TERMO DE REFERÊNCIA

1. Do objeto. CATSER 26107

1.1. Contratação de empresa especializada na prestação do serviço de Plataforma PABX em Nuvem, incluindo os recursos de acesso ao STFC, ligações locais, nacionais e internacionais, bem como o acesso à plataforma em nuvem via link Internet dedicado, com SD-WAN (segurança e Wi-fi), serviços de instalação, configuração, suporte, manutenção e treinamento, conforme especificações constantes neste Termo de Referência.

2. Da justificativa.

2.1. Com a evolução dos sistemas de comunicação e as demandas que a nova realidade das relações corporativas e de atendimento à população faz necessária a modernização nos seus sistemas de comunicação do TRE/ES, tanto interna quanto externa, gerando ganhos de performance com a implementação de novas funcionalidades, tendo como diretrizes:

2.1.1. Gerenciar e prover suporte tecnológico na implantação e operacionalização de todos os serviços de comunicação de voz corporativa baseado numa plataforma em nuvem.

2.1.2. Disponibilizar uma solução de comunicação moderna e eficiente, que permita seu acesso dentro das dependências das unidades da Justiça Eleitoral do Estado do Espírito Santo, bem como em ambiente de trabalho remoto.

2.1.3. Assegurar que os incidentes e problemas sejam prontamente identificados e solucionados.

2.1.4. Oferecer os serviços de infraestrutura de acesso tanto à rede pública de telefonia quanto ao acesso à plataforma em nuvem.

2.1.5. Prover os serviços necessários à sua operacionalização e funcionamento adequados, como implantação, treinamento e manutenção.

3. Das Definições.

3.1. Definições principais:

a) Agência Nacional de Telecomunicações - ANATEL: Entidade integrante da Planejamento Pública Federal indireta, com sede no Distrito Federal, submetida a regime autárquico especial e vinculada ao Ministério das Comunicações, com a função de órgão regulador das telecomunicações.

b) Serviço Telefônico Fixo Comutado – STFC: Serviço de telecomunicações que, por meio da transmissão de voz e de outros sinais, destina-se à comunicação entre pontos fixos determinados, utilizando processos de telefonia.

c) Área Local: Área geográfica contínua de prestação de serviços, definida pela ANATEL, segundo critérios técnicos e econômicos, onde é prestado o STFC na modalidade local.

d) ATA: Adaptador para telefone analógico.

e) Telefonia Local: Serviço de telecomunicações que, por meio de transmissão de voz e de outros sinais, destina-se à comunicação entre pontos fixos determinados, situados em uma mesma Área Local.

f) Área de tarifação básica - ATB: Parte da área local dentro da qual o serviço é prestado ao assinante, em contrapartida aos serviços ou preços do plano de serviços de sua escolha, sem valores adicionais para atendimento.

g) Prestadora de Serviço Telefônico Fixo Comutado: Empresa outorgada ou autorizada a prestar serviço telefônico fixo comutado nas modalidades local, nacional ou internacional.

h) Perfil de Tráfego: Quantitativo médio mensal estimado, em minutos, de ligações telefônicas efetuadas, em função do horário e das localidades de destino de maior ocorrência e levando em consideração o tempo médio de duração das chamadas.

i) Distância Geodésica: É a menor distância entre dois pontos possível de ser percorrida por um móvel. Por exemplo, a menor distância entre o Brasil e o Japão é uma linha reta, porém um avião não pode fazer este percurso, pois a superfície da Terra é redonda, então o menor percurso possível de ser realizado é uma curva chamada geodésica.

j) Código de Área: Identificação de uma área de numeração fechada da rede pública de telecomunicações ou de um acesso a um serviço com abrangência nacional, cujo formato é (AB). Exemplo: Estado de Sergipe – 79, Estado de Alagoas – 82, Estado da Bahia – 71.

k) Índice de Serviços de Telecomunicações - IST: Índice normatizado pela Resolução nº 420 da ANATEL para ser aplicado no reajuste e atualização de valores associados à prestação de serviços de telecomunicações.

l) Unidade de Resposta Audível – URA: Serviço ou sistema interativo que permite a resposta automática de chamadas através de mensagens personalizadas,

permitindo ainda a interação entre o usuário e a mesma, através da interpretação automática de opções discadas pelo usuário chamador através do teclado do telefone.

4. Da plataforma PABX em nuvem.

4.1. Características gerais:

4.1.1. Fornecer solução de central única de telefonia IP em nuvem, baseada em SIP conforme RFC 3261.

4.1.2. Todos os elementos como ATAs, IADs, Telefones IP, Gateways, Servidores da solução devem interoperar utilizando apenas SIP conforme RFC 3261 e demais.

4.1.3. A solução deverá estar hospedada em datacenters com redundância geográfica que possuam no mínimo as certificações ISO 27001, ISO 27017, ISO 27018, SOC1, SOC2, SOC3, PCI DSS, CSA STAR E HITRUST CSF, caso não possuam as certificações acima listadas, também será aceito a certificação Tier3.

4.1.4. Solução de voz sobre IP (VOIP) para colaboradores fora do ambiente de trabalho por meio de acesso internet.

4.1.5. Solução de voz sobre IP (ToIP-Telefonia Sobre IP) nas unidades corporativas atendidas pela CONTRATADA com a solução integral.

4.1.6. Possuir uma única base de configuração, independentemente do número de sítios, de maneira que todas as funcionalidades e recursos devam estar presentes e disponíveis em quaisquer pontos da rede.

4.1.7. Possuir capacidade de registrar telefones através do protocolo DHCP.

4.1.8. Deverá realizar de forma automática o provisionamento dos telefones IP’s.

4.1.9. Permitir bloqueio de chamadas para códigos de acesso compostos por menos de 8 dígitos. A inclusão de números não permitidos deverá ser realizada pelo administrador do sistema.

4.1.10. Sistema de Tarifação, com emissão de Relatórios WEB, com no mínimo as seguintes informações:

4.1.10.1. Relatório de chamadas: informações de data/hora das chamadas, ramal de origem, número de destino, categoria da chamada (Local, LDN, interna, etc.), duração e as informações do usuário que realizou a chamada: nome e centro de custo.

4.1.11. Solução de Gerenciamento Centralizado, com gerência proativa visando uma recuperação mais rápida de falha.

4.1.12. Permitir manutenção remota e outras funcionalidades contempladas nesta solução.

4.1.13. Suportar operação e configuração via interface gráfica GUI.

4.1.14. Estar baseado em plataformas capazes de prover interfaces gráficas que integre todos os aplicativos necessários para o completo gerenciamento da solução.

4.1.15. Implementar gerenciamento via protocolo SNMP.

4.1.16. Permitir visualizar o status do dispositivo, sistema de alarmes e assistência para isolamento de problemas.

4.1.17. Gerenciar e executar Backups de configuração de todos os equipamentos da solução, excetuando-se os telefones IP's.

4.1.18. Gerar relatórios de qualidade de voz nas ligações, agendado previamente com no mínimo 5 (cinco) dias de antecedência.

4.1.18.1. Os testes deverão ser realizados através da rede de dados com intuito de aferir problemas que possam afetar a qualidade da voz como por exemplo: perda de pacote, latência.

4.1.19. Deve suportar MIB.

4.1.20. Possuir ferramentas de manutenção apropriadas para telefonia IP, tais como relatórios de performance de rede (erros CRC entre outros), latência e perda de sinalização;

4.1.21. Permitir reinicialização dos telefones IPs a partir da interface de administração;

4.1.22. Possuir mecanismos para proteger a si mesmo contra ataques, além da proteção dos processos rodando no servidor pela detecção de anomalias por comportamento.

4.1.23. Permitir a utilização de telefones IP (SIP) e softphones (homologados pela solução contratada). Os usuários deverão se registrar ao sistema através de identificação de usuário e senha (obrigatória).

4.1.24. Suportar o protocolo SRTP (SecureReal-TimeProtocol) para a criptografia e autenticação.

4.1.25. Possuir capacidade de integração com serviços de diretório, suportando o protocolo LDAP para a base de usuários.

4.1.26. Disponibilizar autenticação de usuários e segurança via LDAP ou RADIUS com AAA.

4.1.27. Possuir recursos de acesso à Rede de Telefonia Fixa Comutada (RTFC)

4.1.28. Solução de Softphone, para PC, celular e tablet com sistemas IOS, Android e Windows PC.

4.1.29. Segurança da Camada de Transporte (TLS)

4.1.30. Solução de Mobile Phone.

4.1.31. Capacidade para no mínimo 1000 (mil) usuários.

4.1.32. Não serão aceitas soluções de PABX em nuvem baseadas em softwares livres.

4.2. Tipo de Ramais de Usuários

4.2.1. Ramal Tipo I - deverá possuir no mínimo as funcionalidades abaixo:

4.2.1.1. Captura de Chamadas: Um membro de um grupo poderá puxar a chamada que foi direcionada para outro membro.

4.2.1.2. Chamada em Espera: possibilidade de colocar uma chamada em espera, para efetuar outra atividade ou ligação.

4.2.1.3. Rechamada: permite que um Ramal, ao ligar para outro que esteja ocupado, realize uma rechamada quando o número de destino desocupar, mediante a digitação de um código.

4.2.1.4. Função Cadeado: Permitir que uma Ramal seja bloqueado, via senha, pelo usuário.

4.2.1.5. Não perturbe: Permitir que o ramal fique indisponível para receber chamadas até que a configuração seja retirada.

4.2.1.6. Transferência: Permitir o envio de uma chamada para outra linha.

4.2.1.7. Softphone: Permitir utilização do ramal como um Softphone em um computador, para que não seja necessário a utilização de aparelhos.

4.2.1.8. Plano de Chamadas: Permitir que o administrador configure perfis de chamadas de entrada/Saída para um usuário.

4.2.1.9. Permitir que um usuário faça uma conferência entre a linha do usuário e mais 2 outras linhas.

4.2.1.10. Dispositivos por usuários: 2 (permite que o ramal seja vinculado até 2 tipos de dispositivos seja aparelhos, softphone mobile ou softphone desktop).

4.2.1.11. Serviço de correio de voz com função de receber os recados deixados quando a ligação não for atendida. Estes recados deverão ser enviados para um e-mail previamente cadastrado. Cada ramal deverá possuir seu próprio correio de voz.

4.2.1.12. Permitir a troca de mensagens de texto (chat corporativo) entre os usuários.

4.2.1.13. Permitir a criação de espaços virtuais para até 15 participantes internos (áudio, vídeo e compartilhamento de conteúdo).

4.2.2. Ramal Tipo II - deverá possuir, no mínimo, as funcionalidades dos ramais tipo I e as informadas abaixo:

4.2.2.1. Chefe Secretária: permitir que o usuário atenda à chamada de outro ramal, e possa transferi-las.

4.2.2.2. Permite que um usuário faça uma conferência entre a linha do usuário e mais 14 outras linhas.

4.3. URA de Atendimento:

4.3.1. A CONTRATADA deverá disponibilizar um sistema de atendimento automático do tipo URA, que ao receber uma nova chamada telefônica, reproduz um menu de opções para o cliente.

4.3.2. As mensagens de voz devem ser customizáveis.

4.3.3. O áudio da fila de espera deve ser customizável.

4.3.4. Deve permitir a criação de menus e sub-menus até um limite de 120 (menus + sub-menus).

4.3.5. O serviço de gravação personalizada das mensagens será de responsabilidade da CONTRATANTE.

4.3.6. Deverá ser disponibilizado o serviço de URA tanto para a solução de PABX em nuvem quanto para a solução de Call Center em Nuvem.

4.4. Aparelhos Telefônicos e Headsets

4.4.1. Os aparelhos telefônicos e headsets deverão ser fornecidos pela CONTRATADA, no regime de aluguel conforme quantidades descritas no Anexo D, devem ser homologados pela ANATEL e possuir as características mínimas abaixo:

4.4.1.1. Aparelho IP

a)Tecnologia IP, VOIP.

b) Display LCD.

c) Até 1 contas SIP.

d) Switch Ethernet 10/100 de duas portas RJ-45, PoE integrado.

e) Alto-falante Full-Duplex.

f) Controle de volume e função mute.

g) Deverá possui IEEE 802.3af Power over Ethernet, classe 1 ou 2.

h) Agenda Remota XML.

i) Viva-voz Full-duplex.

j) Suporte a [VLAN].

k) Menu de Navegação.

l) QoS: marcação 802.1p / Q (VLAN), ToS da Camada 3, DSCP.

m) IEEE802.1X.

n) Segurança da Camada de Transporte (TLS).

o) Plano de discagem, navegador XML, URL de ação e ação URI.

p) Discagem rápida, linha direta.

q) Atribuição de IP: estático / DHCP / PPPoE.

r) Fonte de alimentação.

s) Deverá ser homologado com a solução de comunicação ofertada, garantindo assim total compatibilidade das funcionalidades.

t) Deverá possui manual em língua portuguesa.

u) Deverá possui teclas de funções programáveis.

v) Deverá possui Viva-voz.

w) Deverá possui duas portas Ethernet 10/100 Base-T.

4.4.1.2. Headsets

a) Headset Biauricular.

b) Receptores ergonômicos.

c) Tubo de voz flexível.

d) Microfone com função noise cancelling.

e) Áudio: Estéreo.

f) Proteção contra choques e surtos acústicos.

g) Tubo flexível com ângulo regulável.

h) Haste do tubo de voz com giro de 280 graus com limitador no próprio eixo.

i) Cabo USB blindado com filtro de proteção EMI.

j) Protetor bucal em espuma antialérgica.

k) Produto adequado com a norma NR17.

l) Velocidade de 2.0 para banda larga.

m) Controle de Volume Digital.

n) Tecla Mute.

o) Compatível com Windows 98/ XP / 2000 / Vista / 7 /8/9/10 / Mac OS 9.0 / Linux.

4.5. Solução de Call Center em Nuvem.

4.5.1. A Plataforma em Nuvem deverá disponibilizar também licenças de usuários (agentes e supervisores) para uso pelo Call Center da CONTRATADA, com as seguintes características:

4.5.1.1. Suportar os seguintes algorítimos de distribuição de chamadas: sequencial, simultâneo, ponderado e para atendente com o maior tempo disponível.

4.5.1.2. Roteamento baseado em habilidades: agentes são associados a diferentes filas com diferentes prioridades de distribuição.

4.5.1.3. Log in e log out através de portal.

4.5.1.4. Os atendentes devem ter os seguintes possíveis status: Sign in/out, disponível, indisponível e pós-atendimento.

4.5.1.5. Priorização de filas.

4.5.1.6. Priorização de quais chamadas serão entregues para os atendentes.

4.5.1.7. Repriorização de chamadas não atendidas que retornam para a fila.

4.5.1.8. Opções de roteamento quando atendente não atende a chamada.

4.5.1.9. Transbordo para filas.

4.5.1.10. Definição do tamanho máximo da fila.

4.5.1.11. Definição do tempo máximo de espera na fila.

4.5.1.12. Configuração de tratamento para chamadas em fila quando não há atendentes logados: sem tratamento, ocupado, transferência para um destino específico, serviço noturno, aplicação de tom de controle de chamada ou aplicação de um anúncio.

4.5.1.12.1. Serviço noturno: Definição de horário de atendimento com roteamento especifico para chamadas fora do horário de atendimento. Deve ser possível também ativar o serviço noturno de forma manual pelo portal ou por código de ativação de serviços pelo telefone.

4.5.1.13. Associação de calendário para tratamento diferenciado.

4.5.1.14. Desvio forçado: as novas chamadas serão temporariamente encaminhadas para o destino configurado, mediante ativação deste serviço efetuada pelo Administrador ou pelo Supervisor do portal ou pelo telefone.

4.5.1.15. Suportar mensagem de boas vindas de áudio (customizável).

4.5.1.16. Possibilitar carregar as mensagens acima pelo portal de administração.

4.5.1.17. Mesmo havendo atendentes disponíveis, as mensagens de boas vindas poderão ter opção de configuração.

4.5.1.18. Suportar a aplicação de mensagem de tempo de espera estimado ou posição na fila.

4.5.1.19. Suportar música quando parte é colocada em retenção.

4.5.1.20. Suportar mensagens de conforto. Estas devem ser aplicadas periodicamente enquanto chamada estiver na fila.

4.5.1.21. Apresentar informações sobre a chamada encaminhada para o atendente: Número do chamador, número chamado ou nome, tempo em espera na fila, chamadas ainda na fila, chamada mais tempo na fila, mensagem de sussurro, corrente de chamada diferenciado para chamadas vindas do DAC, alerta de chamada em retenção.

4.5.1.22. Permitir ao atendente transferir a chamada com um único click.

4.5.1.23. Suporte a click to dial.

4.5.1.24. Possuir funcionalidades básicas de telefonia, como realizar ou receber chamadas, transferências, rechamadas, conferência, etc.

4.5.1.25. Permitir a configuração e ativação dos serviços de desvios (incondicional, ocupado, não atende, indisponível).

4.5.1.26. Disponibilizar histórico de chamadas.

4.5.1.27. Suportar lista de contatos.

4.5.1.28. Permitir integração com LDAP Server para contatos.

4.5.1.29. Suportar Integração com Outlook.

4.5.1.30. Suportar Integração com o Banco de Dados.

4.5.1.31. Suportar Integração com sistemas de CRM.

4.5.1.32. Agenda telefônica customizada.

4.5.1.33. Escalonamento de chamadas.

4.5.1.34. Conferências de áudio.

4.5.1.35. Códigos de finalização de atendimento com sua respectiva descrição.

4.5.1.36. Permitir o gerenciamento dos atendentes com a troca de status, visualização do status da fila, monitoração das chamadas dos agentes.

4.5.1.37. Permitir o gerenciamento das chamadas nas filas: atender chamada que está na final, promover chamadas e transferir chamadas.

4.5.1.38. Solução deve ter um dashboard web que apresenta em tempo real informações sobre as principais informações das filas e dos atendentes como horario de log in, horário de log out, a quantas filas o atendente está associado, status corrente, porcentagem do tempo que ficou disponível, tempo médio de atendimento, tempo médio de pos atendimento, etc.

4.5.1.39. Disponibilizar relatórios que poderão ser exportados em xls e pdf.

4.5.1.40. Cliente Web para os Agentes.

4.5.1.41. Cliente Web para os Supervisores.

4.5.1.42. A interface do Call Center deve conterá, no mínimo, os seguintes elementos:

Elemento de interface	Descrição
Painel do logotipo	A interface da janela principal do Call Center deve conter um painel de logotipo que exibe o logotipo do cliente ou da empresa do Call Center, mensagens globais, links para outros elementos da interface ou funções do Call Center e informações sobre o usuário conectado.
Console de chamadas	O Call Console é onde você visualiza e gerencia suas chamadas atuais. Barra de cabeçalho, Dialer, Chamadas atuais, Chamada de conferência.
Painel de contatos	O painel Contatos contém seus diretórios de contatos e permite gerenciar seus contatos e usar contatos para fazer chamadas ou executar ações, como transferir para contato ou fila, nas chamadas existentes.
Páginas de configurações	Permitem definir várias configurações no nível do usuário e do aplicativo.
Painel de controle	O Painel é uma exibição de atalho para chamadas ativas na central de atendimento.

4.6. Softphone Desktop.

4.6.1. Telefone no formato de software, podendo ser instalado em PC’s, com sistema operacional Windows ou MAC.

4.6.2. Suportar chamadas telefônicas externas.

4.6.3. Suportar chamada em espera.

4.6.4. Suportar transferência de chamadas.

4.6.5. Suportar retenção de chamada.

4.6.6. Suportar conferência a 3.

4.6.7. Suportar os codecs G.711, G.722 e G.729.

4.6.8. Suportar lista de contatos.

4.6.9. Permitir integração com LDAP Server para contatos.

4.6.10. Permitir a configuração e ativação dos serviços de desvios (incondicional, ocupado, não atende, indisponível) no servidor SIP e não localmente.

4.6.11. Os arquivos com as credenciais dos usuários devem ser criptografados para evitar que um acesso remoto consiga ter esta informação.

4.6.11.1. Os arquivos com o histórico de comunicações devem ser criptografados para evitar que um acesso remoto consiga ter esta informação.

4.6.11.2. Os arquivos com a lista de contatos devem ser criptografados para evitar que um acesso remoto consiga ter esta informação.

4.6.12. Suporte SIP/TLS com mecanismos de segurança conforme NIST com algorítimo de criptografia AES-256 e com suporte a função hash SHA384.

4.6.13. Suporte a SRTP com AES-128 Counter Mode para proteção e Hash Message Authentication Code (HMAC) SHA-1 para autenticação.

4.7. Aplicativo de Comunicação Unificada PC.

4.7.1. Software para ser instalado em sistema operacional Windows ou MAC.

4.7.2. Suportar chamadas telefônicas de telefonia.

4.7.3. Suportar chamada em espera.

4.7.4. Suportar transferência de chamadas.

4.7.5. Suportar retenção de chamada.

4.7.6. Suportar conferência de até 15 participantes.

4.7.7. Suportar os codecs G.711, G.722 e G.729.

4.7.8. Suportar lista de contatos.

4.7.9. Permitir integração com LDAP Server para contatos.

4.7.10. Permitir a configuração e ativação dos serviços de desvios (incondicional, ocupado, não atende, indisponível) no servidor SIP e não localmente.

4.7.11. Suportar serviços de presença, chat, áudio e vídeo, compartilhamento de tela, transferência de arquivos.

4.7.12. Suportar codecs de áudio G.711, G.729 e G.722.

4.7.13. Suportar codecs de vídeo H.264 com resoluções QCIF, CIF, VGA e HD.

4.7.14. Os arquivos com as credenciais dos usuários devem ser criptografados para evitar que um acesso remoto consiga ter esta informação.

4.7.14.1. Os arquivos com os históricos de comunicações devem ser criptografados para evitar que um acesso remoto consiga ter esta informação.

4.7.14.2. Os arquivos com a lista de contatos devem ser criptografados para evitar que um acesso remoto consiga ter esta informação.

4.7.15. Suporte SIP/TLS com mecanismos de segurança conforme NIST com algoritmo de criptografia AES-256 e com suporte a função hash SHA384.

4.7.16. Suporte a SRTP com AES-128 Counter Mode para proteção e Hash Message Authentication Code (HMAC)-SHA-1 para autenticação.

4.8. Versão Mobile do Softphone.

4.8.1. O Softphone Mobile para smartphones e tablets deve ser do mesmo fabricante da solução de PABX na Nuvem;

4.8.2. Ser compatível com Smartphones que utilizem sistemas operacionais Android e iOS;

4.8.3. Disponibilizar o aplicativo no Marketplace de cada sistema operacional, Google e Apple;

4.8.4. Possuir interface gráfica, simulando teclado numérico e display do telefone IP;

4.8.5. Suportar o protocolo SIP;

4.8.6. Possuir lista de contatos local;

4.8.7. Permitir acesso às listas externas via padrão LDAP;

4.8.8. Possuir lista de chamadas efetuadas, recebidas e perdidas;

4.8.9. Suportar a criptografia de Payload;

4.8.10. Suportar videoconferências ponto a ponto, integradas na própria aplicação Softphone;

4.8.11. Suportar os codecs G.711, G.722, iLBC e iSAC;

4.8.12. Suportar os codec H.263 e H.264, para chamadas de videoconferência;

4.8.13. Permitir a visualização do status de presença dos usuários da plataforma;

4.8.14. Permitir a realização de conferências;

4.8.15. Suportar regras para direcionamento das chamadas;

4.8.16. Permitir comutar a chamada em andamento entre dispositivos de forma simples;

4.8.17. Permitir a configuração do dispositivo de preferência para o recebimento de ligações;

4.8.18. Possibilitar acesso aos recursos disponibilizados pela plataforma de comunicação unificada por intermédio de acesso via Smartphone.

4.8.19. Suportar no mínimo o idioma Português.

4.9. Solução de Gravação.

4.9.1. Deverá ser em nuvem, assim como toda a solução.

4.9.2. Permitir que as gravações dos ramais dos grupos de gravação só possam ser acessíveis pelos supervisores dos respectivos grupos ou por qualquer auditor.

4.9.3. Permitir a criação de no mínimo 10 grupos de gravação.

4.9.4. Permitir que o cliente nomeie colaboradores com perfil de auditoria para que estes possam acessar qualquer gravação.

4.9.5. Registrar (log) dos usuários que acessarem as gravações armazenadas.

4.9.6. Permitir armazenamento automático (periódico) em ambiente externo.

4.9.7. Permitir que as gravações fiquei armazenadas pelo período mínimo de 1 ano.

4.9.8. Permitir que os perfis de supervisão possam, através da console do browser, localizar as gravações através de filtros de busca: por data e hora, duração da chamada, número originador da chamada, número de destino da chamada. Estes parâmetros dos filtros podem ser usados simultaneamente (função lógica “AND”).

4.9.9. Realizar a gravação de qualquer terminal registrado no sistema, mesmo os que estejam utilizando somente a solução de software (softphone) e terminais conectados na referida infraestrutura.

4.10. Ferramenta de Gerenciamento.

4.10.1. Permitir a criação de Grupos de Ramais e alterações.

4.10.2. Gerenciar diagnósticos e relatórios de falhas.

4.10.3. Possuir alarmes de falhas.

4.11. Repasse de Conhecimento.

4.11.1. A CONTRATADA proverá repasse de conhecimento sobre a solução disponibilizada de central telefônica cujo público-alvo será a equipe da CONTRATANTE responsável pela gestão e operação do serviço. O repasse poderá ser realizado remotamente ou na sede da CONTRATANTE, a critério da contratada.

4.11.1.1. O repasse deve ser realizado na primeira semana após a implantação integral da solução.

4.11.1.2. O repasse deve envolver todo e qualquer tema necessário a gestão e operação da central telefônica em nuvem, aparelhos IP e softwares, em especial suas configurações e recursos.

4.11.2. A CONTRATADA proverá repasse de conhecimento sobre a solução SD-WAN cujo público-alvo será a equipe de TIC da CONTRATANTE. O repasse poderá ser realizado remotamente ou na sede da CONTRATANTE, a critério da contratada.

4.11.2.1. O repasse deve ser realizado primeira semana após a implantação integral da solução.

4.11.2.2. O repasse deve envolver todo e qualquer tema necessário à gestão e operação da solução SD-WAN, em especial suas configurações e recursos.

5. Dos entroncamentos digitais de acesso ao STFC.

5.1. Os entroncamentos digitais correspondem a acessos ao STFC (Serviço Telefônico Fixo Comutado) através de circuitos E1 SIP com 30 acessos simultâneos.

5.2. Junto a cada entroncamento digital serão fornecidas uma faixa de ramais DDR (Discagem Direta a Ramal) com blocos de 50 ramais em sequência.

5.3. No momento da contratação do serviço, caso seja necessária uma quantidade maior de ramais, deverá ser possível a adição de blocos extras de 50 ramais DDR cada.

5.4. Após a contratação inicial, a adição de blocos extras de ramais DDR na mesma sequência do bloco originalmente disponibilizado será objeto de consulta da CONTRATANTE junto à CONTRATADA.

5.5. As quantidades previstas de Entroncamentos Digitais e blocos DDR encontram-se na tabela do Anexo B:

5.6. Os Entroncamentos Digitais deverão possuir franquia ilimitada para ligações locais e de longa distância nacional, seja destinada à terminais fixos ou móveis de qualquer operadora, em todo o território nacional.

5.7. Os entroncamentos digitais deverão ser bidirecionais.

5.8. Não será exigido portabilidade de numeração existente.

5.9. A título de informação, segue abaixo perfil de tráfego atualmente utilizado (não vincula a presente contratação):

QUANTIDADE MINUTOS/MENSAL

Edifícios sede e anexo

fixo-fixo: 15.000 minutos

fixo-móvel: 5.000 minutos

Cartórios eleitorais nos municípios de Vitória, Vila Velha, Cariacica e Serra

fixo-fixo: 7.500 minutos

fixo-móvel: 700 minutos

Cartórios eleitorais nos demais municípios do estado

fixo-fixo: 20.000 minutos

fixo-móvel: 5.000 minutos

Todo estado - LDN.

ldn - intra-regional -fixo-fixo - região I (grande vitória) - 12.494 minutos

ldn - inter-regional - fixo-fixo - região II e III (interior) - 722 minutos

ldn - intra-regional - fixo-móvel - região I (grande vitória) - 564 minutos

ldn - inter-regional - fixo-móvel - região II e III (interior) - 44 minutos

6. Do acesso à plataforma PABX em nuvem.

6.1. A CONTRATADA deverá prover o serviço de acesso à Plataforma de PABX em Nuvem por meio de um acesso à Internet Dedicado para cada unidade do Tribunal Regional Eleitoral do Espírito Santo, com garantia de desempenho, segurança, suporte a diversos protocolos e utilização de endereçamento IP privativo.

6.2. O acesso à Internet Dedicado para cada unidade integrada na solução SD-WAN deve ser nas velocidades 10, 20 e 50 Mbps, dimensionados com base nas quantidades de ramais para acesso à Plataforma de PABX em Nuvem e na necessidade de acesso aos sistemas administrativos e judiciais, conforme ANEXO C.2

6.3. Para a sede do TRE-ES deverá ser disponibilizado acesso à Internet Dedicado com velocidade de 700 Mbps, dimensionado com base nas quantidades de ramais para acesso à Plataforma de PABX em Nuvem e na necessidade de acesso aos sistemas administrativos e judiciais, conforme ANEXO C.1.

6.4. A tecnologia de acesso à Internet Dedicado (enlace IP Dedicado) da CONTRATADA deverá possibilitar tráfego de dados, voz e vídeo.

6.5. Não será permitida a entrega de múltiplos links para alcançar as velocidades previstas, tais como MLPPP (MultiLink Point-to-Point Protocol) ou Link Agregation.

6.6. O serviço de comunicação de dados deverá ser implementado pela CONTRATADA, através do Backbone IP, de forma escalável, conforme a demanda de expansão e da CONTRATADA.

6.7. A CONTRATADA deverá prover, ao menos, 08 (oito) endereços IPv4 públicos, alocado de modo fixo, para cada acesso solicitado.

6.7.1. Deverá ser fornecido junto com cada enlace desta solução um bloco de IPv4 tipo /29 (6 IPs úteis para hospedeiros).

6.7.2. Deverá ser fornecida planilha de endereços IPv4 de todos os enlaces 2 (dois) dias úteis após a assinatura de contrato.

6.8. O circuito de comunicação através de ENLACE IP DEDICADO, compatível com o Backbone IP, deverá ser composto de acesso dedicado determinístico e simétrico (download = upload), através de meio físico terrestre do tipo fibra óptica (convencional ou GPON), inclusive nos atendimentos de última milha.

6.9. Será permitida subcontratação de terceiro exclusivamente para o acesso à última milha, ou seja, para o acesso entre a CONTRATADA e o local de prestação do serviço. A subcontratação não eximirá a responsabilidade da CONTRATADA, observada a qualidade, a fidelidade ao objeto e a garantia sobre a totalidade dos serviços prestados.

6.10. A CONTRATADA será responsável pela instalação e manutenção do circuito de IP Dedicado, incluindo o fornecimento dos equipamentos necessários para atendimento dos seus serviços nas dependências da CONTRATANTE.

6.10.1. Caberá à CONTRATANTE fornecer o local de instalação dos equipamentos da CONTRATADA, bem como a alimentação em conformidade com as normas ABNT NBR-5410 e NBR-13571.

6.10.2. A CONTRATANTE será responsável pelo provimento da infraestrutura necessária, nas suas dependências, como dutos para passagem de cabos, obras civis, dentre outros.

6.10.3. Será de responsabilidade da CONTRATANTE disponibilizar a rede interna para instalação dos equipamentos da CONTRATADA. Entende-se por rede interna, todo cabeamento (metálico ou óptico) necessário desde o distribuidor geral (DG), onde é entregue o acesso da CONTRATADA, até o local definido para o rack, que suportará os equipamentos (modems, dentre outros) necessários ao funcionamento do link.

6.11. A responsabilidade pela instalação e manutenção de todos os equipamentos vinculados ao Contrato será única exclusivamente da CONTRATADA.

6.11.1. Deverão estar inclusos os serviços de manutenção preventiva e corretiva de todos os equipamentos que comporão cada circuito da rede, a serem prestados pela CONTRATADA.

6.12. A CONTRATANTE poderá promover a alteração da topologia a qualquer hora e momento, sendo essa mudança discutida anteriormente e de forma ampla com a CONTRATADA, para análise de viabilidade técnica e econômica.

6.13. A CONTRATADA deverá estar ciente, antes da instalação dos equipamentos e da entrega dos links de comunicação, do ambiente em que estes recursos serão instalados. Para isso, a CONTRATANTE estará à disposição para quaisquer esclarecimentos que se façam necessários. Quaisquer incompatibilidades detectadas entre as características elétricas e de estrutura do ambiente disponibilizado e as características técnicas dos equipamentos da CONTRATADA a serem instalados deverão ser comunicadas antecipadamente à CONTRATANTE para análise e deliberação.

6.14. Os serviços de instalação deverão ser realizados de segunda a sexta-feira, das 12:00 às 18:00, salvo negociação entre as partes interessadas.

6.15. A CONTRATADA deverá disponibilizar, para os enlaces IP Dedicado com velocidade igual ou superior à 300 Mbps, o serviço de proteção contra ataques de volumetria do tipo DDoS (Denial of Service) no backbone da CONTRATADA.

6.15.1. São características mínimas exigidas para o serviço de proteção contra ataques de volumetria:

6.15.1.1. O serviço de Anti-DDoS deverá estar configurado no backbone próprio da CONTRATADA, não necessitando assim da instalação de appliance físico nas dependências da CONTRATANTE.

6.15.1.2. A CONTRATADA será responsável por monitorar 24h x 7d o tráfego Internet direcionado ao link IP Dedicado principal, instalado na sede do TRE/ES e, caso identifique um possível ataque, deverá entrar em contato com o representante designado pela CONTRATANTE e com sua autorização iniciar o processo de mitigação do ataque de DDoS no prazo de até 15 min.

6.15.1.3. Não serão admitidas soluções de Anti-DDoS hospedadas em datacenters de terceiros.

6.16. A CONTRATADA disponibilizará uma solução de gerenciamento proativa dos enlaces IP Dedicados com as seguintes características:

6.16.1. Deve contemplar módulos de gerência de falhas, desempenho, disponibilidade, relatórios e gestão de nível de serviço.

6.16.2. Deverá disponibilizar portal web para visualização de informações on-line, de forma gráfica, para o acompanhamento e monitoração do estado global e detalhado do ambiente.

6.16.3. O serviço de gerenciamento de acessos da CONTRATADA deverá atuar de forma proativa, antecipando-se aos problemas na rede e garantindo o cumprimento do Acordo de Nível de Serviço (ANS), realizando abertura, acompanhamento e fechamento de chamados de falhas relacionadas com indisponibilidade, operando em regime 24x7, todos os dias do ano.

6.16.4. O portal web a ser disponibilizado deve permitir o acesso a todos os recursos e módulos através de única autenticação, sem a necessidade de realizar outros logins para acessar qualquer outro recurso de gerenciamento.

6.16.5. Deverá ser escalável, permitindo futuras ampliações no número de elementos de rede a serem gerenciados.

6.16.6. Deverá permitir acessos de usuários com perfis diferenciados, com limitação de acesso a consoles, dispositivos, menus, alarmes e indicadores, entre outros.

6.16.7. Deverá permitir acesso de até 5 (cinco) usuários logados simultaneamente.

6.16.8. A solução deverá permitir a criação de grupos de perfis de acesso, que serão associados a tipos de usuários.

6.16.9. Os perfis deverão prever configurações em níveis de alertas, equipamentos, interfaces, aplicações, funcionalidades de monitoração, inventário, entre outros.

6.16.10. O portal web deve ser acessível sem necessidade de instalação de clients específicos. Portanto, não serão aceitas soluções que não sejam nativas em web ou

que requeiram a instalação de agentes nos desktops dos colaboradores da CONTRATANTE.

6.16.11. O acesso deverá ser via web, padrão HTTP/HTTPS, e em português, portanto não serão aceitas soluções que não possuam interface de usuário em português do Brasil.

6.16.12. A solução deverá ser acessível através dos principais browsers do mercado, tais como, Internet Explorer, Firefox, Google Chrome e Safari.

6.16.13. Deverá permitir a exportação das informações para relatórios em formatos comerciais.

6.16.14. A solução de gerenciamento de rede deverá gerar alertas quando os thresholds “limites” configurados para um componente monitorado sejam excedidos, como, por exemplo, utilização de CPU, memória, interfaces, volume de erros ou tempo de resposta de serviços.

6.16.15. A solução deverá fornecer, através do portal, visualização de informações da rede, on-line (em intervalos de 5 minutos e de forma gráfica), apresentando, no mínimo, os seguintes itens para cada um dos elementos monitorados:

6.16.15.1. Topologia da rede, incluindo os roteadores e seus enlaces, com visualização do estado operacional de todos os elementos da rede (enlaces e equipamentos). O estado operacional dos elementos da rede deverá ser atualizado automaticamente sempre que os mesmos sofrerem alterações.

6.16.15.2. Alarmes e eventos ocorridos na rede, com informações de data, hora, duração de ocorrência e identificação dos recursos gerenciados.

6.16.15.3. Consumo de banda dos enlaces (entrada e saída), separados por dia e mês.

6.16.15.4. Consumo de banda por classe de serviço, separados por dia e mês.

6.16.15.5. Ocupação de memória e CPU dos roteadores (se houver).

6.16.15.6. Retardo dos enlaces, separados por dia e mês.

6.16.15.7. Perda de pacotes (descarte) no sentido IN e OUT, em %.

6.16.15.8. Taxa de erros, em erros por segundo.

6.16.15.9. Latência, em milissegundos.

6.16.16. A solução deve fornecer o inventário dos equipamentos e enlaces da rede contendo, no mínimo, as seguintes informações:

6.16.16.1. Enlace: designação, tecnologia e nível de serviço.

6.16.16.2. Roteador (se houver): fabricante, modelo e configuração física (interfaces, memória, slots, dentre outros).

6.16.16.3. Endereçamento lógico: endereços IP e máscaras.

6.16.17. A solução deve possuir funcionalidade de backup de configuração dos elementos gerenciados, alarmes para alterações realizadas e relatório de mudanças.

6.16.18. A solução deverá permitir adicionar a nomenclatura conhecida pelo CONTRATANTE para os recursos gerenciados.

6.16.19. A solução de Gerenciamento deverá realizar registro de todas as ocorrências de alarmes/eventos em log de históricos e/ou em base de dados, contendo informações de data e hora de ocorrência, identificando os recursos gerenciados e armazenando os dados pelo período mínimo de 6 (seis) meses.

6.16.20. A solução de Gerenciamento deverá permitir a criação de Relatórios. Tais relatórios devem poder ser exportados conforme os principais métodos como: pdf, csv, xls. A seguir são apresentados os relatórios desejados:

6.16.20.1. Relatórios de desempenho sumarizado por período especifico.

6.16.20.2. Relatórios de desempenho classificados em uma visão TOP N, como exemplo, Top N Roteadores % de utilização de CPU, Top N Interfaces % de utilização, Top N Interfaces com descartes, dentre outros.

6.16.20.3. Relatórios de disponibilidade com períodos específicos.

6.16.20.4. Dashboards relacionando falhas, desempenho e disponibilidade.

6.16.20.5. Dashboards executivos com visões sumarizadas de indicadores operacionais (Taxa de Reincidência, Reparos no Prazo e Taxa de Falha).

7. Do detalhamento dos enlaces de acesso à Internet e da solução SD-WAN

7.1. Serviço composto por instalação e configuração dos enlaces de telecomunicação, instalação dos equipamentos de segurança SD-WAN, instalação dos equipamentos de rede sem fio (WI-FI), disponibilização do gerenciamento proativo 24x7 contra falhas, disponibilização de gerenciamento proativo 24x7 de segurança e disponibilização de portais de gerência de falhas e de segurança, conforme parâmetros definidos no ANEXO C (C.1 e C.2).

7.1.1. A disponibilização do gerenciamento proativo contra falhas e de segurança e dos respectivos portais serão parte integrante do fornecimento dos enlaces e do serviço de segurança.

7.1.2. Em relação ao serviço de wi-fi:

7.1.2.1. O quantitativo inicial de equipamentos está previsto no ANEXO C.

7.1.2.2. Em sendo identificada necessidade, a instalação de equipamentos WI-FI adicionais poderá ser solicitada, para qualquer endereço onde houver link dedicado instalado, nos limites constantes no ANEXO D.

7.1.2.2.1. O equipamento WI-FI adicional deverá ser entregue, instalado e configurado no local indicado na respectiva ordem de serviço no prazo máximo de 15 (quinze) dias.

7.1.3. Em relação aos enlaces de telecomunicação:

7.1.3.1. Deverão ser providos enlaces de comunicação full-duplex, síncronos, dedicados, com garantia de 100% de entrega da velocidade nominal, e de acesso à Internet (IP).

7.1.3.2. Os enlaces previstos no ANEXO C podem ser ativados ou desativados a qualquer tempo durante a vigência do CONTRATO, conforme necessidade da CONTRATANTE, mantendo-se um quantitativo mínimo de 75% dos pontos ativos.

7.1.3.3. Durante a execução do contrato pode ser solicitada a instalação de novos enlaces em qualquer um dos 78 municípios do estado do Espírito Santo, mesmo que o município não integre as tabelas iniciais constantes no ANEXO C.

7.1.3.4. Deve ser prevista pela CONTRATADA, durante a execução do contrato, a alteração de endereço, nos limites constantes no ANEXO D. A alteração de endereço deve ser considerada como uma instalação.

7.1.3.5. As instalações no decorrer do contrato devem ser efetuadas no prazo de 45 (quarenta e cinco) dias.

7.1.4. Em relação aos equipamentos de segurança SD-WAN.

7.1.4.1. Devem ser fornecidos appliances tipo Next-Generation Firewall (NGFW) para todos os enlaces previstos no ANEXO C.

7.1.4.1.1. Deverão ser configurados túneis VPN IPSEC entre o equipamento SD-WAN alocado na sede do Tribunal (ANEXO C.1) e os equipamentos SD-WAN alocados nas unidades remotas (ANEXO C.2).

7.1.4.2. Devem possuir capacidade de processamento de inspeção compatível com o dobro da largura de banda dos enlaces previstos no ANEXO C, a fim de permitir a utilização de enlaces MPLS de mesma largura de banda integrados a esta solução.

7.1.4.3. A CONTRATADA deverá, sem qualquer ônus para o Tribunal, integrar a solução SD-WAN e segurança aos links MPLS já contratados pelo Tribunal Regional Eleitoral do Espírito Santo junto à operadora de mercado.

7.1.4.4. Após instalação e configuração, a administração ficará a cargo do CONTRATANTE, com suporte da CONTRATADA..

7.1.4.5. A CONTRATADA deverá fazer um repasse de conhecimento em relação à configuração e administração dos equipamentos.

7.2. O enlace da Sede, anexo C.1:

7.2.1. Deverá ser livre de quaisquer filtros, controles, traffic shapping, trunking, aceleradores ou quaisquer outras soluções de filtragem, de aceleração ou de redução de desempenho.

7.2.2. Deverá ser configurado para possibilitar conexão VPN de contingência para os enlaces MPLS das unidades remotas.

7.2.2.1. Deverá permitir o uso de túneis VPN IPSEC entre um equipamento SD-WAN alocado na sede do Contratante e equipamentos SD-WAN alocados em suas unidades remotas.

7.2.3. Deverá atender aos seguintes parâmetros de desempenho, em caráter líquido (sem descontos por sobrecargas de quaisquer protocolos de quaisquer camadas, inclusive de criptografia da VPN do SD-WAN), medidos separadamente, por no mínimo 1 minuto e em horários aleatórios, através de acesso a serviço de medição da Entidade Aferidora da Qualidade de Acesso à Banda Larga (EAQ) da Anatel:

7.2.3.1. Largura de Banda de 700 Mbps.

7.2.3.2. Latência média máxima definida em 50 ms (considerado apenas se a vazão do enlace estiver até 80% da largura de banda nominal).

7.2.3.3. Perda de pacotes máxima definida em 2% (considerado apenas se a vazão do enlace estiver até 80% da largura de banda nominal).

7.2.3.4. Vazão líquida de sustentada de 100% da largura de banda nominal, de entrada e de saída, simultaneamente.

7.2.4. Deverá adotar MTU padrão de 1500 bytes, podendo ser ajustado em caso de necessidade.

7.2.5. Deverá possuir disponibilidade mínima mensal de 99,5%, não devendo ficar individualmente indisponível por mais do que 3,6h por mês, sob pena da glosa prevista no Anexo A - Tabela 3.

7.2.6. Deverá possuir um enlace com dupla abordagem de acesso por fibras ópticas na última milha (um enlace provido por dois caminhamentos distintos de fibras ópticas no trecho entre a estação e o equipamento de interconexão) até o local de instalação.

7.2.7. Deverá possuir capacidade de tráfego multisserviços em IPv4, permitindo o uso de VPN IPSEC sobre protocolo IP.

7.2.8. Deverá prover conexão através de interfaces disponíveis por cabo metálico e por fibra óptica, à escolha de uso pelo Contratante.

7.2.9. A infraestrutura da contratada deverá possuir no Brasil ao menos 5 (cinco) pontos de presença (PoP), sendo um deles em Vitória/ES.

7.2.9.1. Somente serão aceitos como PoPs válidos aqueles que possuam redundância nos enlaces de comunicação de dados com o backbone da contratada;

7.2.9.2. A velocidade mínima de saída do PoP localizado em Vitória/ES para as demais localidades no Brasil deverá totalizar a velocidade de 5 Gbps (cinco gigabits por segundo).

7.2.10. A infraestrutura deverá possuir enlaces de comunicação de dados com outras prestadoras, de abrangência nacional, possibilitando a capitalização do acesso em todo o Brasil.

7.2.11. O backbone da contratada deverá possuir, pelos menos, três pontos de troca de tráfego com provedores que possuam Sistemas Autônomos (AS - Autonomous Systems) independentes, sendo que cada um deverá ter, no mínimo, velocidade de 1 Gbps. Um desses pontos de troca deverá ser com um provedor internacional.

7.2.12. Deverá possuir serviço de proteção contra-ataques distribuídos de negação de serviço (Distributed Denial of Service – DDoS), com as seguintes características:

7.2.12.1. 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.

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

7.2.12.3. Prover informações de origem de ataque dos países, ranges de IPs e características do tipo de ataque.

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

7.2.12.5. 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:

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

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

7.2.12.5.3. Realizar autenticação de conexão TCP, quando do recebimento de pacotes Syn.

7.2.12.5.4. Limitar o número de conexões TCP simultâneas de um mesmo host.

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

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

7.2.12.5.7. Ataques denominados de “Comand-and-Control”, Point of Sale Malware, Remote Access Trojans RAT’s via feed atualizado diariamente.

7.2.12.5.8. Ataques à camada de aplicação, incluindo protocolos HTTP e DNS Volumétricos.

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

7.2.12.7. DNS BlackList; RegEx para registros específicos ou flags de recursão. Possuir mecanismos de quando bloquear um ataque por expressão regular DNS, selecionar se bloqueia apenas o ataque ou o host temporariamente.

7.2.12.8. Autenticação em query DNS por requisição em TCP.

7.2.12.9. Autenticação em JavaScript e Redirect para HTTP.

7.2.12.10. Adicionar expressão regular de payload em black-list.

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

7.2.12.12. 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.

7.2.12.13. 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.

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

7.2.12.15. 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.

7.2.12.16. A contratada deverá prover o serviço de mitigação sem limitação de tempo de duração do ataque, com quantidade ilimitada de eventos de ataque ao longo da vigência contratual.

7.2.12.17. O Contratante deverá ser informado de possíveis ataques identificados pela contratada no prazo máximo de duas horas.

7.2.12.18. O Contratante poderá comunicar a contratada suspeitas de ataques que esteja sofrendo, cabendo à contratada uma análise e envio de relatório.

7.3. Os enlaces das Unidades Remotas, anexo C.2:

7.3.1. Deverão possuir disponibilidade mensal de 97%, não devendo ficar indisponíveis continuamente por mais do que 21,6 h por mês, sob pena da glosa prevista no Anexo A - Tabela 3.

7.3.2. Deverão possuir abordagem de última milha (trecho entre a estação e o equipamento no local de instalação) exclusivamente por fibras ópticas em toda a sua extensão.

7.3.3. Deverão possuir capacidade de tráfego multisserviços em IPv4, permitindo o uso de VPN IPSEC sobre protocolo IP.

7.3.4. Deverão possuir latência máxima de 100 ms, entre o local de instalação e sistema de teste de velocidade diretamente acoplado ao IX Ponto de Tráfego de Troca (PTT) de Vitória-ES.

7.3.5. Deverão adotar MTU mínimo de 1500 bytes, podendo ser ajustado em caso de necessidade.

7.3.6. Deverão atender aos seguintes parâmetros de desempenho, em caráter líquido (sem descontos por sobrecargas de quaisquer protocolos de quaisquer camadas, inclusive de criptografia da VPN do SD-WAN, medidos separadamente, por no mínimo 1 minuto e em horários aleatórios, através de acesso a serviço de medição de acesso da Entidade Aferidora da Qualidade de Acesso à Banda Larga (EAQ) da Anatel):

7.3.6.1. Latência média máxima definida para cada tipo de enlace (considerado apenas se a vazão do enlace estiver até 80% da largura de banda nominal).

7.3.6.2. Perda de pacotes máxima definida para cada tipo de enlace (considerado apenas se a vazão do enlace estiver até 80% da largura de banda nominal).

7.3.6.3. Vazão de 100% da largura de banda nominal.

7.4. Os equipamentos SD-WAN da sede:

7.4.1. Devem consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração.

7.4.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.

7.4.3. As funcionalidades de proteção de rede que compõe a plataforma de segurança podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação.

7.4.4. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

7.4.5. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação.

7.4.6. Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q.

7.4.7. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP.

7.4.8. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding.

7.4.9. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM).

7.4.10. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay.

7.4.11. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server.

7.4.12. Os dispositivos de proteção de rede devem suportar sFlow.

7.4.13. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames.

7.4.14. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas.

7.4.15. Deve suportar NAT dinâmico (Many-to-1).

7.4.16. Deve suportar NAT dinâmico (Many-to-Many).

7.4.17. Deve suportar NAT estático (1-to-1).

7.4.18. Deve suportar NAT estático (Many-to-Many).

7.4.19. Deve suportar NAT estático bidirecional 1-to-1.

7.4.20. Deve suportar Tradução de porta (PAT).

7.4.21. Deve suportar NAT de Origem.

7.4.22. Deve suportar NAT de Destino.

7.4.23. Deve suportar NAT de Origem e NAT de Destino simultaneamente.

7.4.24. Deve poder combinar NAT de origem e NAT de destino na mesma politica.

7.4.25. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico.

7.4.26. Deve suportar NAT64 e NAT46.

7.4.27. Deve implementar o protocolo ECMP.

7.4.28. Deve suportar SD-WAN de forna nativa.

7.4.29. Deve implementar balanceamento de link por hash do IP de origem.

7.4.30. Deve implementar balanceamento de link por hash do IP de origem e destino.

7.4.31. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links.

7.4.32. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais.

7.4.33. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede.

7.4.34. Enviar log para sistemas de monitoração externos, simultaneamente.

7.4.35. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL.

7.4.36. Proteção anti-spoofing.

7.4.37. Implementar otimização do tráfego entre dois equipamentos.

7.4.38. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2).

7.4.39. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3).

7.4.40. Suportar OSPF graceful restart.

7.4.41. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede.

7.4.42. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego.

7.4.43. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego.

7.4.44. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.

7.4.45. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente.

7.4.46. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3.

7.4.47. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster.

7.4.48. A configuração em alta disponibilidade deve sincronizar: Sessões.

7.4.49. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede.

7.4.50. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs.

7.4.51. A configuração em alta disponibilidade deve sincronizar: Tabelas FIB.

7.4.52. O modo de alta disponibilidade deve possibilitar monitoração de falha de link.

7.4.53. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance.

7.4.54. Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo-ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos.

7.4.55. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas.

7.4.56. O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado a exportar configuração dos sistemas virtuais (contextos) por ambas as interfaces.

7.4.57. Controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos).

7.4.58. Deve apoiar um tecido de segurança para fornecer uma solução de segurança holística abrangendo toda a rede.

7.4.59. O tecido de segurança deve identificar potenciais vulnerabilidades e destacar as melhores práticas que poderiam ser usadas para melhorar a segurança e o desempenho geral de uma rede.

7.4.60. Deve existir um Serviço de Suporte que oferece aos clientes uma verificação de saúde recorrente com um relatório de auditoria mensal personalizado de seus appliances NGFW e sem fio (quando for o caso).

7.4.61. A console de administração deve suportar no mínimo inglês e Português.

7.4.62. A console deve suportar a administração de pontos de acesso compatíveis.

7.4.63. A solução deve suportar integração nativa de equipamentos de proteção de correio eletrônico, firewall de aplicações, proxy, cache e ameaças avançadas.

7.4.64. Deverá suportar controles por zona de segurança:

7.4.64.1. Controles de políticas por porta e protocolo.

7.4.64.2. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.

7.4.64.3. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.

7.4.65. Firewall deve ser capaz de aplicar a inspeção UTM (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis.

7.4.66. Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente às políticas de firewall.

7.4.67. Deve suportar automatização de situações como detecção de equipamentos comprometidos, estado do sistema, mudanças de configuração, eventos específicos, e aplicar uma ação que possa ser notificação, bloqueio do equipamento, execução de scripts ou funções em nuvem pública.

7.4.68. Deve suportar o padrão de indústria 'syslog' protocol para armanazemento usando o formato Common Event Format (CEF).

7.4.69. Deve suportar integração de nuvens públicas e integração SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage e Kubernetes.

7.4.70. Deve suportar o protocolo padrão da indústria VXLAN.

7.4.71. A solução deve permitir a implementação sem assistência de SD-WAN.

7.4.72. Em SD-WAN deve suportar QoS, modelamento de tráfego, rotas por políticas, VPN IPSec.

7.4.73. A solução deve suportar a integração nativa com soluções de sandboxing, proteção de correio eletrônico, cache e firewall de aplicação Web.

7.4.74. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo.

7.4.75. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail.

7.4.76. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs.

7.4.77. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor.

7.4.78. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

7.4.79. Identificar o uso de táticas evasivas via comunicações criptografadas.

7.4.80. Atualizar a base de assinaturas de aplicações automaticamente.

7.4.81. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos.

7.4.82. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas.

7.4.83. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante.

7.4.84. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações.

7.4.85. Deve possibilitar a diferenciação de tráfegos Peer-to-Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos.

7.4.86. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos.

7.4.87. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo.

7.4.88. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos.

7.4.89. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc).

7.4.90. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação.

7.4.91. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação.

7.4.92. Deve ser possível configurar Application Override permitindo selecionar aplicações individualmente.

7.4.93. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall.

7.4.94. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware).

7.4.95. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

7.4.96. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade.

7.4.97. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

7.4.98. Deve permitir o bloqueio de vulnerabilidades.

7.4.99. Deve incluir proteção contra ataques de negação de serviços.

7.4.100. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de decodificação de protocolo.

7.4.101. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise para detecção de anomalias de protocolo.

7.4.102. Deverá possuir o seguinte mecanismos de inspeção de IPS: IP Defragmentation.

7.4.103. Deverá possuir o seguinte mecanismos de inspeção de IPS: Remontagem de pacotes de TCP.

7.4.104. Deverá possuir o seguinte mecanismos de inspeção de IPS: Bloqueio de pacotes malformados.

7.4.105. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc.

7.4.106. Detectar e bloquear a origem de portscans.

7.4.107. Bloquear ataques efetuados por worms conhecidos.

7.4.108. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS.

7.4.109. Possuir assinaturas para bloqueio de ataques de buffer overflow.

7.4.110. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto.

7.4.111. Identificar e bloquear comunicação com botnets.

7.4.112. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.

7.4.113. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação.

7.4.114. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas.

7.4.115. Os eventos devem identificar o país de onde partiu a ameaça.

7.4.116. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.

7.4.117. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos.

7.4.118. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

7.4.119. Caso o firewall possa ser coordenado por software de segurança do computador do usuário final (laptop, desktop, etc.) deve ter um perfil onde se possa

executar a análise de vulnerabilidade nestes equipamentos de usuário e assegurar que estes execute versões compatíveis.

7.4.120. Fornecem proteção contra ataques de dia zero por meio de estreita integração com os componentes Security Fabric, incluindo NGFW, Sandbox (on-premise e nuvem).

7.4.121. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).

7.4.122. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito.

7.4.123. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL.

7.4.124. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs.

7.4.125. Possuir pelo menos 60 categorias de URLs.

7.4.126. Deve possuir a função de exclusão de URLs do bloqueio, por categoria.

7.4.127. Permitir a customização de página de bloqueio.

7.4.128. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site).

7.4.129. Além do Explicit Web Proxy, suportar proxy Web transparente.

7.4.130. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local.

7.4.131. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários.

7.4.132. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à utilização de sistemas virtuais, segmentos de rede, etc.

7.4.133. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;

7.4.134. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários.

7.4.135. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal).

7.4.136. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.

7.4.137. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD.

7.4.138. Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso à internet e gerenciamento da solução.

7.4.139. Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator.

7.4.140. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.

7.4.141. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem.

7.4.142. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino.

7.4.143. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo.

7.4.144. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus.

7.4.145. Suportar a criação de políticas de QoS e Traffic Shaping por porta.

7.4.146. O QoS deve possibilitar a definição de tráfego com banda garantida.

7.4.147. O QoS deve possibilitar a definição de tráfego com banda máxima.

7.4.148. O QoS deve possibilitar a definição de fila de prioridade.

7.4.149. Suportar marcação de pacotes Diffserv, inclusive por aplicação.

7.4.150. Suportar modificação de valores DSCP para o Diffserv.

7.4.151. Suportar priorização de tráfego usando informação de Type of Service.

7.4.152. Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes.

7.4.153. Permitir a criação de filtros para arquivos e dados pré-definidos.

7.4.154. Os arquivos devem ser identificados por extensão e tipo.

7.4.155. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc).

7.4.156. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos.

7.4.157. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos.

7.4.158. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

7.4.159. Suportar a criação de políticas por geo-localização, permitindo o trafego de determinado Pais/Países sejam bloqueados.

7.4.160. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

7.4.161. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

7.4.162. Suportar VPN Site-to-Site e Cliente-To-Site.

7.4.163. Suportar IPSec VPN.

7.4.164. Suportar SSL VPN.

7.4.165. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1.

7.4.166. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14.

7.4.167. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2).

7.4.168. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);

7.4.169. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.

7.4.170. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6.

7.4.171. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting.

7.4.172. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies.

7.4.173. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL.

7.4.174. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;

7.4.175. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL.

7.4.176. Deverá manter uma conexão segura com o portal durante a sessão.

7.4.177. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior).

7.4.178. O equipamento deve suportar NGFW Throughput de 11Gbps.

7.4.179. O equipamento deve suportar 8 milhões de sessões TCP concorrentes.

7.4.180. O equipamento deve suportar 500 mil novas sessões TCP por segundo.

7.4.181. O equipamento deve suportar 10 mil Firewall Policies.

7.4.182. O equipamento deve suportar 2000 Gateway-to-Gateway IPsec VPN Tunnels

7.4.183. O equipamento deve suportar 4 Gbps de SSL-VPN Throughput.

7.4.184. O equipamento deve ter IPv4 Firewall Throughput de 25Gbps para pacotes de 64Bytes UDP.

7.4.185. O equipamento deve suportar 10 Gbps de Threat Protection Throughput.

7.4.186. O equipamento deve conter pelo menos 16 interfaces GE RJ45.

7.4.187. O equipamento deve conter pelo menos 4 interfaces 10GE SFP+.

7.4.188. O equipamento deve conter pelo menos 8 interfaces GE SFP.

7.4.189. O equipamento deve suportar 49 mil Client-to-Gateway IPsec VPN Tunnels.

7.4.190. O equipamento deve possuir uma interface USB.

7.4.191. O equipamento deve suportar 55 Gbps de IPsec VPN Throughput.

7.4.192. O equipamento deve possuir HD SSD interno de pelo menos 400G.

7.5. Os equipamentos SD-WAN das unidades remotas:

7.5.1. Deverão possuir pelo menos quatro interfaces GigabitEthernet (100/1000Base-T)

7.5.2. Deverão possuir vazão mínima de 200 Mbps para SSL inspection ou NGFW ou Applicaon Control.

7.5.3. Deverão possuir vazão mínima de 200 Mbps para tráfego VPN.

7.5.4. Deverão possuir vazão mínima de 200 Mbps para IPS.

7.5.5. Deverão suportar no mínimo 50.000 sessões de firewall simultâneas;

7.5.6. Deverá possuir funcionalidade Next Generation Firewall para reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.

7.5.7. Deverão ser otimizados para análise de conteúdo de aplicações em camada 7.

7.5.8. Deverão ser do tipo appliance, não sendo aceito equipamento do tipo servidor ou com sistema operacional de propósito geral.

7.5.9. Deverão implementar funcionalidade de anti-spoofing, configurável por segmento de rede de modo que seja possível utilizar o próprio endereçamento da interface ou especificar quais redes serão utilizadas como referência para permitir/negar o ingresso de um pacote.

7.5.10. Deverão permitir a configuração de ISP (rota padrão estática) com a utilização de probe para verificar a disponibilidade do provedor.

7.5.11. A probe deve permitir verificar o acesso HTTP a pelo menos 1 (um) site web e deve considerar o provedor indisponível em caso de falha.

7.5.12. As funcionalidades de controle de aplicações, filtro de URLs, VPN IPSec e SSL, QoS, SSL Decryption e protocolos de roteamento dinâmico deverão operar em caráter permanente, podendo ser utilizadas durante toda a vigência do contrato.

7.5.13. Deverão possuir, pelo menos, as seguintes funcionalidades:

7.5.13.1. Policy based roung ou policy based forwarding.

7.5.13.2. Jumbo Frames.

7.5.13.3. DHCP Relay.

7.5.13.4. Suportar IGMP, v2 e v3.

7.5.13.5. Permitir a administração remota, protegida por autenticação usuário/senha e utilizando pelo menos os protocolos SSHv2 e HTTPS.

7.5.13.6. Roteamento IP Multicast através do protocolo PIM nas versões 1 e 2 e nos modos Sparse Mode e Dense Mode, não sendo exigida a implementação dos dois modos de forma simultânea.

7.5.13.7. Roteamento estático, OSPF, BGP e PBR (Policy Base Roung).

7.5.13.8. Encaminhamento de tráfego IPv4 e IPv6 (MP-BGP).

7.5.13.9. Cliente NTP.

7.5.13.10. SNMP nas versões 2c e 3 com restrição dos endereços para consultas.

7.5.13.11. Protocolo de informações de fluxo como Nelow, sFlow, IPFIX ou similar.

7.5.14. Deverão suportar NAT dos seguintes tipos:

7.5.14.1. NAT dinâmico (Many-to-1).

7.5.14.2. NAT dinâmico (Many-to-Many).

7.5.14.3. NAT estático (1-to-1).

7.5.14.4. NAT estático (Many-to-Many).

7.5.14.5. NAT estático bidirecional 1-to-1.

7.5.14.6. Tradução de porta (PAT).

7.5.14.7. NAT de origem.

7.5.14.8. NAT de destino.

7.5.14.9. NAT de origem e NAT de destino simultaneamente.

7.5.15. Deverão possuir controle de política de firewall, contemplando:

7.5.15.1. O controle de aplicações por grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias.

7.5.15.2. Controle, inspeção e descriptografia de SSL por política para tráfego de entrada (inbound) e saída (outbound).

7.5.15.3. Suporte offload de certificado em inspeção de conexões SSL de entrada (inbound).

7.5.15.4. Permissão de bloqueio de, pelo menos, os seguintes tipos de arquivos ou extensões: bat, cab, dll, exe, pif, e reg.

7.5.15.5. Suporte a objetos e regras multicast.

7.5.15.6. O agendamento de políticas em horários pré-definidos, de maneira automática.

7.5.15.7. Suporte a criação de políticas com data de expiração.

7.5.16. Deverá realizar o controle de aplicações, possuindo:

7.5.16.1. A capacidade de reconhecer aplicações, independente de porta e protocolo.

7.5.17. A capacidade de balancear o tráfego das aplicações entre múltiplos enlaces, simultaneamente.

7.5.18. A capacidade de definição de qual enlace será utilizado em situação normal por determinada aplicação.

7.5.19. A liberação e o bloqueio das aplicações, sem a necessidade de especificação de portas e protocolos.

7.5.20. O reconhecimento das diversas aplicações diferentes, incluindo, mas não limitado a: peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, audio, vídeo, proxy, mensageria instantânea, compartilhamento de arquivos, e-mail.

7.5.21. Habilidade de inspecionar o payload de pacote de dados com o objetivo de detectar, através de expressões regulares, assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo.

7.5.22. A capacidade de identificar o uso de táticas evasivas, ou seja, visualizar e controlar as aplicações e os ataques que utilizam comunicações criptografadas, tais como Skype e ataques utilizando a porta 443.

7.5.23. A capacidade de decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant

Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas.

7.5.24. A possibilidade da liberação e do bloqueio das aplicações (ou de suas funcionalidades) por usuário, grupo de usuários, endereço IP ou rede específica.

7.5.25. Atualização automática da base de assinaturas de aplicações.

7.5.26. A possibilidade de adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras.

7.5.27. A permissão de solicitação de inclusão de aplicações na base de assinaturas de aplicações do fabricante.

7.5.28. A função de alertar o usuário quando uma aplicação for bloqueada.

7.5.29. A possibilidade de diferenciação e controle de partes das aplicações como, por exemplo, permitir o Gtalk chat mas bloquear a transferência de arquivos, permitir acesso ao Facebook mas bloquear a visualização de vídeos, permitir acesso ao whatsapp mas bloquear a transferência de arquivos.

7.5.30. A possibilidade de diferenciação de aplicações Proxies (ghostsurf, freegate, ultrasurf, tor, etc) possuindo granularidade de controle/políticas para os mesmos.

7.5.31. A possibilidade da criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

7.5.31.1. Tecnologia utilizada nas aplicações (Client-Server, Browser Based, Network Protocol, etc).

7.5.31.2. Nível de risco da aplicação.

7.5.32. A configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall, considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

7.5.33. A inspeção de arquivos incorporados em outros arquivos ou arquivos que tenham sua extensão alterada na tentava de contornar sua detecção.

7.5.34. Deverá realizar a Identificação de usuários, contemplando:

7.5.34.1. A capacidade de criação de políticas baseadas na visibilidade e controle de quem (usuários e grupos de usuários) está utilizando quais aplicações através da

integração com serviços de diretório, autenticação via Ldap, Microsoft Active Directory e base de dados local.

7.5.34.2. Autencação Kerberos.

7.5.35. A capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários.

7.5.36. Integração com o Microsoft Active Directory, permitindo identificar usuários dentro de grupos, mesmo que estejam em uma hierarquia de grupo dentro de grupo.

7.5.37. Suporte a identificação de múltiplos usuários conectados, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão em uso.

7.5.38. Atualização da identificação de um usuário caso este mude de endereço IP e mesmo que mais de um dispositivo esteja sendo utilizado de forma simultânea, evitando a necessidade de que sejam configurados endereços fixos.

7.5.39. Suporte a QoS, contemplando:

7.5.39.1. A capacidade de controlar as aplicações por políticas de máximo de largura de banda por aplicação, tanto de áudio como de vídeo streaming.

7.5.39.2. A funcionalidade de configurar horários para navegação, permitindo controle por usuário e tempo.

7.5.39.3. A criação de políticas de QoS por usuário/grupo do LDAP/AD, aplicações (traffic shaping) e interface física ou lógica do equipamento.

7.5.39.4. Priorização de protocolos de voz e vídeo como H.323, SIP, SCCP, MGCP e aplicações como Skype, Teams, Hangout e similares.

7.5.40. Suporte a conformação de tráfego com, pelo menos, Traffic Policing. e Traffic Shaping.

7.5.41. Classificação de tráfego com no campo DSCP.

7.5.42. A marcação e priorização do tráfego previamente classificado com base no campo DSCP.

7.5.43. Suporte à VPN, contemplando:

7.5.43.1. VPN IPSec com capacidade de implementar túneis site-to-site do tipo hub-and-spoke.

7.5.43.2. O estabelecimento do túnel utilizando uma “chave secreta” ou certificados digitais.

7.5.43.3. Implementação de IKEv1 e IKEv2.

7.5.43.4. Suporte pelo menos aos seguintes algoritmos de criptografia: 3DES, AES-128, AES-192 e AES256.

7.5.43.5. Suporte pelo menos aos seguintes algoritmos de autenticação: MD5, SHA-1, SHA-256, SHA-384, SHA-512.

7.5.44. Filtro de URLs, contemplando:

7.5.44.1. Filtro de URL HTTP e HTTPS.

7.5.44.2. Filtro de conteúdo HTTP.

7.5.44.3. SSL Scanner.

7.5.44.4. Proxy transparente HTTP/HTTPS;

7.5.44.5. Cache de dados;

7.5.44.6. Bloqueio de acesso com mensagem customizada, de forma a permitir que o usuário solicite a liberação por meio de formulário ou justificava;

7.5.44.7. Monitoramento do tráfego internet independente de plataforma, sistema operacional ou aplicação.

7.5.44.8. Filtragem sem necessidade da instalação de agentes nas estações.

7.5.45. Controle de acesso à Internet, contemplando:

7.5.45.1. Regras baseadas tanto na requisição quanto na resposta HTTP.

7.5.45.2. Regras baseadas em horário do dia.

7.5.45.3. Controle de downloads/uploads de arquivos pelo nome, tipo ou extensão do arquivo.

7.5.45.4. Controle de acesso à Internet por domínio.

7.5.45.5. Controle de acesso à Internet por categorias de sites web.

7.5.45.6. Controle de acesso à Internet por lista de sites web proibidos (blacklist) customizável.

7.5.45.7. Controle de acesso à Internet por lista de sites web permitidos (whitelist) customizável.

7.5.45.8. Mecanismo automático para detecção e bloqueio em tempo real de tráfego (inbound/outbound) originado por códigos maliciosos tipo malwares ou spywares.

7.5.45.9. Mecanismo automático para detecção de tráfego tunelado na porta 80.

7.5.45.10. Páginas de erro e bloqueio customizáveis.

7.5.45.11. Compatibilidade com filtros de busca segura (safe-search filters), oferecidos por sites web de busca.

7.5.45.12. Controle de acesso por definição e aplicação das regras com expressões regulares.

7.5.45.13. Liberação/bloqueio de componentes específicos de sites de redes sociais, tais como chat e comentários do site www.facebook.com ou postagem no site www.twitter.com.

7.5.45.14. Controle de acesso por geolocalização.

7.5.46. Categorização de sites web, contemplando:

7.5.46.1. Base de dados com no mínimo 15 (quinze) milhões de URL's cadastradas, e pelo menos 45 (quarenta e cinco) categorias previamente definidas e possibilidade de criação de novas categorias personalizadas.

7.5.46.2. A classificação/categorização de sites de acordo com o assunto.

7.5.46.3. Mecanismo de cadastro de novas URLs junto ao fabricante para a devida categorização.

7.5.46.4. Mecanismo de reclassificação, quando necessário.

7.5.47. Atualização da base de sites, contemplando:

7.5.47.1. Atualização automática da base de sites pela solução, via Internet, em dias e horários customizáveis.

7.5.47.2. Atualização transparente, sem comprometer a execução dos serviços, principalmente no caso de falhas no acesso à base de sites.

7.5.47.3. Mecanismos de manutenção da base de sites incluindo a reclassificação de sites antes "maliciosos" que foram "descontaminados", para o retorno do acesso à normalidade.

7.5.48. Deverá oferecer acesso através de rede sem fio no próprio equipamento e/ou através de access-point adicional gerenciado localmente e monitorado pela mesma solução, contemplando, no mínimo:

7.5.48.1. Suporte aos padrões 802.11 b/g/n/ax de rede sem fio.

7.5.48.2. Banda dupla simultânea, nas frequências 2,4 GHz e 5 GHz.

7.5.48.3. Suporte à conexão mínima de 50 usuários simultâneos.

7.5.48.4. Alcance mínimo de 30 metros.

7.5.48.5. Filtro de controle de acesso baseado em endereço de rede.

7.5.48.6. Suporte a VLANS.

7.5.48.7. Suporte a múltiplos SSID.

7.5.48.8. Capacidade de isolamento de tráfego entre usuários no mesmo SSID.

7.5.48.9. Suporte à detecção de intrusos.

7.5.48.10. Log de acessos, com possibilidade de envio do log para servidor syslog.

7.5.48.11. Suporte à autenticação IEEE 802.1x em servidor Radius do Contratante.

7.5.49. Suportar os seguintes padrões de criptografia:

7.5.49.1. WPA, WPA2 e WPA3.

7.5.49.2. TKIP.

7.5.49.3. AES.

7.5.50. Deve ser possível criar políticas para a modelagem do tráfego definindo, pelo menos, os seguintes parâmetros:

7.5.50.1. IP de Origem.

7.5.50.2. IP de Destino.

7.5.50.3. Porta TCP/UDP de Destino.

7.5.50.4. URL de destino.

7.5.50.5. Aplicação de camada 7.

7.5.51. Deve permitir o provisionamento e configuração de maneira automática, sem a necessidade de intervenção manual, quando ligado e conectado à rede.

7.5.52. Todos os equipamentos, produtos, peças ou softwares que compõem a solução de telecomunicação deverão ser monitorados por serviço de gerenciamento de segurança proativo.

7.5.52.1. Os serviços de monitoramento de segurança serão realizados em regime de 24 horas por dia, sete dias por semana.

7.5.52.2. Deverá executa as ações necessárias à resposta aos incidentes de segurança identificados de forma a manter os serviços disponíveis e operacionais.

7.5.52.3. Deverá mapear e executar os processos de resposta dos incidentes de segurança ocorridos e registrar em base de conhecimento.

7.5.52.4. Deverá efetuar a manutenção das regras e políticas do parque monitorado para responder a incidentes.

7.5.52.5. Deverá informar ao Contratante incidentes de segurança da informação.

7.5.52.6. Deverá verificar, diariamente, a disponibilização, pelo fabricante, de patches, correções e versões ou releases mais recentes dos softwares empregados na solução.

7.5.52.7. Deverá comunicar à contratada a existência do patch juntamente com os respectivos problemas resolvidos e as novas funcionalidades disponibilizadas sempre que estiver disponível.

7.5.53. Deverá atualizar os módulos da solução, isto é, fornecer e instalar patches, correções e versões ou releases mais recentes dos softwares, sempre que autorizado pelo Contratante.

7.5.54. Deverá executar atividades de gestão, suporte, manutenção, administração e resolução de problemas, mudanças de regras e de configuração, de cada um componente da solução, remotamente ou on-site.

7.5.55. Deverá fazer o ajuste fino (tunning) de toda a solução, adequando-a ao ambiente do Contratante e às customizações de configuração necessárias para atender às suas necessidades.

7.5.56. Serão considerados incidentes de segurança qualquer ação que vise comprometer a integridade, a confidencialidade das informações ou a disponibilidade dos serviços de tecnologia da informação do Contratante, tais como:

7.5.56.1. Acessos indevidos.

7.5.56.2. Instalação de códigos maliciosos.

7.5.56.3. Indisponibilidade dos serviços (DoS e DDoS).

7.5.56.4. Ataques por força bruta.

7.5.56.5. Exploração de vulnerabilidades.

8. Da Contratação.

8.1. O objeto é constituído por uma solução global, tendo em vista a inviabilidade de fracionamento.

8.2. A prestação fragmentada da solução seria prejudicada com a contratação de empresas distintas, uma vez que todos os bens e serviços pretendidos estão intrinsecamente relacionados. Tal organização permite ganhos quanto à instalação, configuração e operacionalização de toda a solução.

9. Dos critérios de seleção do fornecedor.

9.1. Da qualificação técnica operacional.

9.1.1. Apresentar, para fins de qualificação técnico-operacional, atestado de capacidade técnica, expedido por pessoa jurídica de direito público ou privado, que comprove a execução satisfatória de fornecimento de serviço de PABX em nuvem com, no mínimo, 150 (cento e cinquenta) ramais.

9.2. Da qualificação econômico-financeira.

9.2.1. Apresentar, para fins de qualificação econômico-financeira, quando cabível, a certidão negativa de feitos sobre Falência e Concordata ou Execução Patrimonial, expedida pelo distribuidor da sede da licitante.

10. Do critério de julgamento.

10.1. O julgamento da licitação será realizado pelo critério do MENOR PREÇO GLOBAL, observadas as regras de aceitação das propostas fixadas neste termo de referência.

10.2. Os preços unitários finais e totais propostos deverão ser, no máximo, aqueles contidos na tabela de valores máximos de referência anexa ao edital da licitação.

10.3. Excepcionalmente, poderá ser acatado preço de cada serviço superior ao fixado na tabela de preços máximos de referência, desde que não haja sucesso na tentativa de negociação com o licitante e cujas circunstâncias demonstrem que é globalmente mais vantajoso para a Administração, mediante despacho fundamentado.

10.4. A proposta deverá ser apresentada na forma definida o Anexo B.

11. Do Pagamento.

11.1. Do prazo de pagamento:

11.1.1. O Contratante pagará à Contratada o valor correspondente à contratação, mediante depósito bancário em sua conta-corrente, até o 5º da útil subsequente ao atesto pelo setor competente deste Tribunal, desde que não haja fato impeditivo

provocado pela mesma, obedecida a ordem cronológica de exigibilidade, nos termos do art. 5º, da Lei nº 8.666/93.

11.2. Das condições para pagamento:

11.2.1. A Contratada deverá, junto a apresentação do documento fiscal, informar os dados do seu domicílio bancário (banco, agência e conta) para o correspondente pagamento.

11.2.2. A empresa optante pelo SIMPLES, para usufruir da isenção da retenção de tributos e contribuições estabelecida pela IN SRF n° 1234/2012, deverá apresentar declaração ORIGINAL (01) via na forma do Anexo IV daquela instrução normativa, JUNTO COM A NOTA FISCAL. CÓPIA NÃO É VÁLIDA.

11.2.3. A declaração de que trata o item anterior poderá ser apresentada por meio eletrônico, com a utilização de certificação digital disponibilizada pela Infraestrutura de Chaves Públicas Brasileira (ICPBrasil), desde que no documento eletrônico arquivado pela fonte pagadora conste a assinatura digital do representante legal e respectiva data da assinatura.

11.2.4. Havendo erro no documento fiscal ou circunstância que impeça a liquidação da despesa, aquele será devolvido à Contratada pelo Fiscal do contrato e o pagamento ficará pendente até que a mesma providencie as medidas saneadoras.

11.2.5. Todas as faturas emitidas pela contratada deverão possuir uma data de vencimento única.

11.2.6. Toda a cobrança indevida deverá ser tratada formalmente, e, caso necessário, deverá a contratada ressarcir ao contratante, valores indevidamente cobrados, mediante crédito em fatura a ser emitida no mês subsequente ao da cobrança indevida.

12. Da Contratação e dos prazos.

12.1. A contratada deverá, a partir da assinatura do contrato, e respeitando-se os prazos estipulados nas normas da ANATEL, tomar todas as providências necessárias à implantação da solução, de forma que a prestação dos serviços se inicie efetivamente, sem qualquer tipo de interrupção, em até 60 dias.

12.2. O prazo de início da prestação dos serviços admite prorrogação somente nos casos em que o motivo do atraso ocorrer por comprovado impedimento ou reconhecida força maior, devidamente justificado e aceito pela Administração do TRE-ES.

12.3. A solicitação de adiamento do prazo de início da prestação dos serviços deverá ser sempre por escrito, devendo ser recebida contemporaneamente ao fato que ensejá-lo.

12.4. Após a instalação das linhas, o funcionamento do serviço será conferido pelo setor competente, e constatada qualquer irregularidade, a empresa deverá providenciar o reparo ou substituição da linha, no prazo máximo de 48 horas após o recebimento da informação.

12.5. O contrato a ser celebrado terá duração de 60 (sessenta) meses.

13. Da implantação da solução.

13.1. A implantação da solução se dará de forma parcelada de acordo com cronograma de execução a ser elaborado pela Contratada em conjunto com a Contratante, em até 5 (cinco) dias após a assinatura do respectivo instrumento contratual.

14. Dos locais de implantação da solução.

14.1. Os locais estão contemplados no ANEXO C, bem como o quantitativo de equipamentos por local.

15. Do recebimento do objeto.

15.1. O recebimento do objeto será realizado pelas unidades técnicas da Contratante, podendo ser aceito ou rejeitado, no todo ou em parte, a cada execução, para efeito de posterior verificação de sua conformidade com as especificações constantes neste termo de referência e na proposta.

15.2. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser corrigidos/refeitos/substituídos no prazo fixado pelo fiscal do contrato, às custas da Contratada, sem prejuízo da aplicação de penalidades.

16. Das obrigações da contratada.

16.1. A licitante vencedora, sujeitar-se-á a mais ampla e irrestrita fiscalização por parte da Contratante, encarregada de acompanhar a execução.

16.2. Cumprir as demais disposições contidas neste termo de referência.

16.3. Manter comunicação formal com a instituição por meio de endereço eletrônico, o qual deve ser verificado diariamente e acusado o recebimento. Não o fazendo, no decurso de 5 (cinco) dias corridos, o seu silêncio será reputado como comunicação/notificação recebida.

16.4. Executar os serviços de acordo com os requisitos de quantidades, especificações técnicas, manuais de operação (quando couber) e demais condições consignadas nas propostas técnicas e/ou de preços, de acordo com Termo de Referência.

16.5. Executar os serviços impreterivelmente, nos prazos previstos, no local designado e conforme especificações constantes no Termo de Referência;

16.6. Comunicar à contratante, no prazo máximo de 02 (dois) dias úteis que antecedam o prazo de vencimento da execução, os motivos que impossibilitem o seu cumprimento;

16.7. Responsabilizar-se perante a Administração e terceiros, por ações ou omissões de seus empregados, prepostos e contratados, das quais resultem danos ou prejuízos a pessoas ou bens, não implicando corresponsabilidade da contratante.

16.8. Responsabilizar-se por todos os custos, diretos e indiretos, inclusive transporte e de pessoal, necessários à adequada e regular entrega dos materiais/bens contratados, em plena conformidade com os termos e especificações, inclusive prazos, horários e local de entrega, previstos neste Termo de Referência e anexos;

16.9. Pagar todos os tributos, contribuições fiscais e parafiscais que incidam ou venham a incidir, direta e indiretamente, sobre os produtos vendidos, bem como eventual custo de frete e entrega, inclusive seguro;

16.10. Assumir todos os encargos sociais, trabalhistas, fiscais, previdenciários e comerciais resultantes da execução contratual, bem como por eventuais demandas de caráter cível ou penal;

16.11. Manter, durante a vigência contratual, todas as condições de habilitação e qualificação exigidas na licitação correspondente, devendo comunicar à Administração, por escrito, qualquer normalidade de caráter urgente e prestar esclarecimentos julgados necessários;

16.12. Designar 01 (um) preposto com poderes de decisão para representar a CONTRATADA, principalmente no tocante à eficiência e agilidade na execução dos serviços objeto da contratação, devendo, também, disponibilizar Central de Atendimento da CONTRATADA para tratar dos casos abaixo:

16.12.1. Substituir equipamentos;

16.12.2. Configurar equipamentos CPE’s;

16.12.3. Prestar manutenções preventivas em acessos de dados;

16.12.4. Dirimir dúvidas em relação às funcionalidades dos equipamentos e serviços da CONTRATADA, diretamente com os gestores da conta da CONTRATANTE;

16.12.5. Disponibilizar treinamento aos gestores da CONTRATANTE, acerca da ferramenta de gerenciamento dos serviços de dados, a ser disponibilizada pela CONTRATADA, sem custos para a CONTRATANTE.

16.12.6. Auxiliar no processo de verificação das faturas (tarifas acordadas, identificação de valores, metodologia de cobrança), bem como operacionalização do programa disponibilizado, via WEB, pela CONTRATADA para controle do faturamento;

16.12.7. Facilitar a interação com o Consultor de Relacionamentos da CONTRATADA;

16.12.8. Agir sempre que solicitado em situações que surgirem, considerando o objetivo do Contrato;

16.12.9. Permitir comunicação com a CONTRATADA através do Gestor do Contrato na CONTRATANTE.

16.12.10. Responsabilizar-se integralmente pelo fornecimento dos serviços e materiais necessários à sua execução, nos prazos, nas quantidades e nos padrões de qualidade exigidos.

16.12.11. Providenciar a correção das falhas ou irregularidades constatadas pela CONTRATANTE na execução dos serviços, de acordo com os níveis de SLA exigidos pela CONTRATANTE, conforme Anexo A.

16.12.12. Responder por quaisquer interferências de estranhos nos acessos em serviço, bem como zelar pela integridade da comunicação.

16.13. Implantar, de forma adequada, a supervisão permanente dos serviços, de modo a obter uma operação correta e eficaz.

16.14. Projetar, dimensionar (hardwares, softwares e recursos humanos), implantar (instalar, ativar, configurar e ajustar), operacionalizar, gerenciar e manter os equipamentos de conectividade, telecomunicações e segurança utilizados na prestação de todos os serviços contratados.

16.15. Responder pelo cumprimento dos postulados legais vigentes no âmbito federal, estadual ou municipal, bem como, assegurar os direitos e cumprimento de todas as obrigações estabelecidas por regulamentação da ANATEL.

16.16. Fornecer mensalmente à CONTRATANTE as faturas com detalhamento individual de cada serviço contendo todas as despesas realizadas previstas no Contrato, cobrando os serviços efetivamente utilizados.

16.17. Comunicar à CONTRATANTE, por escrito, qualquer anormalidade nos serviços e prestar todos os esclarecimentos julgados necessários.

16.18. Não veicular em nenhuma hipótese, publicidade ou qualquer outra informação acerca da prestação dos serviços do Contrato, sem prévia autorização da CONTRATANTE.

16.19. Acatar as orientações da CONTRATANTE, sujeitando-se a mais ampla e irrestrita fiscalização, atendendo as reclamações formuladas.

16.20. Atender prontamente às solicitações de serviços de instalação, mudança de endereço, ampliação ou qualquer outro tipo de serviço eventualmente requisitado através de Ordem de Serviço.

16.21. Atender prontamente às convocações de reuniões presenciais e semanais para tratar de eventuais melhorias na prestação dos serviços objeto desta contratação, assim como para acompanhamento das solicitações de serviços e de reparos dos acessos de dados da CONTRATANTE.

16.22. Comunicar à CONTRATANTE, com antecedência mínima de 05 (cinco) dias, da ocorrência de interrupções temporárias, totais ou parciais dos serviços programados pela CONTRATADA para efetuar manutenções ou reparos de ordem técnica.

17. Das obrigações da contratante.

17.1. Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;

17.2. Exercer o acompanhamento e a fiscalização, por servidor especialmente designado, anotando em registro próprio as falhas detectadas e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

17.3. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução, fixando prazo para a sua correção, certificando-se que as soluções por ela propostas sejam as mais adequadas;

17.4. Receber os produtos de acordo com as especificações descritas neste documento, rejeitando, no todo ou em parte, o fornecimento executado em desacordo com o Contratado;

17.5. Pagar à Contratada o valor resultante da execução, no prazo e condições estabelecidas neste Termo de Referência;

17.6. Possibilitar o acesso da equipe técnica da CONTRATADA ao local de instalação dos equipamentos, orientando-a sobre dúvidas referentes às características técnicas do ambiente de instalação.

18. Da Lei Geral de Proteção de Dados Pessoais (LEI nº 13.709/2018)

18.1. É vedada às partes a utilização de todo e qualquer dado pessoal, repassado em decorrência da execução contratual, para finalidade distinta da contida no objeto da contratação, sob pena de responsabilização administrativa, civil e criminal.

18.2. Para fins de execução do objeto contratado e de cumprimento de obrigação legal ou regulatória, o Contratante poderá proceder ao tratamento dos dados pessoais dos representantes legais da Contratada, inclusive para publicação nos portais de Transparência do Contratante.

19. Do reajuste e revisão de preços.

19.1. Os preços referentes aos objetos contratados poderão ser reajustados com fulcro na Constituição Federal e da Lei 8.666/93.

19.2. O reajuste de preços deverá ser requerido pelo contratado, sob pena de preclusão.

20. Da fiscalização.

20.1. A fiscalização da contratação será exercida por um representante da Administração, ao qual competirá dirimir as dúvidas que surgirem no curso da execução do contrato, e de tudo dará ciência à Administração.

20.2. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da fornecedora, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

21. Das sanções administrativas.

21.1. Penalidades

Item	Descumprimento	Percentual diário	Limite de dias	Percentual total	Base de incidência
1	Atraso na entrega	0,5%	10	5%	Valor do objeto

2	Atraso excepcional de entrega	0,5%	10	5%	Valor do objeto
3	Atraso na reparação	2%	5	10%	Valor do objeto
4	Inexecução contratual	-	-	30%	Valor do objeto inexecutado

21.2. Outras Sanções com Grau de Severidade

21.2.1. Grau de Severidade Leve

L1 – Notificação de Descumprimento Contratual– Quando for o caso, a CONTRATADA será notificada e deve adequar-se à exigência contratual formalizada pela Equipe de Gestão Contratual em até10 (dez) dias úteis, contados a partir da data de recebimento da notificação. Findo o prazo e mantendo-se os motivos que levaram a notificação, a CONTRATADA estará sujeita a multa diária de 0,1% sobre o valor mensal do objeto, limitados ao total de até 30 (trinta) dias corridos, quando restará configurada uma inexecução contratual.

21.2.2. Grau de Severidade Moderado

M1 – Multa fixa (MLT-FIXA) de 2% sobre o valor mensal do objeto OU multa diária (MLT-DIÁRIA) de 0,2% sobre o valor mensal do objeto. Nos casos da multa diária, a CONTRATADA deve adequar-se em no máximo até 10 (dez) dias corridos, quando restará configurada uma inexecução contratual.

M2 – Multa fixa (MLT-FIXA) de 3% sobre o valor mensal do objeto ou multa diária (MLT-DIÁRIA) de 0,3% sobre o valor mensal do objeto. Nos casos da multa diária, a CONTRATADA deve adequar-se em no máximo até 5 (dias) dias corridos, quando restará configurada uma inexecução contratual.

M3 – Multa fixa (MLT-FIXA) de 5% sobre o valor mensal do objeto ou multa diária (MLT-DIÁRIA) de 0,5% sobre o valor mensal do objeto.Nos casos da multa diária, a CONTRATADA deve adequar-se em no máximo até 5 (cinco) dias corridos, quando restará configurada uma inexecução contratual.

21.2.3. Grau de Severidade Grave/Inexecução Contratual

Multa de 30% (trinta por cento) sobre o objeto inexecutado e ressarcimento à contratante o valor correspondente ao período inexecutado, com as devidas atualizações.;

G1 – Rescisão contratual

G2 – Suspensão por até 5 (cinco) anos de participação em licitação;

G3 – Declaração de inidoneidade para licitar ou contratar com a Administração Pública.

21.2.4. Relação de Eventos

A Relação de Eventos apresenta um conjunto não exaustivo dos eventos causadores de sanções contratuais. Para cada um dos eventos descritos, uma ou mais sanções poderão ser aplicadas. A tabela a seguir apresenta uma amostra do relacionamento de eventos e sanções. O número dentro da tabela descreve o número de vezes (primeira ocorrência e demais reincidências) que o evento ocorreu durante a vigência do contrato (nota-se que, de acordo com os critérios, a reincidência aumentará o grau de severidade).

RELAÇÃO DE EVENTOS							
Evento	Grau de Severidade						
	Leve	Moderado			Grave		
	L1	M1	M2	M3	Inexecução Contratual		
					G1	G2	G3
Apresentar documentação falsa					1ª	1ª	1ª
Não mantiver a Proposta					1ª	1ª	1ª
Fraudar a execução do contrato					1ª	1ª	1ª
Comportar-se de modo inidôneo					1ª	1ª	1ª
Fizer declaração falsa ou cometer fraude fiscal					1ª	1ª	1ª
Negar-se a assinar o contrato no prazo estabelecido					1ª	1ª	1ª
Não designar Preposto	1ª						
Não executar o repasse de conhecimento até o término da primeira semana após a implantação integral da solução.(MTL-DIÁRIA)				1ª			
Indisponibilidade dos serviços por período superior à 48 horas, cuja justificativa não for acatada pelo TRE/ES (MLT-DIÁRIA)				1ª em diante			
Deixar de cumprir determinação formal ou instrução do fiscalizador, por ocorrência		1ª	2ª a 4ª	6ª a 10ª	11ª		
Não responder dentro do prazo estabelecido os esclarecimentos solicitados pela fiscalização do contrato no que diz respeito ao cumprimento do objeto contratado, mesmo os de ordem técnica, operacional ou administrativa. (MLT-FIXA)	1ª	2ª	3ª	4ª a 10ª	11ª		
Deixar de comunicar formalmente à CONTRATANTE, com pelo menos **5 dias de antecedência**, sobre a indisponibilidade dos serviços.		1ª a 2ª	3ª a 4ª	5ª a 7ª	8ª		
Descumprir qualquer dispositivo do termo de sigilo, da política de segurança ou do código de ética da CONTRATANTE					1ª	1ª	1ª
Não guardar sigilo dos dados processados no					1ª	1ª	1ª

TRE/ES e/ou divulgar sem autorização formal do Gestor ou Fiscal Técnico do Contrato, informações tratadas nas dependências da CONTRATANTE.							
Deixar de comunicar formalmente a Equipe de Gestão Contratual as eventuais irregularidades (MLT-FIXA)		1ª	2ª	3ª	4ª		
Descumprimento total ou parcial das obrigações assumidas por mais de 30 (trinta) dias corridos para o caso de notificações L1, 10 (dez) dias corridos no caso de multas com grau de severidade M1 e 5 (cinco) dias corridos para multas com grau de severidade M2 e M3, cuja justificativa não for acatada pelo TRE/ES					1ª	1ª	1ª
Qualquer outra obrigação prevista não cumprida pela CONTRATADA. (MLT-FIXA ou MLT-DIÁRIA), conforme o caso	1ª	2ª	3ª	4ª em diante			

22. Do sigilo das informações cadastrais.

22.1. Todas as informações relativas à CONTRATANTE e constantes do cadastro da CONTRATADA deverão ser tratadas como confidenciais e somente poderão ser fornecidas quando solicitadas:

22.1.1. Pela CONTRATANTE;

22.1.2. Em decorrência de determinação judicial.

22.2. Os conhecimentos, dados e informações de propriedade do CONTRATANTE, relativos a aspectos econômico-financeiros, tecnológicos e administrativos, tais como produtos, sistemas, técnicas, estratégias, métodos de operação e todos e quaisquer outros, repassados por força do objeto do presente Termo de Referência, constituem informação privilegiada e como tal, tem caráter de confidencialidade, só podendo ser utilizados, exclusivamente, no cumprimento e execução das condições estabelecidas neste Contrato, sendo expressamente vedado à CONTRATADA:

22.2.1. Utilizá-los para fins outros, não previstos neste Instrumento;

22.2.2. Repassá-los a terceiros e empregados não vinculados diretamente ao objeto proposto.

23. Da disponibilidade e desempenho.

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

23.2. O serviço será considerado INDISPONÍVEL a partir do início de uma interrupção registrada na Central de Atendimento/Supervisão da CONTRATADA, feito por ela mesma, ou a partir da comunicação de interrupção feita pela CONTRATANTE via telefone para Abertura de Chamados de Falha / Inoperância de circuitos e/ou equipamentos (hardware e/ou software).

23.3. O prazo para atendimento às chamadas técnicas, durante a vigência do Contrato, para situações de indisponibilidade nos serviços, incluindo a reparação dos serviços, deverá ser de acordo com o Anexo A deste Termo de Referência.

23.4. A disponibilidade do serviço será calculada, para um período de 01 (um) mês, através da seguinte fórmula:

D = (T0 – Ti)/T0 x 100

Onde:

D = Disponibilidade;

T0 = período de operação (1 mês), em minutos;

Ti = tempo total de indisponibilidade do ponto de acesso, ocorrida no período de operação (1 mês), em minutos.

23.5. No cálculo de disponibilidade, não serão consideradas as interrupções programadas e aquelas de responsabilidade da CONTRATANTE.

23.6. No caso de falhas na prestação do serviço, ocorrência de interrupções ou anormalidades que afetem o desempenho e a segurança da rede e qualquer circuito e/ou equipamento (hardware e/ou software) serão de responsabilidade da CONTRATADA, que concederá desconto, de forma automática e sem intervenção da CONTRATANTE, na fatura do mês subsequente, conforme a equação seguinte, limitado ao valor da Fatura Mensal dos serviços prestados:

Desc = (P x I)/1440

Onde:

Desc = Valor do desconto em R$ (reais) relativo ao circuito dedicado indisponível.

P = Preço mensal em R$ (reais) do circuito.

I = Quantidade de períodos de 30 minutos que o serviço ficou indisponível.

1440 = número de 30 minutos existentes no mês.

23.7. Para efeito de desconto, o período de indisponibilidade a ser considerado será de 30 (trinta) minutos consecutivos. Os períodos de indisponibilidade, ainda que fração de 30 (trinta) minutos, serão considerados, para fins de desconto, como períodos inteiros de 30 (trinta) minutos.

23.8. Deverá ser entendido como tempo indisponível o tempo (em minutos) entre a abertura do chamado técnico pela CONTRATANTE ou pela CONTRATADA e a completa solução do incidente. Caso seja comprovado que o incidente foi causado pela CONTRATANTE ou o mesmo for considerado improcedente, o tempo de indisponibilidade não será computado no cálculo.

23.9. Havendo necessidade de interrupção do serviço para a realização de manutenções preventivas, a CONTRATADA deverá comunicar à CONTRATANTE com antecedência mínima de 05 (cinco) dias. Essas intervenções deverão ocorrer entre 00:00h e às 06:00h, incluindo os finais de semana, salvo negociação prévia entre as partes interessadas.

23.10. Serão excluídas do cálculo de indisponibilidade as interrupções programadas para manutenção, desde que a comunicação seja feita de acordo com os critérios do subitem anterior. Também serão excluídas as interrupções causadas por falta de energia elétrica nas localidades e indisponibilidades formalmente justificadas pela CONTRATADA e aceitas pela CONTRATANTE.

24. Da garantia, suporte e manutenção.

24.1. 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. Entende-se por operar: manter os recursos e os serviços de telecomunicações (central de atendimento, centro de gerência e supervisão, estrutura de manutenção e equipamentos de comunicação de dados) necessários para a efetiva funcionalidade da rede, considerando o ambiente operacional da CONTRATANTE e as atividades desenvolvidas neste ambiente relacionadas aos serviços contratados.

24.2. A CONTRATADA obriga-se, durante o prazo de vigência do Contrato, a garantir os equipamentos que fazem parte da solução proposta, incluindo assistência técnica e manutenção.

24.3. A CONTRATADA deverá prestar manutenção técnica especializada com atendimento dos requisitos técnicos abaixo relacionados:

24.4. Disponibilizar uma Central de Atendimento através de número telefônico de tarifação reversa, para que os usuários autorizados da CONTRATANTE façam registros de ocorrências, solicitações de reparo, bem como o acompanhamento da solução dos problemas, disponibilizando um número de ocorrência sempre que um chamado for efetuado. Esse atendimento deverá estar disponível 24 (vinte e quatro) horas por dia e 07 (sete) dias por semana, durante todo o ano.

24.5. A CONTRATADA deverá disponibilizar técnicos para realizar atividades de suporte à conectividade, isto é, disponibilizar recursos especializados para resolver problemas específicos de desempenho/integração, alterações das características e configurações, dentre outros serviços, em horário comercial. Caso seja necessária a realização dessas atividades fora do horário comercial, será negociado pela CONTRATANTE com a CONTRATADA.

24.6. O prazo para atendimento às chamadas técnicas, durante a vigência do Contrato, para situações de indisponibilidade nos serviços, incluindo a reparação dos serviços, deverá ser de acordo com o Anexo A deste Termo de Referência.

24.7. A CONTRATADA comprometer-se-á a designar profissionais plenamente capacitados para prestar suporte técnico à CONTRATANTE.

24.8. A execução de qualquer serviço pela CONTRATADA que possa interferir no funcionamento da Rede Corporativa da CONTRATANTE a qualquer tempo, deverá ser comunicada à CONTRATANTE com, pelo menos, 05 (cinco) dias úteis de antecedência e receber autorização formal, com o aceite expresso da CONTRATANTE, levando-se sempre em consideração o interesse desta.

24.9. Caso a CONTRATADA detecte alguma falha e/ou inoperância de qualquer circuito de dados instalados, a mesma deverá independente do registro do chamado técnico pela CONTRATANTE, tomar as devidas providências para a solução da anomalia.

24.10. O ingresso de pessoas não pertencentes ao corpo técnico da CONTRATADA, nas dependências da CONTRATANTE deverá ser comunicado via e-mail, com antecedência de, pelo menos, 02 (dois) dias úteis.

24.11. A CONTRATANTE poderá solicitar à CONTRATADA vistorias preventivas nos circuitos de dados, quando identificar problemas de desempenho, tendo a CONTRATADA obrigação de realizá-las e apresentar relatórios técnicos em, no máximo, 05 (cinco) dias úteis após cada solicitação.

25. Do sistema de gestão de contas.

25.1. A CONTRATADA deverá disponibilizar um sistema de gestão de contas online, sem ônus à CONTRATANTE, que ofereça, no mínimo, as funcionalidades a seguir:

25.1.1. Deverá ser acessado via web e compatível com navegadores padrão de mercado, tais como: Internet Explorer, Microsoft Edge, Google Chrome e Mozilla Firefox;

25.1.2. Deverá utilizar o protocolo HTTPS para acesso ao portal;

25.1.3. Deverá ser em idioma português do Brasil;

25.1.4. Deverá disponibilizar manual de utilização para auxílio dos usuários;

25.1.5. Deverá possuir alerta para acesso à área exclusiva de notificações para o usuário;

25.1.6. Deverá possuir recurso de enviar notificações de novas contas para o e-mail aos usuários;

25.1.7. Deverá armazenar os dados históricos de contas pelo período mínimo de 04 (quatro) meses no sistema para acesso imediato, podendo ser solicitado à CONTRATADA o envio de qualquer fatura por e-mail a qualquer momento, quando se fizer necessário;

25.1.8. Deverá permitir visualizar as contas de todos os serviços contratados;

25.1.9. Deverá possuir, no mínimo, 03 (três) níveis de usuários com as seguintes permissões:

25.1.10. Nível 1 – Será o administrador principal da CONTRATANTE, possuindo a maior hierarquia e poderá executar as funções de criação/exclusão de usuários, visualização/alteração de relatórios, visualização de faturas e associação de usuários aos contratos/serviços.

25.1.11. Nível 2 – Será o administrador de contas, possuindo as mesmas atribuições de Nível 1, com exceção de alteração de relatórios, ou seja, poderá apenas visualizar.

25.1.12. Na plataforma deverá possibilitar a criação de usuários via o perfil Nível 1, sendo que o novo usuário deverá receber uma notificação por e-mail para completar seu cadastro e ser ativado na plataforma

25.1.13. A plataforma deverá prever um limite de, no máximo, 07 (sete) dias para que o novo usuário possa completar seu cadastro e ativar o usuário. Caso o prazo seja expirado, o convite deverá ser reenviado e permitir que o gestor administrativo tenha autonomia de criar ou cancelar qualquer perfil que precise e a qualquer momento;

25.1.14. Deverá prever que o usuário, com perfil administrativo, possa visualizar Contas/Contratos de mais de um CNPJ/Razão Social, podendo ter perfis diferentes por CNPJ/Razão Social;

25.1.15. Deverá permitir que o usuário, com perfil administrativo, possa criar todo e qualquer perfil;

25.1.16. Deverá permitir, via portal, a redefinição da senha de acesso dos usuários;

25.1.17. Deverá possuir filtro para visualização de dados com, pelo menos: Produto, CNPJ e Nome do Órgão/Entidade;

25.1.18. Deverá possuir sinalização para controle de leitura de contas;

25.1.19. Deverá permitir a exportação de contas nos formatos PDF e FEBRABAN;

25.1.20. Deverá permitir a exportação de contas em massa;

25.1.21. Deverá oferecer visualização de, no mínimo, os seguintes campos:

25.1.21.1. Tipo do Documento.

25.1.21.2. CNPJ.

25.1.21.3. Razão Social do Cliente.

25.1.21.4. Data de Vencimento.

25.1.21.5. Data Disponibilização da Conta.

25.1.21.6. Valor Total.

25.1.21.7. Mês de Referência da Conta.

25.1.22. Deverá sempre apresentar a conta atual válida. Caso haja mudança na conta/fatura em virtude de contestações, o portal deverá apresentar a conta ajustada com um flag para diferenciação.

25.1.23. A CONTRATADA deverá promover treinamento à CONTRATANTE para, no mínimo, 05 (cinco) pessoas e no máximo 10 (dez) pessoas com instrutores devidamente capacitados e todo o material necessário.

25.1.24. O treinamento deverá ocorrer nas dependências da CONTRATANTE ou de modo remoto, por webconferência.

25.1.25. O portal ofertado deverá substituir as contas físicas, que não precisarão ser enviadas para a CONTRATANTE.

25.1.26. A CONTRATADA deverá enviar as contas detalhas por meio digital, via e-mail ou aplicativo instalado no computador da CONTRATANTE.

26. Das considerações finais.

26.1. Será admitida subcontratação, conforme disposto neste Termo de Referência, exclusivamente ao item 6.8, não eximindo a responsabilidade da CONTRATADA, observada a qualidade, a fidelidade ao objeto e a garantia sobre a totalidade dos serviços prestados, cabendo-lhe também a devida supervisão e coordenação dessas atividades.

ANEXO A – ACORDO DE NÍVEIS DE SERVIÇO

Abaixo estão listados os acordos de níveis de serviço exigidos para cada um dos serviços constantes no objeto deste Termo de Referência:

Tabela 1 – Instalação do Serviços

SERVIÇO	PRAZO MÁXIMO EM DIAS DE INSTALAÇÃO	PRAZO EM HORAS DE REPARO
Plataforma de PABX em Nuvem	60 dias	Ver Tabela 4
Acesso ao STFC (Entroncamento Digital E1)	60 dias	06 horas
Acesso IP Dedicado à Plataforma em Nuvem	45 dias	06 horas

Tabela 2 – Alteração de Endereço e Serviço de Wi-fi

SERVIÇOS AUXILIARES	PRAZO MÁXIMO EM DIAS DE EXECUÇÃO
Alteração de Endereço de Acesso IP Dedicado à Plataforma de Nuvem	60 dias
Instalação de Wi-fi	60 dias

Tabela 3 – Disponibilidade dos enlaces de acesso ao PABX em nuvem

SOLUÇÃO	NÍVEL DE SERVIÇO	DEDUÇÃO POR DESCUMPRIMENTO
Enlace IP unidade remota (Anexo C.2)	Disponibilidade mensal de 97%.	Desconto de 0,1432% por hora de indisponibilidade sobre o valor mensal do enlace a cada ciclo de pagamento após a tolerância de 21,6 horas de indisponibilidade.
	Latência média de 100 ms (a cada hora)	Desconto de 0,05% por hora de latência média superior a 100 ms a cada ciclo de pagamento.
Enlace de acesso na Sede do Tribunal (Anexo C.1)	Disponibilidade mensal de 99,5%.	Desconto de 0,1396% por hora de indisponibilidade sobre o valor mensal do enlace a cada ciclo de pagamento após a tolerância de 3,6 horas de indisponibilidade.
	Latência média de 50 ms (a cada hora)	Desconto de 0,05% por hora de latência média superior a 50 ms a cada ciclo de pagamento.

Tabela 4 – Interrupção de Serviços

Item	Atividade ou Serviço	Métrica	Prazo
1	• Paralisação total do sistema comprometendo os recursos disponíveis (componentes do core, periféricos ou aplicação); • Interrupção de serviço essencial para o negócio do cliente, classificada como situação de emergência.	Prazo em horas úteis após confirmação de recebimento de chamado	6
2	• Paralisação parcial do sistema comprometendo até 50% dos recursos disponíveis (componentes do core, periféricos ou aplicação), exceto falhas isoladas (um usuário ou pequeno grupo de usuários) que não resultem em impacto na operação global do equipamento.	Prazo em horas úteis após confirmação de recebimento de chamado	10
3	• Manutenção corretiva em falhas isoladas (não crítico que causa impacto mínimo ou nulo no desempenho do sistema); • Atendimento agendado; • Programação de pequeno, médio ou grande porte; • Requisição de serviço ou situação que não se enquadre na condição de severidade alta ou média.	Prazo em horas úteis após confirmação de recebimento de chamado	72

Para todos os serviços:

Os prazos de instalação começam sua contagem a partir da respectiva emissão da Ordem de Serviço.

Os prazos de reparo começam sua contagem a partir do momento da abertura do chamado junto à Central de Atendimento da CONTRATADA e emissão do respectivo número do chamado.

ANEXO B – PLANILHA DE PREÇOS

PLANILHA DE PREÇOS					
ESTIMATIVA SERVIÇO DE PLATAFORMA PABX EM NUVEM					
ITEM	DESCRIÇÃO	QUANT. ESTIMADA	VALOR MENSAL UNITÁRIO	VALOR MENSAL TOTAL	VALOR TOTAL PARA 60 MESES (A)
1	Licença de Ramal Tipo 1	367	R$23,74	R$8.712,58	R$522.754,80
2	Licença de Ramal Tipo 2	8	R$27,36	R$218,88	R$13.132,80
3	Licença de URA	10	R$27,86	R$278,60	R$16.716,00
4	Licença Atendente de Call Center	30	R$138,41	R$4.152,30	R$249.138,00
5	Licença de Supervisor de Call Center	1	R$195,57	R$195,57	R$11.734,20
6	Aluguel de Aparelho IP	375	R$24,69	R$9.258,75	R$555.525,00
7	Aluguel de Headset	30	R$17,37	R$521,10	R$31.266,00
8	Funcionalidade de Gravação (por ramal)	30	R$32,57	R$977,10	R$58.626,00
9	Entroncamento Digital E1 SIP com 30 canais e 50 ramais DDR	4	R$1.304,35	R$5.217,40	R$313.044,00
10	Blocos Adicionais de 50 ramais DDR	4	R$50,00	R$200,00	R$12.000,00
11	Link IP Dedicado 10 Mbps	51	R$1.076,35	R$54.893,85	R$3.293.631,00
12	Link IP Dedicado 20 Mbps	13	R$1.398,05	R$18.174,65	R$1.090.479,00
13	Link IP Dedicado 50 Mbps	11	R$1.793,76	R$19.731,36	R$1.183.881,60
14	Link IP Dedicado Sede 700 Mbps	1	R$4.898,80	R$4.898,80	R$293.928,00
15	Equipamento SD-WAN Sede	2	R$970,70	R$1.941,40	R$116.484,00
16	Equipamento SD-WAN Unidades Remotas	75	R$456,80	R$34.260,00	R$2.055.600,00
17	Equipamento WiFi	6	R$121,73	R$730,38	R$43.822,80
18	Solução de gerência centralizada	1	R$2.500,00	R$2.500,00	R$150.000,00

19	Serviço de Gerenciamento do Link Dedicado	77	R$220,00	R$16.940,00	R$1.016.400,00
VALOR TOTAL 60 MESES					R$11.028.163,20

ANEXO C – LOCALIDADES E PERFIS DE ACESSO

C.1 - DEMANDA ESTIMADA DA SEDE DO TRIBUNAL										
ID	Unidade Eleitoral	Município	Quantidade de licenças (ramais)	Link IP Dedicado com Roteador *	Roteadores Wi-fi **	Licença de Ramal Tipo 1	Licença de Ramal Tipo 2	Aluguel de Aparelho IP	Aluguel de Headset	Endereço
1	Sede e anexo do TRE/ES	VITÓRIA	240	700 Mbps	0	232	8	240	30	Avenida João Batista Parra, nº 575 – Praia do Suá Vitória/ES - CEP 29052-123

C.2 - DEMANDA ESTIMADA DAS UNIDADES REMOTAS								
ID	Unidade Eleitoral	Município	Quantidade de licenças (ramais)	Link IP Dedicado com Roteador *	Roteadores Wi-fi **	Licença de Ramal Tipo 1	Aluguel de Aparelho IP	Endereços
1	01ª ZONA ELEITORAL	VITÓRIA	3	50 Mbps	3	3	3	Rua Muniz Freire, s/nº, 3º andar, Fórum Muniz

								Freire, Cidade Alta - Vitória/ES - CEP. 29015-140
2	02ª ZONA ELEITORAL	CACHOEIRO DE ITAPEMIRIM	3	20 Mbps	0	3	3	Av.Gov. Francisco Lacerda de Aguiar, nº 221, Gilberto Machado, Cachoeiro de Itapemirim/ES - CEP 29303-383
3	03ª ZONA ELEITORAL	CASTELO	2	10 Mbps	0	2	2	Avenida Nsa. Sra. da Penha, nº 790, Centro - Castelo/ES - CEP. 29360-000
4	04ª ZONA ELEITORAL	ALEGRE	2	10 Mbps	0	2	2	Rua Oscar de Almeida Gama, nº 263, Centro - Alegre/ES CEP. 29500-000
5	05ª ZONA ELEITORAL	MIMOSO DO SUL	2	10 Mbps	0	2	2	Rua Gervásio Monteiro, 105, Centro , Mimoso do Sul/ES - CEP 29400-000
6	06ª ZONA ELEITORAL	COLATINA	3	20 Mbps	0	3	3	Avenida Vitória, nº 44, Maria das Graças - Colatina /ES CEP. 29705-021
7	07ª ZONA ELEITORAL	BAIXO GUANDU	2	10 Mbps	0	2	2	Rua Madame Albertina Holz, nº 79, Centro Baixo Guandu / ES - CEP. 29730-000
8	Posto Laranja da Terra	LARANJA DA TERRA	1	10 Mbps	0	1	1	Avenida luiz obermuller Filho, 85, Centro, Laranja da Terra/ES CEP: 20615-000

9	08ª ZONA ELEITORAL	AFONSO CLÁUDIO	2	10 Mbps	0	2	2	Rua Anália Vieira de Souza, 275, São Vicente - Afonso Cláudio/ES CEP. 29600-000
10	09ª ZONA ELEITORAL	SANTA LEOPOLDINA	2	20 Mbps	0	2	2	Ladeira Rosalina Ribeiro Nunes, s/n, Centro, Santa Leopoldina - CEP 29640-000
11	Posto Santa Maria de Jetibá	SANTA MARIA DO JETIBÁ	1	10 Mbps	0	1	1	Rua Augusto Jacob, 33,Centro - Santa Maria de Jetibá
12	10ª ZONA ELEITORAL	IBATIBA	2	10 Mbps	0	2	2	Rua Cantídio Roberto de Morais, nº 144, Novo Horizonte - Ibatiba/ES CEP.29395-000
13	Posto Brejetuba	BREJETUBA	1	10 Mbps	0	1	1	Av. Ângelo Uliana, s/n - Bairro: Uliana - Brejeturba/ES
14	11ª ZONA ELEITORAL	SANTA TERESA	2	10 Mbps	0	2	2	Avenida José Ruschi, nº 37, Centro - Santa Teresa /ES CEP. 29650-000
15	Posto Itarana	ITARANA	1	10 Mbps	0	1	1	Praça Ana Matos, nº 50 - Centro, Itarana/ES
16	12ª ZONA ELEITORAL	ALFREDO CHAVES	1	10 Mbps	0	1	1	Rua Lauro Ferreira Pinto, nº 575, Centro - Alfredo Chaves / ES CEP. 29240-000
17	13ª ZONA ELEITORAL	GUAÇUÍ	2	10 Mbps	0	2	2	Rua Emiliana Emery, nº 41, Ljs. 01 e 02, Centro - Guaçuí - ES CEP. 29560-

								000
18	14ª ZONA ELEITORAL	IBIRAÇU	2	10 Mbps	0	2	2	Rua Arlindo Vicente, nº 221 – Térreo - Ericina - Ibiraçu / ES CEP 29670-000
19	15ª ZONA ELEITORAL	DOMINGOS MARTINS	2	10 Mbps	0	2	2	RUA PRESIDENTE VARGAS, Nº 242, Loja B, Centro, Domingos Martins/ES - CEP 29.260-000
20	16ª ZONA ELEITORAL	ITAGUAÇU	1	10 Mbps	0	1	1	Av. 17 de Fevereiro, nº 240, Centro - Itaguaçu / ES CEP. 29690-000
21	Posto São Roque do Canaã	SÃO ROQUE DO CANAÃ	1	10 Mbps	0	1	1	Rua Lourenço Roldi, 88, São Roquinho, São Roque do Canaã/ES CEP 29.665-000
22	17ª ZONA ELEITORAL	ANCHIETA	2	10 Mbps	0	2	2	Rodovia do Sol, nº 2273, Ljs 04 e 05, Ed.Parmagnani e Silva, Justiça II, Anchieta/ES - CEP 29230-000
23	Posto Piúma	PIÚMA	1	10Mbps	0	1	1	Av. Eduardo Rodrigues, 58 - Acaiaca – CEP: 29.285-000
24	18ª ZONA ELEITORAL	IÚNA	2	10 Mbps	0	2	2	Av. Deputados João Rios, 372, Centro, Iúna / ES CEP. 29390-000
25	Posto Ibitirama	IBITIRAMA	1	10 Mbps	0	1	1	Rua Edgar Santana Alves, nº 54, Centro -

								Ibitirama/ES - CEP 29540-000
26	19ª ZONA ELEITORAL	MUNIZ FREIRE	1	10 Mbps	0	1	1	Rua Feniano Mitleg, nº 36, Centro - Muniz Freire / ES CEP. 29380-000
27	Posto Irupi	IRUPI	1	10 Mbps	0	1	1	Rua Laurentina Miranda Leal, 245, Centro, Irupi – CEP 29.398-000
28	20ª ZONA ELEITORAL	ARACRUZ	2	20 Mbps	0	2	2	Rua Isaura Sfalsin Rosa, 15, Jequitibá - Aracruz/ES CEP. 29193-084
29	21ª ZONA ELEITORAL	SÃO MATEUS	3	20 Mbps	0	3	3	Rua Cel. Constantino Cunha, 1262, Bairro de Fátima, São Mateus/ES CEP.29933-530
30	22ª ZONA ELEITORAL	ITAPEMIRIM	2	10 Mbps	0	2	2	Rua Melchíades Félix de Souza, nº 150, Serramar - Itapemirim / ES CEP. 29330-000
31	23ª ZONA ELEITORAL	BARRA DE SÃO FRANCISCO	2	20 Mbps	0	2	2	Rua Deolindo Dazílio, nº 03, Centro - Barra de São Francisco/ES - CEP 29960-000
32	Posto Água Doce do Norte	ÁGUA DOCE DO NORTE	1	10 Mbps	0	1	1	Rua Alacy Costa, s/n, Centro, Ginásio de Esportes, Água Doce do Norte
33	24ª ZONA ELEITORAL	GUARAPARI	3	20 Mbps	0	3	3	Rua Santana do Iapó, nº 330, Muquiçaba - Guarapari / ES CEP.

								29215-020
34	25ª ZONA ELEITORAL	LINHARES	2	50 Mbps	0	2	2	Av. Aracruz, nº 810, Colina, Linhares / ES CEP. 29900-399
35	26ª ZONA ELEITORAL	SERRA	3	50 Mbps	0	3	3	Rua Floriano Peixoto, 205, São Judas Tadeu, Serra-ES CEP 29.177-008
36	27ª ZONA ELEITORAL	CONCEIÇÃO DA BARRA	1	20 Mbps	0	1	1	Av. Jones dos Santos Neves, nº 264, Centro - Conceição da Barra ES-CEP.29960-000
37	Posto Pedro Canário	PEDRO CANÁRIO	1	10 Mbps	0	1	1	Av. Amália Negreiro de Castro, nº 275, Centro - Pedro Canário / ES CEP. 29970-000
38	30ª ZONA ELEITORAL	NOVA VENÉCIA	2	20 Mbps	0	2	2	Rua Vicente Alves de Oliveira, n. 71, bairro Beira Rio, Nova Venécia/ES - CEP: 29.830-000.
39	Posto Eleitoral Vila Pavão	VILA PAVÃO	1	10 Mbps	0	1	1	Rua Vasco Coutinho, nº 28 (Sec.da Cultura), Centro, Vila Pavão/ES - CEP 29843-000
40	32ª ZONA ELEITORAL	VILA VELHA	3	50 Mbps	0	3	3	Rua Quinze de Novembro, nº 288, Praia da Costa - Vila Velha /ES CEP. 29101-055
41	33ª ZONA ELEITORAL	ECOPORANGA	1	10 Mbps	0	1	1	Rua Otília da Costa, nº 49, Centro, Ecoporanga / ES

								CEP. 29850-000
42	34ª ZONA ELEITORAL	CARIACICA	3	50 Mbps	0	3	3	Avenida Getúlio Vargas, nº 107, Campo Grande - Cariacica / ES CEP. 29146-070
43	35ª ZONA ELEITORAL	ICONHA	2	10 Mbps	0	2	2	Avenida Danilo Monteiro Castro, nº 206, Centro Iconha / ES CEP. 29280-000
44	Posto Vargem alta	VARGEM ALTA	1	10 Mbps	0	1	1	Rua Willian Rose, 120 - Centro, Vargem Alta - ES, 29295-000
45	36ª ZONA ELEITORAL	PANCAS	1	10 Mbps	0	1	1	Rua Jovino Nonato da Cunha, s/nº, Beco do Ade, Lj.02,Centro-Pancas/ES CEP. 29750-000
46	Posto Eleitoral Mantenópolis	MANTENÓPOLIS	1	10 Mbps	0	1	1	Rua Floriano Rubim, s/nº, Centro - Mantenópolis / ES CEP. 29770-000
47	Posto Eleitoral Alto Rio Novo	ALTO RIO NOVO	1	10 Mbps	0	1	1	Rua Paulo Martins, 276, (Fórum) Centro - Alto Rio Novo
48	37ª ZONA ELEITORAL	SÃO GABRIEL DA PALHA	2	20 Mbps	0	2	2	Av. Lions Club, 252, Centro -São Gabriel da Palha/ES CEP. 29780-000
49	Posto Vila Valério	VILA VALÉRIO	1	10 Mbps	0	1	1	Avenida Padre Francisco, nº 217 - 15, Bairro Boa Vista - Vila Valério - ES 29785-000
50	38ª ZONA	MONTANHA	1	10 Mbps	0	1	1	Avenida Antônio Paulino,

	ELEITORAL							470, Centro, Montanha / ES CEP. 29890-000
51	39ª ZONA ELEITORAL	PINHEIROS	1	10 Mbps	0	1	1	Rua Matias Barbosa dos Santos, nº 187, Centro - Pinheiros / ES CEP. 29980-000
52	Posto Boa Esperança	Boa Esperança	1	10 Mbps	0	1	1	Av. Senador Eurico Resende, 780, centro, CEP. 29.845-000.
53	40ª ZONA ELEITORAL	VENDA NOVA DO IMIGRANTE	2	10 Mbps	0	2	2	Rua Gregório Zandonade, nº 15, Marmim,Venda Nova do Imigrante/ES CEP. 29375-000
54	Posto Conceição de Castelo	CONCEIÇÃO DO CASTELO	1	10 Mbps	0	1	1	Av. José Grilo, nº 348, Centro - Conceição do Castelo - CEP 29370-000
55	41ª ZONA ELEITORAL	JAGUARÉ	1	10 Mbps	0	1	1	Rua Ângelo Brioschi, s/nº, Centro - Jaguaré - CEP 29950-000
56	Posto Sooretama	SOORETAMA	1	10 Mbps	0	1	1	Rua Basílio Cerri,44, Térreo - Centro - Sooretama - CEP: 29927-000
57	43ª ZONA ELEITORAL	MARATAÍZES	1	20 Mbps	0	1	1	Rua Rubens Rangel, nº 1574, Lojas 04 e 05, Cidade Nova, Marataízes/ES
58	Posto Presidente Kennedy	PRESIDENTE KENNEDY	1	10 Mbps	0	1	1	Rua Átila Vivácqua Vieira, nº 148, térreo - Centro - Presidente Kennedy / ES -

								CEP.29350-000
59	44ª ZONA ELEITORAL	BOM JESUS DO NORTE	2	10 Mbps	0	2	2	Rua Carlos Xavier, nº 527, Centro, Bom Jesus do Norte/ES CEP.29460-000
60	Posto de Dores do Rio Preto	DORES DO RIO PRETO	1	10 Mbps	0	1	1	Av. Firmino Dias, nº 222, Centro, Dores do Rio Preto/ES CEP. 29.580-000
61	46ª ZONA ELEITORAL	ÁGUIA BRANCA	1	10 Mbps	0	1	1	Av. João Quiuqui, nº 444, Centro, Águia Branca / ES CEP 29795-000
62	Posto Marilândia	MARILÂNDIA	1	10 Mbps	0	1	1	Rua Espírito Santo, 79 - Centro - Marilândia -CEP 29725-000
63	Posto São Domingos do Norte	SÃO DOMINGOS DO NORTE	1	10 Mbps	0	1	1	Rodovia ES 080, KM 44 (Rod. do Café ou Rod. Gether Lopes de Farias) - CEP: 29.745-000
64	47ª ZONA ELEITORAL	VIANA	2	20 Mbps	0	2	2	Rua Aspázia Dias Varejão, 222, Viana Sede / ES - CEP. 29130-013
65	48ª ZONA ELEITORAL	CACHOEIRO DE ITAPEMIRIM	2	20 Mbps	0	2	2	Av. Gov. Francisco Lacerda de Aguiar, nº 221, Gilberto Machado, Cachoeiro de Itapemirim/ES CEP 29303-381
66	51ª ZONA ELEITORAL	RIO BANANAL	1	10 Mbps	0	1	1	Rua João Cipriano, nº 409, Lj. 02, São Sebastião - Rio Bananal / ES CEP 29920-000

67	Posto Gov. Lindemberg	GOV. LINDEMBERG	1	10 Mbps	0	1	1	Rua Delmira de Aguiar, nº 54, Centro - Gov.Lindemberg/ES - CEP 29720-000
68	52ª ZONA ELEITORAL	VITÓRIA	3	50 Mbps	3	3	3	Av. José Mª Vivácqua Santos,nº 600, Jardim Camburi Vitória/ES CEP. 29090-160
69	53ª ZONA ELEITORAL	SERRA	3	50 Mbps	0	3	3	Av. Des. Mário da Silva Nunes, n.º 1420, loja 2 Jardim Limoeiro, Serra/ES CEP. 29164-044
70	54ª ZONA ELEITORAL	CARIACICA	3	50 Mbps	0	3	3	Rodovia Governador José Sette, s/n, Itacibá, Cariacica / ES CEP 29150-410
71	55ª ZONA ELEITORAL	VILA VELHA	3	50 Mbps	0	3	3	Rua Coronel Sodré, nº 512, Centro, Vila Velha/ES-CEP 29100-080
72	57ª ZONA ELEITORAL	VILA VELHA	3	50 Mbps	0	3	3	Av. Nsa Sra. da Penha, nº 230, Ibes - Vila Velha / ES CEP 29108-330
73	59ª ZONA ELEITORAL	SERRA	3	50 Mbps	0	3	3	Av. Abidd Saad, nº 1296, Ljs 08,09 e 10 Jacaraípe – Serra / ES CEP 29175-520
74	Almoxarifado auxiliar	VITÓRIA	1	10 Mbps	0	1	1	Avenida João Batista Parra, nº 351, Praia do Suá/ES
75	Depósito de Urnas	VITÓRIA	1	10 Mbps	0	1	1	Av. José Mª Vivácqua Santos, nº 600, Jardim

								Camburi Vitória/ES CEP. 29090-160

* O roteador disponibilizado com o link de acesso deve ter a função wi-fi habilitada e funcional.

** Quantitativo de roteadores wi-fi para expansão de área. Não está incluído neste quantitativo o roteador principal com wi-fi.

ANEXO D – QUADRO RESUMO COMUNICAÇÃO PABX EM NUVEM

QUADRO RESUMO

ITEM	ENLACE		Alteração de Endereço	WI-FI	Infra Elétrica
	PERFIL	QTDE.			
Comunicação - SEDE	700 Mbps	1	--	0	--
Comunicação – Unidades Remotas	10 Mbps	51	--	0	--
	20 Mbps	13	--	0	--
	50 Mbps	11	--	6	--
TOTAIS		**76**	**--**	**6**	**--**
Serviços de alteração de endereço estimados para a vigência contratual	--	--	30 **	--	--
Equipamentos WI-FI adicionais estimados para a vigência contratual	--	--	--	154*	--

* A serem solicitados por demanda.

** previsão dentro dos 60 meses.

Em 21 de março de 2023.