entre o Distribuidor Geral (DG) e o local onde será instalado o roteador CPE.
     4. O projeto e o memorial descritivo dos serviços deverão ser aprovados pela área de TIC do TRT7.
     5. No interior dos sítios da CONTRATANTE a distância mínima entre os cabos dos dois acessos dos nós do tipo NC deverá ser de 2 (dois) metros.
  2. **ESPECIFICAÇÕES MÍNIMAS OBRIGATÓRIAS DOS EQUIPAMENTOS**
     1. Os roteadores CPE, de propriedade da CONTRATADA, deverão ser dimensionados, fornecidos, instalados, configurados, mantidos, gerenciados e operados pela CONTRATADA e deverá ser garantido o desempenho e os níveis de serviços contratados.
     2. Todas as atualizações e correções (patches) de softwares, necessárias para o cumprimento dos requisitos exigidos neste documento, deverão ser realizadas sem ônus adicionais para a CONTRATANTE.
     3. Os roteadores CPE a serem disponibilizados pela CONTRATADA nos sítios deverão atender aos seguintes requisitos:

a) Possuir 2 interfaces LAN: Ethernet IEEE 802.3, 802.3u Especificação 10/100/1000BASE-T (Full Duplex), com conector do tipo RJ-45;

b) Ser fornecidos com todos os componentes, módulos e acessórios necessários ao seu funcionamento atendendo aos requisitos deste estudo;

c) Suportar capacidade de filtros de pacotes (por protocolo, endereço IP de origem, endereço IP de destino, porta de UDP/TCP de origem, porta de UDP/TCP de destino);

d) Suportar classificação de tráfego de acordo com diversos critérios (interface, IP origem/destino, portas TCP/UDP, MAC e serviço) em cada interface física e lógica (sub-interfaces);

e) Suportar gerenciamento de filas com base em classes de tráfego;

f) Suportar mecanismos de escalonamento de filas que permitam a reserva de largura de banda mínima para cada fila. Deverá ser suportado um valor mínimo de 12 filas;

g) Suportar mecanismos de QoS:

h) Suportar mecanismo para descarte preventivo de pacotes (Ex.: WRED ou equivalente);

i) Suportar mecanismos de escalonamento de filas (Ex.: WFQ, WRR ou equivalente).

j) Suporte completo a MIBs que permitam a monitoração de parâmetros de desempenho por classes de serviço;

k) Suportar MIB-II e RMON;

l) Suportar servidor DHCP de acordo com a RFC 2131 (Dynamic Host Configuration Protocol) permitindo a atribuição de endereços IP a estações a partir do roteador;

m) Suportar "BOOTP relay agents" de acordo com a RFC 2131 (Dynamic Host Configuration Protocol) permitindo a atribuição de endereços IP a estações localizadas na rede local a partir de um servidor DHCP localizado em uma rede remota.

n) Suportar RFC791 (Internet Protocol);

o) Suportar protocolos de roteamento: RFC1583 (OSPF), RFC950 e RFC1878 (Suporte a subnets), além de rotas estáticas;

p) Suportar gerenciamento: RFC 1213 (MIB-II), RFC1155 (SMI-TCP/IP), RFC1157 (SNMP). A implementação de SNMP deve ser compatível com versões v2c e v3;

q) Demais mecanismos: RFC1631 (NAT) e IEEE 802.1Q VLAN Trunking;

r) Possuir data e hora ajustada com o relógio do ON (Observatório Nacional) e sincronizado através protocolo NTP (RFC 1305) ou SNTP versão 4 (RFC2030);

* + 1. A CONTRATADA deverá habilitar nos roteadores CPE o protocolo SNMP, disponibilizando nestes uma comunidade SNMP com acesso de leitura e permitir a configuração de traps, pela CONTRATANTE.
    2. A CONTRATADA deverá configurar nós roteadores CPE o acesso remoto por SSH ou telnet, assim como um usuário para uso da CONTRATANTE com um conjunto de permissões “somente leitura”, que permita a leitura da configuração, execução de comandos de diagnóstico (por exemplo ping, traceroute, listagem das rotas e interfaces) e comandos de acesso remoto (ssh, telnet).
    3. A configuração lógica dos roteadores CPE, para cada nível de serviço, será definida pela CONTRATADA com a aprovação da CONTRATANTE.
  1. **REQUISITOS DE SEGURANÇA NOS SEGMENTOS**
     1. **CARACTERÍSTICAS GERAIS**
        1. A CONTRATADA deverá manter o controle da segurança física e lógica de seus ambientes operacionais, estabelecendo as políticas de segurança a serem aplicadas aos serviços de telecomunicações contratados.
        2. Essa ação tem como intuito a prevenção de incidentes de segurança de forma a garantir níveis de segurança adequados nos ambientes de suas redes, por onde transitarão as informações da CONTRATANTE.
        3. A CONTRATADA deverá atender aos seguintes requisitos:

a) Prover uma rede logicamente independente e isolada de qualquer rede de terceiros, inclusive da Internet. O isolamento deverá ser realizado em nível lógico do MPLS e em nível 2 (do modelo OSI) para o acesso. Esta garantia deverá ser implantada fim-a-fim e também se aplica às soluções de contingência;

b) Caso solicitado pela CONTRATANTE, a CONTRATADA deverá aplicar nos seus roteadores ou em outros equipamentos de suas redes, exclusivos para prestação de serviços à CONTRATANTE, implementações de segurança tais como: autenticação de roteador CPE, controle de acesso aos dispositivos e listas de acesso;

c) Deverá ser empregado um esquema de autenticação no nível de protocolo de roteamento, de forma que roteadores não autorizados não possam injetar ou descobrir rotas da rede da CONTRATANTE;

* + - 1. d) Manter em seus quadros técnicos especialistas em segurança e prover serviços específicos de prevenção e reação a incidentes de segurança em Tecnologia da Informação. Esses serviços serão acionados pela equipe de segurança da CONTRATANTE.

e) A CONTRATADA deverá configurar de maneira apropriada os elementos de rede para habilitar o logging dos eventos da rede da CONTRATANTE, tais como conexões externas e registros de utilização de serviços (arquivos transferidos via FTP, acessos a páginas web e tentativas de login não autorizado). Os logs devem estar com o horário sincronizado via NTP e possuir o quanto possível de detalhes, sem, no entanto, gerar dados em excesso. A CONTRATADA deve possuir um sistema de Loghost dedicado à coleta e ao armazenamento dos logs gerados pelos dispositivos da rede da CONTRATANTE.

f) A CONTRATADA deverá aplicar e manter atualizados os patches de segurança nos seus roteadores ou em outros equipamentos de suas redes, exclusivos para prestação de serviços à CONTRATANTE.

* + 1. PREMISSAS DE SEGURANÇA
       1. As principais premissas de segurança serão, portanto, as seguintes:

a) Os ambientes operacionais da rede devem ser protegidos em seus níveis físico e lógico;

b) Devem ser empregadas soluções técnicas como autenticação de roteadores CPE, controle de acesso aos dispositivos, listas de acesso e logging, dentre outras;

c) Deverá ser empregado um esquema de autenticação no nível de protocolo de roteamento, de forma que roteadores não autorizados não possam injetar ou descobrir rotas da rede. Esse esquema de autenticação no nível de protocolo de roteamento minimiza problemas relacionados a erros de configuração do ambiente de rede CE-PE.

d) Deverá ser adotado no backbone MPLS principal da rede um esquema de VPN entre os roteadores PEs da operadora. Neste caso a segurança é estabelecida no nível de enlace da rede (camada 2). Caso o nível de segurança exigido pela CONTRATANTE na comunicação entre estes elementos seja superior ao fornecido pela provedora, a CONTRATANTE deverá utilizar uma camada adicional de segurança, no nível 3, como o IPSec por exemplo, que é recomendado nessas situações, para garantir o sigilo das informações trafegadas na rede através da utilização de criptografia.

e) O provedor deverá ser capaz de garantir que uma VPN não sofra interferência de outras VPNs, ou seja, cada túnel virtual deve ser acessível somente pelos usuários legítimos da rede TRT7. Na rede MPLS do provedor, a possibilidade de capturar tráfego de outros componentes não deve existir e para isso não acontecer, os roteadores PE e P devem assim estar corretamente configurados e com as listas de controle de acesso apropriadas.

* 1. **PADRÕES DE ENDEREÇAMENTO IP, ROTEAMENTO E INTERCONEXÃO DOS SEGMENTOS DA REDE** 
     1. **CARACTERÍSTICAS GERAIS**
        1. A CONTRATADA poderá utilizar no interior de sua rede o plano de endereçamento IP que preferir. Entretanto, a CONTRATADA deverá projetar e implementar a solução de forma a permitir a utilização do plano de endereços fornecido pela CONTRATANTE nas redes locais das unidades remotas do TRT7;
        2. A especificação da arquitetura de roteamento entre roteadores PE (Provider Edge) e CE (Customer Edge) será definida pela CONTRATADA em conjunto com a CONTRATANTE. É fortemente necessário que seja empregado um protocolo de roteamento dinâmico com baixo tempo de convergência (menor que 20 segundos). A PROPONENTE deve apresentar na proposta um resumo da solução de roteamento a ser oferecida.
        3. A CONTRATADA deverá projetar e implantar uma solução de roteamento que atenda os requisitos de conectividade, contingência, balanceamento de tráfego e interconexão. A solução de roteamento deverá ser implantada após sua aprovação pela CONTRATANTE.
        4. A solução de roteamento deverá permitir a convergência da rede em um tempo menor que 20 segundos para o caso de mudança topológica da rede causada por falha(s) em enlace(s) ou equipamento(s).
        5. A contratada deverá, se solicitado pela contratante, habilitar o roteamento dinâmico entre roteadores CPE da contratada e equipamentos da contratante, em qualquer tipo de nó (NS ou NC). Devem ser suportados os protocolos BGP e OSPF, para os quais serão aceitos tempos de convergência maiores do que 20 segundos. Nesse caso, não será possível configurar apenas rotas estáticas entre os roteadores PE e CPE em cada circuito, pois anúncios de inclusão ou exclusão de rotas realizadas pelos equipamentos da contratada devem ser propagados pela rede MPLS/BGP. Também poderá ser solicitada a configuração de um protocolo de redundância de gateway (VRRP) entre equipamento da contratada e da contratante.
     2. **PLANO DE ENDEREÇAMENTO**
        1. As premissas para a criação do plano de endereçamento da rede são:
* Deve ser escalável;
* Deve permitir agregação de rotas (endereços contíguos);
* Deve permitir o acesso de qualquer ponto da rede às aplicações compartilhadas na rede;
* Deve levar em conta a redundância de conexões às VPNs.
  + - 1. A distribuição dos endereços deverá ser feita conforme a seguinte regra:

| FAIXA DE  ENDEREÇOS | FUNÇÃO |
| --- | --- |
| 172.16.7.0-31 | Reservado para endereços de loopback dos equipamentos. O primeiro endereço é atribuído ao CE principal, o segundo a CE backup, o terceiro ao Firewall principal e o quarto ao Firewall reserva. O restante dos endereços devem ficar reservados. Caso um sítio não tenha roteadores backup os endereços devem ficar reservados. |
| 172.16.7.32/30 | Interligação PE-CE, com o primeiro endereço atribuído ao PE e o segundo ao CE |
| 172.16.7.36/30 | Interligação PE-CE backup, com o primeiro endereço atribuído ao PE e o segundo ao CE |
| 172.16.7.40/30 | Interligação CE-Firewall, com o primeiro endereço atribuído ao CE e o segundo ao Firewall |
| 172.16.7.44/30 | Interligação CE-Firewall backup, com o primeiro endereço atribuído ao CE e o segundo ao Firewall |

Quadro 3: Endereços dos roteadores e firewall

* + - 1. Os endereços da ligação PE-CE e loopback do roteador CE dos Sítios onde estão localizados os Setores de jurisdição (Varas e unidades) devem ser subtraídos do início da faixa 10.7.Y.0/24 alocada a cada unidade conforme o seguinte esquema:

| FAIXA DE  ENDEREÇOS | FUNÇÃO |
| --- | --- |
| 10.7.Y.0/30 | Alocados para interfaces loopback dos CEs principal e backup |
| 10.7.Y.4/30 | Interligação PE-CE, com o primeiro endereço atribuído ao PE e o segundo ao CE |
| 10.7.Y.8/30 | Interligação PE-CE backup, com o primeiro endereço atribuído ao PE e o segundo ao CE |
| 10.7.Y.12-254 | Uso interno |
| 172.16.7.44/30 | Interligação CE-Firewall backup, com o primeiro endereço atribuído ao CE e o segundo ao Firewall |

Quadro 4: Endereços no BACKBONE

* + - 1. O plano de endereçamento adotado e seu detalhamento, incluindo endereços adotados para cada Sítio, constarão no Projeto Executivo.
    1. **PLANO DE ROTEAMENTO**
       1. As premissas para a criação do plano de roteamento da rede são:
* Deve ser escalável;
* Deve realizar agregação de rotas para endereços contíguos;
* Deve manter o plano de roteamento atual das redes internas do TRT e demais unidades;
* Deve permitir o acesso de qualquer ponto da rede às aplicações compartilhadas;
* Deve permitir a realização de balanceamento de carga entre conexões redundantes.
* O protocolo de roteamento a ser configurado para troca de rotas entre o CE e o PE do provedor de serviços de telecomunicações dependerá das opções disponíveis pela operadora a ser contratada. As possíveis opções são:
* Rotas estáticas: são configuradas rotas estáticas tanto nas VRFs (VPN Routing and Forwarding) do roteador PE quanto no roteador CE;
* E-BGP4 (Border Gateway Protocol Externo): mais robusto, suportando políticas avançadas para a propagação e a filtragem de rotas, porém usa uma grande quantidade de recursos de CPU do roteador CE;
* OSPF (Open Shortest Path First): comumente utilizado, pois possui baixo tempo de convergência, é simples e não utiliza tantos recursos como o BGP. Porém pode não ser a melhor opção para roteamento entre PE e CE, pois dependendo da versão implementada, demanda uma instância do protocolo para cada VRF no PE, requerendo grande quantidade de recursos nos PEs. Desta forma, pode não ser disponibilizado pelos provedores de serviços de telecomunicações para roteamento PE-CE.
  + 1. **PROJETO DE QUALIDADE DE SERVIÇO**
       1. No escopo da conexão de cada cliente, há a necessidade de diferenciação de serviços, incluindo a alocação de banda e priorização de pacotes para redução de atrasos de certas classes de tráfego.
       2. O projeto de QoS da rede deverá ser baseado na Arquitetura de Serviços Diferenciados definida na RFC2475 do IETF.
       3. Na rede MPLS, a classe de serviço pode ser identificada de duas formas principais:
* Através dos 3 bits do campo EXP do cabeçalho do MPLS, fazendo-se o mapeamento do DSCP para o EXP na borda da rede;
* Através do mapeamento de um rótulo para cada par FEC/ classe de serviço.
  + - 1. Foram adotadas premissas iniciais estabelecidas neste documento para a definição das classes de serviço a serem configuradas no BACKBONE.
      2. **Os valores poderão ser ajustados durante e/ou após a implementação da rede, conforme definição do contratante.**
      3. O detalhamento de como deverá ser feito o mapeamento das classes de serviço em códigos DSCP e em códigos EXP do MPLS deverá ser feito na fase de engenharia de detalhes da rede, juntamente com a operadora contratada.
  1. **DIMENSIONAMENTO DOS ENLACES E DEMAIS RECURSOS**
     1. **DISPOSIÇÕES GERAIS**
        1. Da análise da rede
        2. As regras de dimensionamento definidas a seguir não levam em consideração a existência de contingência dos enlaces, sendo os valores sempre calculados como o total de banda ativa necessária ao acesso em cada backbone.
        3. O dimensionamento dos enlaces relativos às conexões de cada sítio TRT-sede se dará através de cálculo baseado no somatório das capacidades de todos os outros enlaces conectados à sede. Isto se deve ao fato do enlace do TRT-sede ter de fluir todo o tráfego proveniente de (ou com destino a) todos seus sítios associados simultaneamente, inclusive o tráfego de Internet. Foi admitido um nível máximo de *oversubscription* de 20%, isto é, o somatório das capacidades dos enlaces dos nós remotos do pode ser superior à capacidade do enlace do nó central deste mesmo backbone nesta proporção.
  2. **REQUISITOS OBRIGATÓRIOS PARA A IMPLANTAÇÃO OU MIGRAÇÃO DA REDE**
     1. A CONTRATADA deverá em no máximo 15 dias corridos, contados a partir da assinatura do Contrato, apresentar o Projeto Executivo contendo o plano de implantação e migração dos serviços.
     2. Os planos de implantação e migração deverão ser aprovados pela CONTRATANTE, em até 5 (cinco) dias corridos após sua apresentação.
     3. Caso o Projeto Executivo não seja aprovado pela Comissão de Implantação da Rede JT, a contratada deverá corrigi-lo e reapresentá-lo em no máximo **5 (cinco)** dias corridos após a comunicação da sua rejeição.
     4. O início da implantação dar-se-á somente após a aprovação, pela CONTRATANTE, do Projeto Executivo.
     5. **A CONTRATADA deverá informar à CONTRATANTE a finalização das instalações físicas, a medida que ocorrem, e quaisquer dificuldades encontradas no processo.**
     6. **A CONTRATANTE irá realizar os testes de aceitação conforme descrito no item 1.11.**
     7. **A não aceitação pela CONTRATANTE das soluções adotadas, devido à não conformidade com as solicitações deste documento, poderá resultar em rescisão total ou parcial do contrato de prestação de serviços.**
  3. **PRAZOS DE IMPLANTAÇÃO**
     1. Ativação de todos os enlaces de comunicação entre o NC e os NS, que terá duração máxima de 90 dias corridos, incluindo instalação e ativação dos circuitos, a contar da data de aprovação do Projeto Executivo.
  4. **CUSTOS DE IMPLANTAÇÃO**
     1. A instalação ou migração de sítios será sem ônus para a CONTRATANTE.
  5. **ACEITAÇÃO**
     1. Haverá dois tipos de aceitação: a aceitação provisória e a aceitação final.
     2. **CRITÉRIOS PARA ACEITAÇÃO PROVISÓRIA**
        1. A aceitação da implantação deverá atender os seguintes requisitos:

a) A aceitação se dará em até 10 dias corridos após a entrega dos serviços do último link.

b) Caso haja rejeição na aceitação dos serviços, a CONTRATANTE irá emitir comunicação formal para a CONTRATADA sanar os problemas apontados, sem que isso gere direito à CONTRATADA de dilação dos prazos definidos.

* + - 1. Os testes de aceitação dos serviços de rede serão compostos, no mínimo, por testes de conectividade/funcionais, testes de contingência e testes da solução de gerência.
      2. Um enlace da rede será considerado aceito nos testes de conectividade/funcionais, se:

a) O tempo de retardo da conexão e o desempenho do roteador CPE estiverem dentro dos limites estabelecidos no Anexo II do TR - Caderno de Métricas para serviços do Grupo 1 - Rede MPLS por um período de 2 dias úteis;

b) A taxa de erro de bit estiver dentro dos limites estabelecidos no Anexo II do TR - Caderno de Métricas para serviços do Grupo 1 - Rede MPLS;

c) A transação padrão de um sistema corporativo on-line, definido pela CONTRATANTE, puder ser completada com sucesso, dentro das características da aplicação;

d) A configuração lógica do roteador CPE for fornecida à CONTRATANTE;

e) Os equipamentos CPEs puderem ser visualizados, consultados e terem seus dados de monitoramento coletados por ferramentas utilizadas nos Tribunais.

* + - 1. A solução do NC será considerada aceita se os testes de funcionamento e comutação, conforme abaixo, forem aprovados pela CONTRATANTE.
      2. Verificação do funcionamento da contingência em:

a) Queda simples de enlace;

b) Queda simples de roteador.

* + - 1. Verificação do tempo de comutação da contingência, conforme especificação da solução, em:
      2. a) Queda simples de enlace;
      3. b) Queda simples de roteador.
      4. Aceito o total de sítios do backbone contratado, seus respectivos enlaces e soluções de contingências, conforme descrito nos itens anteriores, a equipe de fiscalização emitirá o Termo de Recebimento Provisório (TRP).
    1. **CRITÉRIOS PARA ACEITAÇÃO FINAL**
       1. A aceitação final se dará após o término do Período de Funcionamento Experimental - PFE, que se inicia com a emissão do TRP e se encerra após o decurso de um período completo de 10 (dez) dias corridos.
       2. Caso o PFE transcorra sem ocorrência de erros nos enlaces que compõem o item contratado, será emitido o Termo de Recebimento Definitivo (TRD), autorizando, a partir de então, o recebimento das faturas de serviços. O período de efetivo do faturamento deverá iniciar a partir da data de emissão do Termo de Recebimento Definitivo (TRD).
       3. Finalizado o PFE, a solução contratada ainda apresentar falhas de projeto/especificação, estará configurado o atraso na entrega do objeto contratado. O TRT7 poderá entender como inexecução total das obrigações, ensejando a extinção do contrato.
       4. A emissão do TRD não isenta o fornecedor contratado das responsabilidades sobre o pleno funcionamento de todas as facilidades e vantagens oferecidas, estendendo-se a necessidade de teste destas facilidades ao longo de toda vigência contratual.

1. **ESPECIFICAÇÕES TÉCNICAS PARA O ITEM 4**
   1. **DEFINIÇÕES GERAIS**
      1. Serviços de acesso à Internet, com links de comunicação de dados do tipo Banda Larga (“banda larga empresarial”), via fibra óptica, para as unidades remotas (fóruns e varas do trabalho) do TRT7 localizadas no interior do Estado do Ceará.
      2. Os serviços contratados deverão estar em pleno funcionamento nas 14 unidades indicadas no Quadro 5 e de acordo com as condições expressas neste documento, no prazo máximo de **45 (quarenta e cinco) dias corridos**, contados a partir da assinatura do contrato.

| item | taxa mínima de download | Unidade do TRT7 | |
| --- | --- | --- | --- |
| 1 | 200 Mbps | **Fórum do Trabalho de Caucaia**  Endereço: Av. Contorno Sul, s/n – Planalto Caucaia  CEP: 61.605-490 Caucaia/CE | |
| 2 | 200Mbps | **Fórum do Trabalho de Maracanaú**  Endereço: Rua Edson Queiroz, N° 480  Bairro: Piratininga  CEP: 61.905-155 Maracanaú/CE | |
| 3 | 200Mbps | **Fórum do Trabalho da Região do Cariri**  Endereço: Rua Rafael Malzoni, 761  Bairro: São José  CEP: 63.024-030 - Juazeiro do Norte - CE | |
| 4 | 200Mbps | **Fórum do Trabalho de Sobral**  Endereço: Av. Lúcia Sabóia, nº 500 - Centro  CEP: 62.320 - 000 - Sobral/CE | |
| 5 | 200Mbps | **Vara do Trabalho de Aracati**  Endereço: Rua Coronel Alexanzito, 503 - Centro  CEP: 62.800-00 Aracati/CE | |
| 6 | 200Mbps | **Vara do Trabalho de Baturité**  Endereço: Rua Major Pedro Catão, nº 450 - Mondego  CEP: 62.760 - 000 Baturité/CE | |
| 7 | 200Mbps | **Vara do Trabalho de Crateús**  Endereço: Rua Hermínio Bezerra, 801  Bairro: Planalto CE-075  CEP: 63.700 - 000 Crateús/CE | |
| 8 | 200Mbps | **Vara do Trabalho de Iguatu**  Endereço: Rua José de Alencar, 1.155 - Bugi  CEP: 63.500 - 000 Iguatu/CE | |
| 9 | 200Mbps | **Vara do Trabalho de Limoeiro do Norte**  Endereço: Rua Cândido Olímpio de Freitas, nº 1.655 - centro  CEP: 62.930 - 000 L. do Norte/CE | |
| 10 | 200Mbps | **Vara do Trabalho de Pacajus**  Endereço: Av. Vice-Prefeito Expedito Chaves Cavalcante S/N – Cruz das Almas  CEP: 62.870-000 Pacajus/CE | |
| 11 | 200Mbps | **Vara do Trabalho de Quixadá**  Endereço: Rua Tenente Cravo, nº 775  Bairro: Campo Velho  CEP: 63.900 - 000 Quixadá/CE | |
| 12 | 200 Mbps | **Vara do Trabalho de São Gonçalo do Amarante**  Endereço: Av. Paulo Costa, S/N, bairro Carioca  CEP: São Gonçalo do Amarante/CE | |
| 13 | 200 Mbps | **Vara do Trabalho de Tianguá**  Endereço: Rua Manoel da Rocha Teixeira, 1200  Bairro: Nenê Plácido  CEP: 62.327-445 Tianguá/CE | |
| 14 | 200 Mbps | **Vara do Trabalho de Eusébio**  Endereço: Rua Dermeval Carneiro, 115, Centro, Eusébio - CE  CEP: 61760-970 | |

Quadro 5: Locais de instalação e taxas mínimas de download

Tianguá: <https://maps.google.com/maps?q=-3.717017889022827%2C-40.983951568603516&z=17&hl=pt-BR>

**Caucaia**

<https://www.google.com/maps/search/Forum%20Do%20Trabalho%20de%20Caucaia/@-3.7462499141693115,-38.66167449951172,17z?hl=pt-BR>

**São Gonçalo**

<https://www.google.com/maps/place/3%C2%B036'27.8%22S+38%C2%B057'19.9%22W/@-3.6077158,-38.9577093,17z/data=!3m1!4b1!4m4!3m3!8m2!3d-3.6077158!4d-38.9555206?hl=pt-BR>

**Pacajus**

<https://www.google.com/maps/search/Justi%C3%A7a%20Do%20Trabalho%20Pacajus/@-4.16160774230957,-38.470455169677734,17z?hl=pt-BR>

* 1. **DA DISPONIBILIDADE DO LINK DE INTERNET**
     1. O serviço de Acesso à Internet deverá estar disponível 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, durante todo o período de vigência do Contrato.
     2. Entende-se por **disponível** quando o enlace dados possuir todas as seguintes características:

1. Perda de pacotes **inferior** a 1% na conexão com o POP da contratada (*gateway*);
2. Perda de pacotes **inferior** a 1% com destino ao site do TRT7 (www.trt7.jus.br) **OU** perda de pacotes **inferior** a 1% ao *looking glass* do ponto de troca de tráfego de Fortaleza do IX.br (lg.fortaleza.ce.ix.br).
   * 1. A disponibilidade do serviço será calculada para cada um dos 14 link de acesso a internet, para um período de 1 mês, através da seguinte fórmula:

| *D = [ (To – Ti) / To] X 100* | Onde:  D = disponibilidade;  To = período de operação (1 mês), em minutos;  Ti = tempo total de indisponibilidade do circuito de acesso, ocorrida no período de operação (1 mês), em minutos. |
| --- | --- |

* + 1. No cálculo de disponibilidade, não serão consideradas as interrupções causadas e de responsabilidade do CONTRATANTE.
    2. O valor de disponibilidade mínima para cada um dos 14 link de acesso a internet, no período de 1 (um) mês, deverá ser superior a 95%.
    3. Mensalmente, o CONTRATANTE apurará os tempos de inoperância e indisponibilidade, considerando as ocorrências desde a zero hora do primeiro dia do mês até as vinte e quatro horas do último dia do mês anterior ao da apuração.
    4. Caso a disponibilidade mensal apurada para cada link de internet seja inferior a 95%, será aplicada glosa na fatura/nota fiscal referente ao mês de apuração para cada link que apresentar disponibilidade abaixo de 95%.
    5. Na hipótese apresentada acima, para cada minuto de interrupção no serviço que supere os 5% de indisponibilidade admitidos, será aplicada glosa correspondente a 0,01% (um centésimo por cento), calculado sobre o valor mensal e limitado a 30% (trinta por cento) do valor mensal.
  1. **DA MANUTENÇÃO E SUPORTE TÉCNICO**
     1. A Contratada deverá prestar os serviços de manutenção e suporte técnico durante o horário compreendido entre 8h e 15h, de segunda a sexta-feira.
     2. Disponibilizar uma Central de Atendimento telefônico e um endereço eletrônico Internet (e-mail) para que se registrem as ocorrências e as solicitações de reparo, bem como o acompanhamento da solução dos problemas;
     3. O serviço de registro de chamadas deverá estar disponível 24 (vinte e quatro) horas por dia e 7 (sete) dias da semana;
     4. A solução de problemas que envolvam intervenção física nos equipamentos e instalações deverá ocorrer durante o horário compreendido entre 8h e 15h, de segunda a sexta-feira.
  2. **DA ALTERAÇÃO DE ENDEREÇO**
     1. A Contratante poderá, a qualquer tempo durante a vigência deste Contrato, solicitar à Contratada a mudança do local de instalação do circuito de acesso à Internet de qualquer Unidade Laboral.
     2. O prazo para a realização da alteração de local será de 30 (trinta) dias corridos, contados a partir da data do recebimento da comunicação formal.
  3. **DAS CARACTERÍSTICAS TÉCNICAS DA REDE FÍSICA**
     1. O acesso físico, desde o ponto de presença da Contratada até o local de instalação na unidade da Contratante deverá ser efetuado por meio de fibra ótica.
     2. A Contratante disponibilizará, em cada Unidade Laboral, o ambiente físico adequado aos equipamentos instalados pela Contratada.
     3. A Contratada deverá fornecer e instalar, interna e externamente, toda a infraestrutura e o meio físico necessários para o perfeito funcionamento dos serviços relativos ao objeto da contratação.
     4. A Contratada deverá se responsabilizar integralmente pela aquisição de qualquer equipamento e insumo necessário para levar o circuito até o local disponibilizado pela Contratante;
  4. **DAS CARACTERÍSTICAS TÉCNICAS DA REDE LÓGICA**
     1. A velocidade dos links poderá ser assimétrica, ou seja, velocidades de entrada e de saída poderão ser diferentes, sendo que a taxa de download (entrada) deverá corresponder, no mínimo, à TAXA DE DOWNLOAD estabelecidas no Quadro 5 e a taxa de upload (saída) não poderá ser inferior a 50% da TAXA DE DOWNLOAD efetivamente contratada.
     2. A Contratada não poderá:

1. implementar nenhum tipo de filtro de pacotes que possa incidir sobre o tráfego da Contratante, limitando a velocidade de banda Contratada;
2. limitar, de qualquer forma, a velocidade do tráfego no circuito abaixo do valor contratado.
3. aplicar franquia, limitando a capacidade de tráfego ou velocidade de dados.
   1. **DAS CARACTERÍSTICAS TÉCNICAS MÍNIMAS DOS EQUIPAMENTOS A SEREM FORNECIDOS PELA CONTRATADA**
      1. A Contratada deverá fornecer, instalar, configurar e manter em perfeito estado e plenamente operacionais, todos os equipamentos necessários ao funcionamento dos links de internet.
      2. Todo equipamento instalado deverá estar homologado pela Anatel.
      3. O modem/roteador deverá possuir, no mínimo:
4. interface interna (LAN) Gigabit Ethernet 1000BASE-T, padrão IEEE 802.3ab, full-duplex auto-sense, com conector 8P8C, para conexão com a rede local da Contratante;
5. fonte de alimentação interna, bivolt, para as tensões elétricas de 127V / 220V, 60 Hz.
   * 1. Os roteadores deverão acompanhar todos os cabos, software, interfaces, adaptadores e demais acessórios para realizar os serviços de comunicação de dados descritos neste Anexo I do Termo de Referência.
   1. **DA SEGURANÇA DA INFORMAÇÃO**
      1. A Contratada deverá garantir o sigilo e a inviolabilidade das informações que eventualmente possa ter acesso durante os procedimentos de instalação e manutenção de seus equipamentos, bem como durante a operação do serviço.
   2. **DO GERENCIAMENTO DOS SERVIÇOS**
      1. A Contratada deverá disponibilizar ferramenta WEB que permita o acompanhamento da utilização e performance do serviço prestado e emissão de relatórios.
6. **ESPECIFICAÇÕES TÉCNICAS COMUNS PARA OS GRUPOS 2 E 3**
   1. **ITEM 1 - NEXT GENERATION FIREWALL**
      1. **CARACTERÍSTICAS GERAIS**
         1. Os equipamentos deverão ser necessariamente do fabricante CHECK POINT para permitir a total compatibilidade com o equipamento *Check Point 15600* Next Generation *Firewall* já em uso pelo TRT7, permitindo o gerenciamento centralizado.
         2. A solução deverá ser compatível com SNMPv2 e SNMPv3;
         3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos equipamentos desde que obedeçam a todos os requisitos desta especificação;
         4. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;
         5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;
         6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.
         7. Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.
         8. Os FIREWALL deverão ser equipamentos novos de primeiro uso.
         9. Os FIREWALL não devem conter substâncias perigosas em concentração acima da recomendada pelo RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (PB), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil-polibromados (PBBs), éteres difenilpolibromados (PBDEs). O atendimento a este requisito deve ser comprovado pelo licitante vencedor por meio de certificado reconhecido nacionalmente, laudos técnicos emitidos por laboratórios acreditados pelo Inmetro ou declaração do fabricante.
      2. **CAPACIDADE E QUANTIDADES**
         1. Throughput de, no mínimo, 330 Mbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;
         2. Suporte a, no mínimo, 490.000 (quatrocentas e noventa mil) conexões ou sessões simultâneas;
         3. Suporte a, no mínimo, 10.300 (dez mil e trezentas) novas conexões ou sessões por segundo;
         4. Throughput de, no mínimo, 950 Mbps para conexões VPN;
         5. Licenciado ou permitir, pelo menos, 100 conexões ou sessões simultâneas de VPN client-to- site;
         6. Possuir, pelo menos, 6 (seis) interfaces de rede 1Gbps UTP;
         7. Possuir 1 (uma) interface do tipo console ou similar;
         8. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces. Caso um mesmo Throughput seja apresentado mais de uma vez em diferentes métricas, será considerado o de maior valor;
      3. **FUNCIONALIDADES DE FIREWALL**
         1. Deve suportar autenticação para o serviço NTP.
         2. Deve ser possível definir por quais origens de rede são permitidas as conexões do administrador. 4.1.4.3. Deve ser possível restringir o acesso à gerência do equipamento por, pelo menos, endereço IP e Rede.
         3. Deve suportar SNMP v2 e v3.
         4. Deve ser possível realizar captura de pacotes diretamente na gerência do equipamento.
         5. Deve ser possível monitorar a utilização de CPU e memória diretamente na gerência do equipamento.
         6. Deve ser possível realizar a configuração do cluster diretamente na gerência do equipamento.
         7. Deve ser possível conectar a serviços de DDNS;
         8. Deve ser possível configurar o timeout da sessão do administrador na interface web.
         9. Deve ser possível configurar a complexidade da senha do administrador e dias para expirar.
         10. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logs.
         11. A solução deve possibilitar ao administrador realizar a integração com o AD (Active Directory) através de um assistente de configuração na própria interface gráfica do produto;
         12. A solução deve identificar usuários das seguintes fontes pelo menos:
             1. Active Directory: o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;
             2. Autenticação via navegador: para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;
         13. A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;
         14. Na integração com o AD, a operação de cadastro deve ser realizada na própria gerência do equipamento, de maneira simples e sem utilização de scripts de comando;
      4. **FUNCIONALIDADE DE PREVENÇÃO DE AMEAÇAS**
         1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio equipamento sem a necessidade de uso de quaisquer interfaces ou dispositivos externos.
         2. Deve ser possível agendar para que o mecanismo de inspeção receba e implemente atualizações para os ataques emergentes sem a necessidade de reiniciar o equipamento;
         3. Deve ser possível realizar a atualização manualmente sem necessidade de internet através da importação do pacote de atualização.
         4. Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo, pelo menos, os seguintes ataques conhecidos: SQL lnjection, ICMP Denial of Service, força bruta, scanning de portas, CIFS Port overflow, Non Compliant DNS, Non Compliant SMTP, Non Compliant CIFS, Non Compliant MS SQL Server, IKE aggressive Exchange;
         5. Deve ser capaz de bloquear tráfego SSH em DNS tunneling;
         6. A solução deverá ser capaz de inspecionar e proteger apenas hosts internos ou inspecionar todo o tráfego;
         7. A solução deve proteger contra ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning);
         8. A solução deverá possuir pelo menos dois perfis pré-configurados de fábrica para uso imediato e permitir a customização de um perfil;
         9. Em cada proteção de segurança, devem estar inclusas informações como: categoria, tipo de impacto na ferramenta, severidade, e tipo de ação que a solução irá executar;
         10. A solução de IPS deve possuir um modo de solução de problemas, que define o uso de perfil de detecção sem modificar as proteções individuais já criadas e customizadas;
         11. Deve ser possível criar regras de exceção no IPS para que a solução não faça a inspeção de um tráfego específico por pelo menos proteção, origem, destino, serviço ou porta.
         12. Deve ser possível visualizar a lista de proteções disponíveis no equipamento com os detalhes.
         13. A solução deve incluir ferramenta própria ou solução de terceiros para mitigar/bloquear a comunicação entre os hosts infectados com bot e operador remoto (command & contrai).
         14. A solução deve bloquear arquivos potencialmente maliciosos infectados com malware.
         15. A solução de proteção contra malware e bot deve compartilhar a mesma política para facilitar o gerenciamento.
         16. A solução de proteção contra malware e bot deve possuir um modo de solução de problemas, que define o uso de perfil de detecção, sem modificar as proteções individuais já criadas e customizadas;
         17. As proteções devem ser ativadas baseadas em, pelo menos, critério de nível de confiança, ações de proteção e impacto de performance.
         18. Deve ser possível habilitar a trilha das proteções para não logar, criar um log ou gerar um alerta;
         19. Deve ser possível criar regras de exceção para que a solução não faça a inspeção de um tráfego específico por escopo, proteção e definir a ação e log para cada uma delas.
         20. A solução de anti-malware deve suportar protocolos SMTP e P OP 3, FTP, HT TP em qualquer porta;
         21. Deve ser possível definir uma política de inspeção para os tipos de arquivos por:
             1. Inspecionar tipos de arquivos conhecidos que contenham malware;
             2. Inspecionar todos os tipos de arquivos;
             3. Inspecionar tipos de arquivos de famílias específicas;
         22. Deve bloquear acesso a URLs com malware;
         23. Deve ser possível customizar a página exibida para o usuário quando a URL contiver um malware e o acesso for bloqueado;
      5. **FILTRO DE CONTEÚDO WEB**
      6. A solução deverá contar com ferramentas de visibilidade e controle de aplicações web e filtro URL integrada no próprio appliance de segurança que permita a criação de políticas de liberação ou bloqueio baseando-se em aplicações web e URL;
      7. A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser realizada na mesma interface web de gerenciamento;
      8. Deve ser possível configurar com apenas um clique o bloqueio a sites e aplicações que representem um risco de segurança e estão categorizadas como spyware, phishing, botnet, spam, anonymizer ou hacking.
      9. Deve ser possível configurar com apenas um clique o bloqueio a sites com conteúdo inapropriado como sexo, violência, armas, jogos e álcool.
      10. Deve configurar regras para permitir ou bloquear aplicações ou páginas da Internet por pelo menos:
          1. Usuário do Active Directory
          2. IP
          3. Rede
      11. Deve ser possível configurar o bloqueio de compartilhamento de arquivos com origem usualmente ilegais como aplicações torrents e peer-to-peer.
      12. Deve ser possível configurar manualmente o bloqueio de aplicações ou categorias de sites de aplicações indesejadas.
      13. Deve ainda ser possível adicionar uma URL ou aplicação que não está na base de dados.
      14. Deve ser possível limitar o consumo de banda de aplicações.
      15. A base de aplicações deve ser superior a 2900 aplicações, reconhecendo, pelo menos, as seguintes aplicações: bittorrent, gnutella, skype, facebook, linkedin, twitter, gmail, dropbox, whatsapp, etc;
      16. Deve ser possível realizar a recategorização de uma URL através da gerência do equipamento.
      17. Deve ser possível customizar e definir a frequência com que serão exibidas as mensagens para os usuários nas seguintes ações:
          1. Aceitar e informar
          2. Bloquear e informar
          3. Perguntar
      18. **IDENTIFICAÇÃO DE USUÁRIOS**
          1. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logging.
          2. A solução deve possibilitar ao administrador realizar a integração com o AD através de um assistente de configuração na própria interface gráfica do produto;
          3. A solução deve identificar usuários das seguintes fontes:
          4. Active Directory - o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;
          5. Autenticação via navegador - Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;
          6. A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;
          7. Na integração com o AD, a operação de cadastro deve ser realizada na própria interface web de gerência, de maneira simples e sem utilização de scritps de comando;
      19. **FUNCIONALIDADES DE ACESSO REMOTO**
          1. A solução deve prover acesso seguro encriptado aos usuários remotos através da Internet;
          2. A solução deve prover conectividade através de um cliente instalado no computador do usuário e através do navegador do usuário com conexão segura (HTTPS).
          3. Deve suportar pelo menos os seguintes métodos de conexão:
          4. Conexão através de cliente instalado no laptop ou desktop do usuário.
          5. Conexão através de cliente instalado no smartphone e tablets.
          6. Conexão através de navegador com SSL.
          7. Conexão através de cliente nativo Windows L2TP.
          8. Solução deve suportar alterar a porta padrão 443 para estabelecimento de VPN SSL.
          9. A solução deve permitir conexão VPN aos seguintes usuários:Usuários locais na própria base do appliance.
          10. Grupos de usuários locais na própria base do appliance.
          11. Grupos de usuários do Active Directory.
          12. Grupos de usuários Radius.
          13. A solução deve permitir atribuir um endereço específico para o usuário remoto.
      20. **FUNCIONALIDADE DE VPN SITE-TO-SITE**
          1. A solução deve prover acesso seguro criptografado entre duas localidades através da Internet;
          2. A solução deve estabelecer VPN com o site remoto do próprio fabricante ou de terceiros;
          3. A solução deve suportar autenticação com senha ou certificado;
          4. Deve suportar, pelo menos, criptografia AES 128 e 256;
          5. Deve possuir mecanismo para monitorar a saúde do túnel remoto;
          6. Quando o túnel for estabelecido entre dispositivos do mesmo fabricante este deve possuir protocolo proprietário para testar se o túnel está ativo.
      21. **GARANTIA E SUPORTE**
      22. Os equipamentos a serem entregues deverão possuir todas as funcionalidades exigidas neste anexo totalmente licenciadas para um período mínimo de 24 meses sem ônus para o TRT7;
      23. Deverá ser oferecida garantia e suporte por um período mínimo de 24 meses conforme Termo de Garantia (Anexo III do Termo de Referência).
7. **ITEM 1 - INSTALAÇÃO DO NEXT GENERATION FIREWALL**
   1. **CARACTERÍSTICAS GERAIS**
      1. Os equipamentos deverão ser instalados nos endereços e nas quantidades constantes do quadro abaixo:

| item | **quantidade a ser instalada** | Unidade do TRT7 | |
| --- | --- | --- | --- |
| 1 | **1** | **Fórum do Trabalho de Caucaia**  Endereço: Av. Contorno Sul, s/n – Planalto Caucaia  CEP: 61.605-490 Caucaia/CE | |
| 2 | **1** | **Fórum do Trabalho de Maracanaú**  Endereço: Rua Edson Queiroz, N° 480  Bairro: Piratininga  CEP: 61.905-155 Maracanaú/CE | |
| 3 | **1** | **Fórum do Trabalho da Região do Cariri**  Endereço: Rua Rafael Malzoni, 761  Bairro: São José  CEP: 63.024-030 - Juazeiro do Norte - CE | |
| 4 | **1** | **Fórum do Trabalho de Sobral**  Endereço: Av. Lúcia Sabóia, nº 500 - Centro  CEP: 62.320 - 000 - Sobral/CE | |
| 5 | **1** | **Vara do Trabalho de Aracati**  Endereço: Rua Coronel Alexanzito, 503 - Centro  CEP: 62.800-00 Aracati/CE | |
| 6 | **1** | **Vara do Trabalho de Baturité**  Endereço: Rua Major Pedro Catão, nº 450 - Mondego  CEP: 62.760 - 000 Baturité/CE | |
| 7 | **1** | **Vara do Trabalho de Crateús**  Endereço: Rua Hermínio Bezerra, 801  Bairro: Planalto CE-075  CEP: 63.700 - 000 Crateús/CE | |
| 8 | **1** | **Vara do Trabalho de Iguatu**  Endereço: Rua José de Alencar, 1.155 - Bugi  CEP: 63.500 - 000 Iguatu/CE | |
| 9 | **1** | **Vara do Trabalho de Limoeiro do Norte**  Endereço: Rua Cândido Olímpio de Freitas, nº 1.655 - centro  CEP: 62.930 - 000 L. do Norte/CE | |
| 10 | **1** | **Vara do Trabalho de Pacajus**  Endereço: Av. Vice-Prefeito Expedito Chaves Cavalcante S/N – Cruz das Almas  CEP: 62.870-000 Pacajus/CE | |
| 11 | **1** | **Vara do Trabalho de Quixadá**  Endereço: Rua Tenente Cravo, nº 775  Bairro: Campo Velho  CEP: 63.900 - 000 Quixadá/CE | |
| 12 | **1** | **Vara do Trabalho de São Gonçalo do Amarante**  Endereço: Av. Paulo Costa, S/N, bairro Carioca  CEP: São Gonçalo do Amarante/CE | |
| 13 | **1** | **Vara do Trabalho de Tianguá**  Endereço: Rua Manoel da Rocha Teixeira, 1200  Bairro: Nenê Plácido  CEP: 62.327-445 Tianguá/CE | |
| 14 | **1** | **Vara do Trabalho de Eusébio**  Endereço: Rua Dermeval Carneiro, 115, Centro, Eusébio - CE  CEP: 61760-970 | |

Quadro 6: Locais de instalação dos FIREWALL

* + 1. A instalação física deverá ser realizada em rack adequado já disponível nas instalações da CONTRATANTE;
    2. Deverá ser realizada a ativação dos equipamentos e licenças conforme procedimentos requeridos pelo fabricante;
    3. Deverá ser realizada a configuração dos equipamentos conforme parâmetros a serem informados oportunamente pela CONTRATADA na reunião inaugural do contrato;
    4. O recebimento automático de atualizações de segurança será definido na reunião inaugural do contrato;
    5. **Deverá ser realizada a integração de cada equipamento a ser instalado com o equipamento *Check Point 15600* Next Generation *Firewall* atualmente instalado no DATACENTER do TRT7** para:
       1. gerenciamento centralizado de regras e envio de registros de eventos;
       2. autenticação de administradores e usuários de rede;
    6. Deverá ser realizada a migração de todas as regras de FIREWALL, NAT, IPS, QoS, NGFW, além de todas as VPNs e demais funcionalidades existentes no equipamento *Check Point 15600* Next Generation *Firewall* atualmente instalado no DATACENTER do TRT7 e aplicáveis aos novos equipamentos;
    7. Após a instalação, integração e migração, cada equipamento deverá ser monitorado pelo prazo mínimo de 2 (duas) corridas para verificação das condições de funcionamento, troubleshooting de problemas ou não conformidade na operação.