I - ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1 – DEFINIÇÃO E ESPECIFICAÇÃO DOS REQUISITOS

Requisitos de negócio

- Adquirir equipamentos de conexão de rede cabeada e rede sem fio com instalação, garantia, suporte e gerência centralizada.
- Ter uma estrutura de rede com requisitos de segurança que combata acesso não autorizado aos recursos de rede do TRE-MA.
- Substituir equipamentos que se encontram fora de garantia e sem suporte pelo fabricante conforme doc. PAD nº 088448/2019 que demonstra que todos os equipamentos não são mais fabricados e com suporte de hardware e software expirados entre os anos de 2006 e 2018. O referido documento foi retirado do sítio da Avaya que é o fabricante da solução de rede deste regional.

Requisitos de garantia e de instalação

- Garantia de no mínimo 05 (cinco) anos para os equipamentos e ferramenta de gerência, incluindo a atualização de software (correções, "patches", "updates" ou novas "releases").
- Todas as despesas necessárias para a prestação do serviço, que inclui instalação, configuração e suporte no prazo de garantia, já devem estar contempladas no valor do contrato, tais como utilização de equipamentos, translado e estadia de técnicos da CONTRATADA.

Requisitos de experiência e formação profissional da equipe

- O atendimento deverá ser realizado por pessoal técnico especializado na instalação e configuração nos equipamentos e softwares descritos no objeto da licitação.

Requisitos técnicos

A solução da rede cabeada será composta de pilha de switches "core" onde serão ligados os equipamentos do datacenter, as fibras ópticas que interligam as pilhas de switches dos prédios anexo, Fórum eleitoral, as pilhas dos andares e softwares de análise e gerência de rede e a solução de rede sem fio será composta de appliance de gerência físico ou virtual, access points e fontes POE. A solução para o "core" poderá ser proposta em switches modulares, desde que contemple a quantidade de portas mínimas especificadas.

1. CONDIÇÕES GERAIS

1.1. Todos os itens ofertados em cada lote, deverão ser do mesmo fabricante para garantir total compatibilidade sem utilização de modo de interoperabilidade na solução;

1.2. Todos os componentes a serem utilizados ou integrados com os equipamentos da solução, devem ser do próprio fabricante ou estar em conformidade com a política de garantia do mesmo, não sendo permitida a integração de itens de terceiros que possam acarretar em perda parcial da garantia ou não realização da manutenção técnica pelo próprio fabricante quando solicitada.

1.3. Ser fornecido com configuração de CPU e memória (RAM e FLASH) suficiente para implementação de todas as funcionalidades descritas neste documento.

1.4. Os equipamentos devem ser novos e estar em produção. Não serão aceitos equipamentos descontinuados, recondicionados ou usados;

1.5. Os equipamentos devem ser entregues acondicionados adequadamente em suas embalagens originais;

1.6. A solução de gerenciamento ofertada, deverá ser baseada em plataforma "On Premise" (baseada em hardwares físicos que ficam armazenados em nossa infraestrutura), ou seja, deverá ser executada localmente, não sendo aceitas soluções híbridas ou em Cloud;

1.7. Os serviços de instalação, integração, garantia e suporte dos equipamentos e softwares, deverão ser realizados diretamente pelo fabricante de acordo com as exigências contidas no descritivo dos mesmos, estando essas aderentes aos respectivos níveis de serviço necessários a cada um deles.

1.8. O fornecedor deverá informar em proposta marca e modelo dos equipamentos utilizados na solução e apresentar prospecto com as características técnicas do equipamento comprovando-os através de certificados, manuais técnicos, folders e demais literaturas técnicas editadas pelos fabricantes. Serão aceitas cópias das especificações obtidas no site na Internet do fabricante juntamente com o endereço do site. A escolha do material a ser utilizado fica a critério do proponente;

1.9. Implantação:

1.9.1. Os serviços serão realizados em horário a combinar com a CONTRATANTE;

1.9.2. A empresa deverá entregar plano detalhado de implantação que deverá ser aprovado pelo cliente, contendo pelo menos:

1.9.2.1. Cronograma;

1.9.2.2. Topologia de rede atual, contendo levantamento que mostre todos os elementos da rede, tais como, VPNs, VLANs, firewall, servidores, switches, links wan, etc.

1.9.2.3. Levantamento de todas as configurações da rede
novos equipamentos e implantação da nova arquitet

1.9.2.4. Recomendações que forem necessárias para implantação;

1.10. Instalação e configuração de toda a infraestrutura existente conforme diagrama em anexo contemplando:

1.10.1. Instalação e Configuração básica de acesso a gerência via rede;

1.10.2. Instalação e configuração da Gerência e monitoramento em MÓDULO DE GERÊNCIA DE REDE;

1.10.3. Instalação e Configuração de autenticação de usuários em MÓDULO DE CONTROLE DE ACESSO;

1.10.4. Instalação e Configuração de todas as VLANs nos switches core e de acesso;

1.10.5. Instalação e Configuração de stacking em todas as pilhas conforme diagrama e orientação da equipe técnica do TRE-MA;

1.10.6. Instalação e Configuração de ACLs para filtrar acesso vindo de VLANS dos usuários para VLAN de servidores, bloqueando acesso a alguns serviços dos servidores, definidos pela equipe técnica do TRE-MA;

1.10.7. Configuração de agregação de links dos switches conforme diagrama e orientação da equipe técnica do TRE-MA;

1.10.8. Instalação e Configuração de toda a solução de rede sem fio, incluindo instalação e configuração de equipamentos e softwares, customização do captive portal de acordo com as necessidades do TRE-MA, criação e configuração das redes sem fio disponíveis no TRE-MA no momento da instalação, integração com AD para autenticação dos usuários, criação do portal para autenticação, gerenciamento e acesso de convidados e visitantes, implementação de "White e black list", configuração de atribuição de regras para usuários autenticados, configurar a opção de auto registro de convidados, configurar a garantia de largura de banda para redes sem fio;

1.10.9. Todos os switches devem estar com a última versão de firmware e o CONTRANTE deve ter acesso ao sítio para "baixar" outras versões, assim que disponibilizadas, por até 5 (cinco) anos;

1.10.10. A empresa deverá entregar documentação completa AS-BUILT (Como construído), em meio magnético no formato Word editável, contendo pelo menos:

1.10.10.1. Procedimentos de instalação com o passo-a-passo completo da instalação e configuração dos softwares e equipamentos, contendo imagens e comandos necessários para realizar as configurações, códigos de licenças, etc;

1.10.10.2. Arquivos contendo a configuração de todos os dispositivos e softwares instalados pós instalação;

1.10.10.3. Topologia completa da nova arquitetura de rede;

1.10.10.4. Evidências (telas de ferramentas, resultados de comandos, etc.) que demonstrem que foram realizados testes da nova rede;

1.11. Transferência de Tecnologia

1.11.1. O treinamento deverá ser realizado na modalidade workshop com tarefas práticas hands-on, visando assim a melhor fixação dos temas abordados com foco direto na explicação da tecnologia dos produtos ofertados como também nas rotinas de instalação, configuração, gerenciamento, administração e operação dos mesmos, devendo ter duração mínima de 24 (vinte e quatro) horas onde serão abordados no mínimo os seguintes tópicos:

1.11.1.1. Configuração inicial e acesso a gerência;

1.11.1.2. Configuração de VLANS e Roteamentos;

1.11.1.3. Configuração de empilhamento de switches;

1.11.1.4. Configuração de agregação de links;

1.11.1.5. Configuração de switches através das ferramentas de gerência fornecidas;

1.11.1.6. Configuração de ACLs.

2. Switch Tipo 1 – Mínimo 8 portas par trançado

2.1. CARACTERÍSTICAS TÉCNICAS MÍNIMAS

2.1.1. Deve possuir no mínimo 8 (oito) portas RJ-45 10/100/1000 portas com detecção automática;

2.1.2. 2 portas com funcionalidade dupla - cada porta pode ser usada como uma porta 10/100/1000 RJ-45 (10Base-T tipo IEEE 802.3);

2.1.3. 100Base-Tx tipo IEEE 802.3u 1000Base-T Gigabit Ethernet IEEE 802.3ab) ou como um slot SFP (para uso com transceptores SFP);

2.1.4. Deve possuir capacidade de encaminhamento de, no mínimo,14 Mbps;

2.1.5. Deve possuir capacidade de comutação de, no mínimo, 20 Gbps;

2.1.6. Deverá vir acompanhado de cabo console;

2.1.7. Deverá vir acompanhado de cabo de força;

2.2. Empilhamento

2.2.1. Capacidade de empilhar virtualmente no mínimo 4 switches;

2.2.2. Todos os cabos, acessórios, módulos, licenças devem ser fornecidos em conjunto com o equipamento.

2.3. Gerenciamento

2.3.1. Permitir Gerenciamento através de ferramenta de gerenciamento;

2.3.2. Possuir Interface de linha de comando;

2.3.3. Navegador da Web;

2.3.4. Menu de configuração;

2.3.5. Gerenciamento fora de banda (RS – 232C serial ou micro USB)

3. Switch Tipo 2 – Mínimo 24 portas par trançado incluindo 2 portas 10Gb

3.1. CARACTERÍSTICAS TÉCNICAS MÍNIMAS

3.1.1. Deve possuir 24 (vinte e quatro) portas 10/100/1000;
3.1.2. Deve possuir, no mínimo, 2 (duas) portas 1/10G SFP+, sendo que estas duas portas serão utilizadas para uplink com o switch Core.;
3.1.3. Deve possuir capacidade de encaminhamento de, no mínimo, 95 Mbps;
3.1.4. Deve ser instalado em rack padrão EIA (19") e possuir kits completos para instalação.
3.1.5. Deve possuir altura máxima de 1 RU.
3.1.6. Deverá vir acompanhado de cabo console;
3.1.7. Deve possuir capacidade de comutação de, no mínimo, 128 Gbps;
3.1.8. Deve implementar IEEE 802.3az para as portas 10/100/1000;
3.1.9. Deve possuir uma interface de console USB;
3.1.10. Deve suportar empilhamento de no mínimo 4 (quatro) switches;
3.1.11. Deve suportar agregação de link através de LACP com no mínimo 20 (vinte) grupos distribuídos através da pilha, com cada grupo permitindo até 8 (oito) portas;
3.1.12. Deve suportar a agregação de links entre diferentes membros da pilha;
3.1.13. Deve possuir no mínimo 32.000 endereços MAC;
3.1.14. Deve possuir latência máxima de 8µs, considerando pacotes de 64 bytes;
3.1.15. Deve implementar funcionalidade que permita a detecção de links unidirecionais;
3.1.16. Deve implementar funcionalidade que permita a detecção de falhas de uplink;
3.1.17. Deve implementar no mínimo 2000 VLANs simultaneamente;
3.1.18. Deve implementar MVRP (Multiple VLAN Registration Protocol);
3.1.19. Deve implementar LLDP (IEEE 802.1ab);
3.1.20. Deve implementar LLDP-MED;
3.1.21. Deve implementar Q-in-Q (IEEE 802.1ad);
3.1.22. Deve implementar PVST+, RPVST+ ou protocolo compatível;
3.1.23. Deve implementar MSTP (IEEE 802.1s);
3.1.24. Deve implementar túneis VxLAN (VTEP) ou IEEE 802.1aq Shortest Path bridging (SPB-M);

3.2. FUNCIONALIDADES DE CAMADA 3

3.2.1. Deve possuir tabela de roteamento com no mínimo 2.000 rotas IPv4 e 1.000 rotas IPv6;
3.2.2. Deve implementar roteamento estático;
3.2.3. Deve implementar RIP v2, com suporte a autenticação MD5 (RIPv2);
3.2.4. Deve implementar RIPng;
3.2.5. Deve implementar OSPF;
3.2.6. Deve implementar OSPFv3;
3.2.7. Deve implementar Policy-based Routing;
3.2.8. Deve implementar VRRP;
3.2.9. Deve implementar VRRPv3;
3.2.10. Deve implementar servidor DHCP;
3.2.11. Deve implementar DHCP snooping (IPv4 e IPv6);
3.2.12. Deve implementar DHCP relay (IPv4 e IPv6);

3.3. MULTICAST

3.3.1. Deve implementar PIM-SM;
3.3.2. Deve implementar PIM-DM;
3.3.3. Deve implementar MLD snooping;
3.3.4. Deve implementar IGMP v3;

3.4. SOFTWARE DEFINED NETWORKING

3.4.1. Deve implementar OpenFlow 1.3 ou superior;
3.4.2. Deve implementar a separação lógica do tráfego sem suporte a OpenFlow do tráfego com suporte a OpenFlow através de instâncias. O tráfego OpenFlow não pode influenciar o tráfego não openflow no equipamento.
3.4.3. Deve implementar no mínimo 3 instâncias de OpenFlow;
3.4.4. As instâncias de OpenFlow devem suportar a associação de múltiplas VLANs.
3.4.5. Cada instância OpenFlow configurada no equipamento deve suportar, pelo menos, a configuração de 3 controladores SDN.
3.4.6. Deve permitir utilizar intervalo de portas TCP/UDP e flags de TCP como parâmetros nas regras de OpenFlow;
3.4.7. Deve suportar no mínimo 8.000 regras openflow;
3.4.8. Deve possuir interface REST API;
3.4.9. Deve suportar configurações via JSON/REST API com, no mínimo, os seguintes métodos: GET, POST, PUT e DELETE;
3.4.10. Deve suportar a criação de VLANs e ACLs no equipamento através de REST.

3.5. EMPILHAMENTO

3.5.1. Deve suportar empilhamento de no mínimo 6 (seis) switches;

3.5.2. Deve ser fornecido com todos os cabos para empilhamento, módulos para empilhamento e licenças necessários.
3.5.3. Deve possuir capacidade de empilhamento com o switch tipo 3 deste lote.
3.5.4. Deve suportar empilhamento redundante, através da ligação do último switch da pilha ao primeiro switch da pilha.
3.5.5. Deve acompanhar todos os acessórios necessários para realizar o empilhamento, tais como módulos de empilhamento, cabos de empilhamento dedicado com, no mínimo, 1 metro de comprimento, licenças, etc.

3.6. MULTICAST
3.6.1. Deve implementar PIM-SM;
3.6.2. Deve implementar PIM-DM;
3.6.3. Deve implementar MLD snooping;
3.6.4. Deve implementar IGMP v3;

3.7. QoS
3.7.1. Deve implementar controle de broadcast;
3.7.2. Deve implementar rate limiting para pacotes ICMP;
3.7.3. Deve implementar rate limiting para tráfego broadcast e multicast;
3.7.4. Deve implementar rate limiting baseado em tráfego classificado por uma ACL;
3.7.5. Deve suportar espelhamento de portas;
3.7.6. Deve suportar espelhamento de tráfego para um switch remoto.

3.8. SEGURANÇA
3.8.1. Deve implementar controle de acesso baseado em perfis (Role Based Access Control);
3.8.2. Deve implementar VLANs privadas, de forma que permita o isolamento de tráfego de uma porta de acesso das demais portas de acesso de uma mesma VLAN, permitindo acesso apenas para as portas de Uplink (porta promíscua);
3.8.3. Deve implementar 802.1x;
3.8.4. Deve implementar autenticação baseada em web;
3.8.5. Deve implementar autenticação baseada em endereço MAC;
3.8.6. Deve permitir a utilização simultânea de autenticação 802.1x e MAC em uma mesma porta;
3.8.7. Deve implementar TACACS+ ou HWTACACS. Não serão aceitas soluções similares;
3.8.8. Deverá suportar o download de políticas ou ACLs a partir de um software de Controle de Acesso à Rede (NAC), sem necessidade de pré-configuração das regras no switch, permitindo a centralização das políticas;
3.8.9. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita identificar automaticamente o tipo e sistema operacional dos equipamentos que se conectam à rede (device profiling) sem a necessidade de agentes instalados nos dispositivos;
3.8.10. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita verificar se a máquina está em conformidade com a política de segurança antes de entrar na rede, verificando, no mínimo serviços os serviços e antivírus das máquinas. Deve suportar os sistemas operacionais Microsoft Windows, Mac OS e Linux.

3.9. GERENCIAMENTO
3.9.1. Deve implementar NTP com autenticação MD5;
3.9.2. Deve implementar Time Domain Reflectometry (TDR) para testes de cabos UTP, permitindo identificar falhas e verificar a distância do cabo;
3.9.3. Deve suportar duas imagens de software na flash;
3.9.4. Deve suportar múltiplos arquivos de configuração na flash;
3.9.5. Deve permitir o agendamento de tarefas, permitindo executar um comando em um dia e horário específicos;
3.9.6. Deve suportar a autoconfiguração dos switches através de DHCP e software de gerenciamento, sem necessidade de nenhuma intervenção no switch (com configuração de fábrica);
3.9.7. Deve suportar gerenciamento através de plataforma de nuvem do mesmo fabricante, com funcionalidades de gerenciamento de configuração, alertas e notificações e gerenciamento de firmware, sem necessidade de instalação de nenhum software ou dispositivo on-site;
3.9.8. Deve suportar IPSec para comunicação com o sistema de gerenciamento;
3.9.9. Deve implementar sFlow (IPv4 e IPv6);
3.9.10. Deve possuir interface web para configuração;
3.9.11. Deve suportar diagnóstico de transceivers ópticos;
3.9.12. Deve implementar Syslog sobre TLS;
3.9.13. Deve implementar Secure SFTP (SFTP);
3.9.14. Deve implementar SNMP v1/v2/v3;
3.9.15. Deve implementar funcionalidade que permita monitorar o SLA (Service Level Agreement) de conexões IP. Deve suportar os seguintes testes: ICMP Echo, UDP-Echo (em porta configurável) e TCP-Connect (em porta configurável) e Jitter UDP para voz;
3.9.16. Deve implementar compatibilidade com o protocolo CDP para provisionamento de telefones IP ou o protocolo LLDP-MED;
3.9.17. Deve implementar o isolamento de um Access Point rogue conectado ao switch, quando este for detectado por solução de WLAN do mesmo fabricante;
3.9.18. Deve implementar a configuração automática de Access Po
ao switch. Devem ser suportados os seguintes parâmetros

de banda máxima;

3.9.19. Deve suportar o encaminhamento de tráfego para controladora wireless do mesmo fabricante para inspeção e controle de acesso.

3.10. LICENCIAMENTO

3.10.1. Deve ser fornecido com a versão de software mais completa disponível para o equipamento;

3.10.2. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento;

3.11. GARANTIA E SUPORTE

3.11.1. O equipamento ofertado deverá possuir garantia do fabricante na modalidade on-site pelo período mínimo de 60 (sessenta) meses para reposição de peças, mão de obra e atendimento. O prazo máximo para atendimento do chamado deve ser de até o próximo dia útil após a sua abertura. Durante o período da garantia o prazo máximo para o reparo de equipamentos defeituosos a condição normal de funcionamento deverá ser de até 07 (sete) dias úteis.

3.11.2. Caso a garantia padrão do fabricante seja inferior a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante ("part number"), incorporada à solução.

3.11.3. O fabricante deve possuir canais de comunicação e ferramentas adicionais para suporte técnico online como "chat" e "e-mail" em seu site da internet com disponibilidade ainda de área para cadastro da solução de hardware ofertada, possibilitando assim que a CONTRATANTE possa receber de forma proativa, durante todo período da garantia as notificações de atualizações e correções ("hotfix") da solução;

3.11.4. A empresa fabricante do equipamento deverá dispor de um número telefônico tipo 0800 para suporte técnico e abertura de chamados técnicos.

3.11.5. Para efeito de comprovação da garantia, suporte, dos níveis de atendimento e solução exigidos para os equipamentos, deverá ser comprovada a existência da assistência técnica local no domicílio da contratante e na modalidade on-site, devendo essa ser realizada por meio de documentação oficial do fabricante dos produtos e de domínio público, através de catálogos, folder impressos ou da internet, devendo constar o endereço URL na mesma. Caso não seja comprovada por um dos meios citados anteriormente, será possível a comprovação através da apresentação de documentação expressa do fabricante dos equipamentos, indicando a referida assistência técnica que será responsável pelo atendimento e manutenção durante o período de garantia dos produtos ofertados.

4. Switch Tipo 3 – Mínimo 48 portas par trançado incluindo 2 portas 10Gb

4.1. CARACTERÍSTICAS TÉCNICAS MÍNIMAS:

4.1.1. Deve possuir no mínimo 48 (quarenta e oito) portas 10/100/1000 RJ45 BaseT full-duplex sem conversores externos, auto-sense, com MDI-MDIX automático;

4.1.2. Deve possuir, no mínimo, 2 (duas) portas 1/10G SFP+, sendo que estas duas portas serão utilizadas para uplink com o switch Core;

4.1.3. Deve ser instalado em rack padrão EIA (19") e possuir kits completos para instalação.

4.1.4. Deve possuir altura máxima de 1 RU.

4.1.5. Deverá vir acompanhado de cabo console;

4.1.6. Deve permitir o uso simultâneo de todas as portas do equipamento, ou seja, 48 portas Gigabit RJ45, 2 portas SFP/SFP+ de uplink e 2 portas de empilhamento.

4.1.7. Deve suportar a agregação de links entre diferentes membros da pilha;

4.1.8. Deve possuir LED de atividade para as portas RJ45 e SFP+.

4.1.9. Deve possuir porta console RS-232 com conectores DB9 ou RJ-45.

4.1.10. Deve possuir fonte de alimentação primária interna que opere com tensões de entrada entre 110 e 220 VAC e suporte frequência entre 50/60hz.

4.1.11. Deve ser fornecido com pelo menos duas (2) fontes de alimentação redundante interna.

4.1.12. Deve implementar IEEE 802.3az para as portas 10/100/1000;

4.1.13. Deve possuir uma interface de console USB;

4.1.14. Deve suportar agregação de link através de LACP com no mínimo 20 (vinte) grupos distribuídos através da pilha, com cada grupo permitindo até 8 (oito) portas;

4.1.15. Deve suportar a agregação de links entre diferentes membros da pilha;

4.1.16. Deve possuir no mínimo 32.000 endereços MAC;

4.1.17. Deve implementar funcionalidade que permita a detecção de links unidirecionais;

4.1.18. Deve implementar funcionalidade que permita a detecção de falhas de uplink;

4.1.19. Deve implementar no mínimo 2000 VLANs simultaneamente;

4.1.20. Deve implementar MVRP (Multiple VLAN Registration Protocol);

4.1.21. Deve implementar LLDP (IEEE 802.1ab);

4.1.22. Deve implementar LLDP-MED;

4.1.23. Deve implementar Q-in-Q (IEEE 802.1ad);

4.1.24. Deve implementar PVST+, RPVST+ ou protocolo compatível;

4.1.25. Deve implementar MSTP (IEEE 802.1s);

4.1.26. Deve implementar túneis VxLAN (VTEP) ou IEEE 802.1aq Shortest Path bridging (SPB-M).

4.1.27. O switch deve ser homologado na Anatel.

4.2. FUNCIONALIDADES DE CAMADA 3

4.2.1. Deve possuir tabela de roteamento com no mínimo 2.000 rotas IPv4 e 1.000 rotas IPv6;
4.2.2. Deve implementar roteamento estático;
4.2.3. Deve implementar RIP v2, com suporte a autenticação MD5 (RIPv2);
4.2.4. Deve implementar RIPng;
4.2.5. Deve implementar OSPF;
4.2.6. Deve implementar OSPFv3;
4.2.7. Deve implementar Policy-based Routing;
4.2.8. Deve implementar VRRP;
4.2.9. Deve implementar VRRPv3;
4.2.10. Deve implementar servidor DHCP;
4.2.11. Deve implementar DHCP snooping (IPv4 e IPv6);
4.2.12. Deve implementar DHCP relay (IPv4 e IPv6);
4.2.13. Deve implementar PIM-SM;
4.2.14. Deve implementar PIM-DM;
4.2.15. Deve implementar MLD snooping;
4.2.16. Deve implementar IGMP v3.

4.3. SOFTWARE DEFINED NETWORKING

4.3.1. Deve implementar OpenFlow 1.3 ou superior;
4.3.2. Deve implementar a separação lógica do tráfego sem suporte a OpenFlow do tráfego com suporte a OpenFlow através de instâncias. O tráfego OpenFlow não pode influenciar o tráfego não openflow no equipamento;
4.3.3. Deve permitir configurar cada instância como modo ativo (pacotes referentes a fluxos que o switch não conhece são enviados para a controladora) ou modo passivo (pacotes que não se referem a um fluxo na tabela do switch não são enviados para a controladora);
4.3.4. Deve implementar no mínimo 3 instâncias de OpenFlow;
4.3.5. As instâncias de OpenFlow devem suportar a associação de múltiplas VLANs;
4.3.6. Cada instância OpenFlow configurada no equipamento deve suportar, pelo menos, a configuração de 3 controladores SDN;
4.3.7. Deve permitir utilizar intervalo de portas TCP/UDP e flags de TCP como parâmetros nas regras de OpenFlow;
4.3.8. Deve suportar no mínimo 8.000 regras openflow;
4.3.9. Deve possuir interface REST API;
4.3.10. Deve suportar configurações via JSON/REST API com, no mínimo, os seguintes métodos: GET, POST, PUT e DELETE;
4.3.11. Deve suportar a criação de VLANs e ACLs no equipamento através de REST.

4.4. QoS

4.4.1. Deve implementar controle de broadcast;
4.4.2. Deve implementar rate limiting para pacotes ICMP;
4.4.3. Deve implementar rate limiting para tráfego broadcast e multicast;
4.4.4. Deve implementar rate limiting baseado em tráfego classificado por uma ACL;
4.4.5. Deve suportar espelhamento de portas;
4.4.6. Deve suportar espelhamento de tráfego para um switch remoto.

4.5. EMPILHAMENTO

4.5.1. Deve permitir empilhar, de forma que, no mínimo, 6 (seis) switches operem como um único switch virtual.
4.5.2. Deve permitir o gerenciamento do switch e da pilha de switches através de endereço IP único.
4.5.3. Deve suportar empilhamento redundante, através da ligação do último switch da pilha ao primeiro switch da pilha.
4.5.4. Possuir backplane entre os switches da pilha de, no mínimo, 10Gbps para cada direção, com capacidade agregada de 40Gbps de empilhamento por unidade.
4.5.5. Deve acompanhar todos os acessórios necessários para realizar o empilhamento, tais como módulos de empilhamento, cabos de empilhamento dedicado com, no mínimo, 1 metro de comprimento, licenças, etc;
4.5.6. Deve permitir o empilhamento com o switch tipo 2 deste lote.

4.6. SEGURANÇA

4.6.1. Deve implementar controle de acesso baseado em perfis (Role Based Access Control);
4.6.2. Deve implementar VLANs privadas, de forma que permita o isolamento de tráfego de uma porta de acesso das demais portas de acesso de uma mesma VLAN, permitindo acesso apenas para as portas de Uplink (porta promíscua);
4.6.3. Deve implementar 802.1x;
4.6.4. Deve implementar autenticação baseada em web;
4.6.5. Deve implementar autenticação baseada em endereço MAC;
4.6.6. Deve permitir a utilização simultânea de autenticação 802.1x e MAC em uma mesma porta;
4.6.7. Deve implementar TACACS+ ou HWTACACS. Não serão aceitas soluções similares;
4.6.8. Deverá suportar o download de políticas ou ACLsl a partir de um software de Controle de Acesso à Rede (NAC), sem necessidade de pré-configuração das regras no switch, permitindo a centralização das políticas;
4.6.9. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita identificar automaticamente o tipo e sistema operacional dos equipame
necessidade de agentes instalados nos dispositivos;

4.6.10. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita verificar se a máquina está em conformidade com a política de segurança antes de entrar na rede, verificando, no mínimo serviços os serviços e antivírus das máquinas. Deve suportar os sistemas operacionais Microsoft Windows, Mac OS e Linux.

4.7. GERENCIAMENTO

4.7.1. Deve implementar NTP com autenticação MD5;
4.7.2. Deve implementar Time Domain Reflectometry (TDR) para testes de cabos UTP, permitindo identificar falhas e verificar a distância do cabo;
4.7.3. Deve suportar duas imagens de software na flash;
4.7.4. Deve suportar múltiplos arquivos de configuração na flash;
4.7.5. Deve permitir o agendamento de tarefas, permitindo executar um comando em um dia e horário específicos;
4.7.6. Deve suportar a autoconfiguração dos switches através de DHCP e software de gerenciamento, sem necessidade de nenhuma intervenção no switch (com configuração de fábrica);
4.7.7. Deve suportar gerenciamento através de plataforma de nuvem do mesmo fabricante, com funcionalidades de gerenciamento de configuração, alertas e notificações e gerenciamento de firmware, sem necessidade de instalação de nenhum software ou dispositivo on-site;
4.7.8. Deve suportar IPSec para comunicação com o sistema de gerenciamento;
4.7.9. Deve implementar sFlow (IPv4 e IPv6);
4.7.10. Deve possuir interface web para configuração;
4.7.11. Deve suportar diagnóstico de transceivers ópticos;
4.7.12. Deve implementar Syslog sobre TLS;
4.7.13. Deve implementar Secure SFTP (SFTP);
4.7.14. Deve implementar SNMP v1/v2/v3;
4.7.15. Deve implementar funcionalidade que permita monitorar o SLA (Service Level Agreement) de conexões IP. Deve suportar os seguintes testes: ICMP Echo, UDP-Echo (em porta configurável) e TCP-Connect (em porta configurável) e Jitter UDP para voz;
4.7.16. Deve implementar compatibilidade com o protocolo CDP para provisionamento de telefones IP ou o protocolo LLDP-MED;
4.7.17. Deve implementar o isolamento de um Access Point rogue conectado ao switch, quando este for detectado por solução de WLAN do mesmo fabricante;
4.7.18. Deve implementar a configuração automática de Access Point wireless do mesmo fabricante quando conectado ao switch. Devem ser suportados os seguintes parâmetros para a configuração automática: VLAN, CoS, largura de banda máxima;
4.7.19. Deve suportar o encaminhamento de tráfego para controladora wireless do mesmo fabricante para inspeção e controle de acesso.

4.8. LICENCIAMENTO

4.8.1. Deve ser fornecido com a versão de software mais completa disponível para o equipamento;
4.8.2. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento.

4.9. GARANTIA E SUPORTE

4.9.1. O equipamento ofertado deverá possuir garantia do fabricante na modalidade on-site pelo período mínimo de 60 (sessenta) meses para reposição de peças, mão de obra e atendimento. O prazo máximo para atendimento do chamado deve ser de até o próximo dia útil após a sua abertura. Durante o período da garantia o prazo máximo para o reparo de equipamentos defeituosos a condição normal de funcionamento deverá ser de até 07 (sete) dias úteis.
4.9.2. Caso a garantia padrão do fabricante seja inferior a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante (“part number”), incorporada à solução.
4.9.3. O fabricante deve possuir canais de comunicação e ferramentas adicionais para suporte técnico online como “chat” e “e-mail” em seu site da internet com disponibilidade ainda de área para cadastro da solução de hardware ofertada, possibilitando assim que a CONTRATANTE possa receber de forma proativa, durante todo período da garantia as notificações de atualizações e correções (“hotfix”) da solução;
4.9.4. A empresa fabricante do equipamento deverá dispor de um número telefônico tipo 0800 para suporte técnico e abertura de chamados técnicos.
4.9.5. Para efeito de comprovação da garantia, suporte, dos níveis de atendimento e solução exigidos para os equipamentos, deverá ser comprovada a existência da assistência técnica local no domicílio da contratante e na modalidade on-site, devendo essa ser realizada por meio de documentação oficial do fabricante dos produtos e de domínio público, através de catálogos, folder impressos ou da internet, devendo constar o endereço URL na mesma. Caso não seja comprovada por um dos meios citados anteriormente, será possível a comprovação através da apresentação de documentação expressa do fabricante dos equipamentos, indicando a referida assistência técnica que será responsável pelo atendimento e manutenção durante o período de garantia dos produtos ofertados.

5. Switch Tipo 4 – Mínimo 32 portas, incluindo 8 portas 10Gb, 2 portas 40 Gb, layer 3 (SWITCH CORE)

5.1. CARACTERÍSTICAS TÉCNICAS MÍNIMAS

5.1.1. Deve possuir no mínimo 32 (Trinta e duas) portas RJ45 1/10 G

5.1.2. Deve possuir no mínimo 8 (Oito) portas SFP+ 1/10 Gigabit;
5.1.3. Deve possuir no mínimo 2 (duas) portas QSFP+ 40 Gigabit;
5.1.4. Serão permitidos equipamentos modulares, desde que atendam todas as exigências deste edital;
5.1.5. Deve possuir no máximo 1U de altura;
5.1.6. Deve possuir porta de console para gerenciamento e configuração via linha de comando. O conector deve ser RJ-45 ou padrão RS-232 ou USB. (Os cabos e eventuais adaptadores necessários para acesso à porta de console devem ser fornecidos);
5.1.7. Deve possuir no mínimo 1 porta FastEthernet 10/100 ou Gigabit Ethernet 10/100/1000 com conector RJ-45 para administração fora de banda (out-of-band management).
5.1.8. Deve possuir no mínimo 512 MB de memória flash;
5.1.9. Deve possuir memória DRAM de no mínimo 2 Gbytes;
5.1.10. Deve possuir buffer de pacotes de no mínimo 9 Mbytes;
5.1.11. Deve possuir capacidade de encaminhamento de no mínimo 710 Mpps;
5.1.12. Deve possuir capacidade de comutação de no mínimo 960 Gbps;
5.1.13. Deve ser fornecido com pelo menos duas (2) fontes de alimentação redundante interna;
5.1.14. As fontes de alimentação e os ventiladores devem suportar hot-plug;
5.1.15. Deve suportar fluxo de ar reversível, da frente para a traseira (front-to-back) ou da traseira para a frente (back-to-front);
5.1.16. Deve fornecido incialmente com a configuração front-to-back;
5.1.17. Deve possuir Certificado de Homologação na Anatel, de acordo com a Resolução nº 242;
5.1.18. Deve possuir fonte de alimentação interna 110/220VAC;
5.1.19. Deve ser instalável em rack padrão de 19", sendo que deverão ser fornecidos os respectivos Kit's de fixação;
5.1.20. O equipamento deve ser específico para o ambiente de Datacenter com comutação de pacotes de alto desempenho e arquitetura "non blocking".

5.2. DISPONIBILIDADE

5.2.1. Empilhamento:
5.2.1.1. Deve suportar empilhamento sem ocupar portas dianteiras do switch, de forma que, no mínimo, 4 (quatro) switches operem como um único switch virtual.
5.2.1.2. O equipamento deverá ser fornecido com todos os módulos de empilhamento e cabos, e com qualquer tipo de licença necessária para realizar o empilhamento para atender ao projeto de rede do TRE-MA;
5.2.1.3. Deve suportar empilhamento através de portas 10 Gigabit Ethernet ou 40 Gigabit Ethernet padrão, permitindo o empilhamento de equipamentos que estejam em locais distintos, conectados através de fibra óptica;
5.2.1.4. Deve suportar empilhamento redundante, através da ligação do último switch da pilha ao primeiro switch da pilha.
5.2.1.5. Deve permitir empilhamento com o switch tipo 5;
5.2.2. Deve suportar a criação de grupos de agregação de link contendo portas em unidades diferentes da pilha;
5.2.3. Deve implementar agregação de links dinâmico (LACP), com suporte à criação de até 128 grupos. Deve ser possível a formação de grupos com até 16 portas;
5.2.4. Deve suportar atualização de software em serviço (In Service Software Upgrade - ISSU);

5.3. SWITCHING

5.3.1. Deve suportar o modo de comutação cut-through ou ser wire-speed;
5.3.2. Deve possuir tabela para no mínimo 128.000 endereços MAC;
5.3.3. Deve suportar o mínimo 4094 VLANs;
5.3.4. Deve implementar Jumbo frames com tamanho de até 10000 bytes;
5.3.5. Deve implementar MSTP;
5.3.6. Deve implementar IEEE 802.3ad Link Aggregation;
5.3.7. Deve implementar Rapid STP (RSTP, IEEE 802.1w);
5.3.8. Deve implementar Ethernet Virtual Bridging (EVB);
5.3.9. Deve implementar Virtual Ethernet Port Aggregator (VEPA);
5.3.10. Deve Implementar Transparent Interconnection of Lots of Links (TRILL) ou IEEE 802.1aq Shortest Path Bridging (SPB-M);
5.3.11. Deve implementar os protocolos de Data Center Bridging:
5.3.12. Priority Flow control (PFC);
5.3.13. Data Center Bridging Exchange (DCBX);
5.3.14. Deve implementar FCoE;
5.3.15. Deve suportar o modo FCF;

5.4. ROTEAMENTO

5.4.1. Deve implementar roteamento estático IPv4 e IPv6;
5.4.2. Deve implementar RIP, RIPv2 e RIPng;
5.4.3. Deve possuir no mínimo 512 interfaces de roteamento IP (VLAN Interface)
5.4.4. O equipamento ofertado deve implementar roteamento base
5.4.5. O equipamento ofertado deve possuir tabela de roteamer

entradas IPv6;

5.4.6. Deve suportar no mínimo 256 rotas estáticas;

5.4.7. O equipamento ofertado deve permitir autenticação em servidores RADIUS, TACACS+ ou HWTACACS;

5.4.8. Deve suportar dual stack IPv4/IPv6;

5.4.9. Deve implementar Bidirectional Forwarding Detection (BFD), suportando redução do tempo de convergência para OSPF e VRRP;

5.4.10. Deve implementar OSPF v2 e OSPF v3;

5.4.11. Deve implementar BGP.

5.5. QoS

5.5.1. Deve implementar 8 filas de porta;

5.5.2. Deve implementar WFQ (Weighted Fair Queueing), SP (Strict Priority);

5.5.3. Deve implementar Weighted Random Early Discard (WRED)

5.5.4. Deve implementar rate-limiting com granularidade de 64 kbps;

5.6. SEGURANÇA

5.6.1. Deve implementar listas de controle de Acesso (ACL) baseado em endereço IPv4, IPv6 e MAC de origem e destino, porta protocolo e VLAN;

5.6.2. Deve implementar accounting RADIUS;

5.6.3. Deve implementar TACACS+ ou HWTACACS;

5.6.4. Deve implementar proteção contra-ataques de ARP;

5.6.5. Deve implementar proteção contra IP spoofing (IP source guard);

5.6.6. Deve implementar SNMP v1, v2 e v3;

5.6.7. Deve implementar funcionalidade que permita que a configuração de root do Spanning Tree seja mantida mesmo no caso de recebimento de BPDU com maior prioridade (root guard);

5.6.8. Deve implementar SSL;

5.6.9. Deve implementar SSHv2;

5.6.10. Deve implementar a configuração de limites para tráfego broadcast e multicast por porta. Caso os limites configurados sejam excedidos, deve ser possível desabilitar a porta;

5.7. GERENCIAMENTO

5.7.1. Deve permitir o espelhamento de tráfego selecionado por uma ACL para uma porta ou VLAN;

5.7.2. Deve suportar espelhamento remoto;

5.7.3. Deve implementar Secure File Transfer Protocol;

5.7.4. Deve implementar LLDP;

5.7.5. Deve implementar LLDP-MEd;

5.7.6. Deve implementar protocolo de autenticação com as seguintes características: Utiliza o protocolo TCP, garantindo confiabilidade intrínseca; criptografe todo o payload do pacote e não apenas o campo de senha; Implemente autorização para cada comando de configuração;

5.7.7. Deve implementar NTP v3;

5.7.8. Deve suportar Precision Time Protocol (PTP), conforme RFC 1588

5.7.9. Deve suportar a utilização de comandos em linguagem TCL ou UNIX;

5.7.10. Deve suportar a utilização de scripts Python;

5.7.11. Deve permitir a obtenção automática do arquivo de configuração através de servidor sem necessidade de intervenção direta no switch;

5.7.12. Deve implementar as seguintes MIBs:

5.7.13. Deve implementar RFC 1213 MIB II;

5.7.14. Deve implementar RFC 1907 SNMPv2 MIB;

5.7.15. Deve implementar RFC 2571 SNMP Framework MIB;

5.7.16. Deve implementar RFC 2572 SNMP-MPD MIB;

5.7.17. Deve implementar RFC 2573 SNMP-Notification MIB;

5.7.18. Deve implementar RFC 2574 SNMP USM MIB;

5.7.19. Deve implementar RFC 2737 Entity MIB (Version 2);

5.7.20. Deve implementar RFC 3414 SNMP-User based-SM MIB;

5.7.21. Deve implementar RFC 3415 SNMP-View based-ACM MIB;

5.7.22. Deve implementar LLDP-MIB;

5.7.23. Deve implementar sFlow;O equipamento ofertado deve possuir certificado de homologação na Anatel, de acordo com a resolução n° 242;

5.8. GARANTIA E SUPORTE

5.8.1. O equipamento ofertado deverá possuir garantia do fabricante na modalidade on-site pelo período mínimo de 60 (sessenta) meses para reposição de peças, mão de obra e atendimento. O prazo máximo para atendimento do chamado deve ser de até o próximo dia útil após a sua abertura. Durante o período da garantia o prazo máximo para o reparo de equipamentos defeituosos a condição normal de funcionamento deverá ser de até 07 (sete) dias úteis.

5.8.2. Caso a garantia padrão do fabricante seja inferior a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante ("part number"), i

5.8.3. O fabricante deve possuir canais de comunicação e ferram

"chat" e "e-mail" em seu site da internet com disponibilidade ainda de área para cadastro da solução de hardware ofertada, possibilitando assim que a CONTRATANTE possa receber de forma proativa, durante todo período da garantia as notificações de atualizações e correções ("hotfix") da solução;

5.8.4. A empresa fabricante do equipamento deverá dispor de um número telefônico tipo 0800 para suporte técnico e abertura de chamados técnicos.

5.8.5. Para efeito de comprovação da garantia, suporte, dos níveis de atendimento e solução exigidos para os equipamentos, deverá ser comprovada a existência da assistência técnica local no domicílio da contratante e na modalidade on-site, devendo essa ser realizada por meio de documentação oficial do fabricante dos produtos e de domínio público, através de catálogos, folder impressos ou da internet, devendo constar o endereço URL na mesma. Caso não seja comprovada por um dos meios citados anteriormente, será possível a comprovação através da apresentação de documentação expressa do fabricante dos equipamentos, indicando a referida assistência técnica que será responsável pelo atendimento e manutenção durante o período de garantia dos produtos ofertados.

6. Switch Tipo 5 – Mínimo 20 portas SFP+ 10Gb, 2 portas 40 Gb, layer 3 (SWITCH CORE)

6.1. CARACTERÍSTICAS TÉCNICAS MÍNIMAS

6.1.1. Deve possuir no mínimo 20 (Vinte) portas SFP+ 1/10 Gigabit;

6.1.2. Deve possuir no mínimo 2 (duas) portas QSFP+ 40 Gigabit;

6.1.3. Serão permitidos equipamentos modulares, desde que atendam todas as exigências deste edital;

6.1.4. Deve possuir no máximo 1U de altura;

6.1.5. Deve possuir porta de console para gerenciamento e configuração via linha de comando. O conector deve ser RJ-45 ou padrão RS-232 ou USB. (Os cabos e eventuais adaptadores necessários para acesso à porta de console devem ser fornecidos);

6.1.6. Deve possuir no mínimo 1 porta FastEthernet 10/100 ou Gigabit Ethernet 10/100/1000 com conector RJ-45 para administração fora de banda (out-of-band management).

6.1.7. Deve possuir no mínimo 512 MB de memória flash;

6.1.8. Deve possuir memória DRAM de no mínimo 2 Gbytes;

6.1.9. Deve possuir buffer de pacotes de no mínimo 9 Mbytes;

6.1.10. Deve possuir capacidade de encaminhamento de no mínimo 710 Mpps;

6.1.11. Deve possuir capacidade de comutação de no mínimo 960 Gbps;

6.1.12. Deve ser fornecido com pelo menos duas (2) fontes de alimentação redundante interna;

6.1.13. As fontes de alimentação e os ventiladores devem suportar hot-plug;

6.1.14. Deve suportar fluxo de ar reversível, da frente para a traseira (front-to-back) ou da traseira para a frente (back-to-front);

6.1.15. Deve fornecido incialmente com a configuração front-to-back;

6.1.16. Deve possuir Certificado de Homologação na Anatel, de acordo com a Resolução nº 242;

6.1.17. Deve possuir fonte de alimentação interna 110/220VAC;

6.1.18. Deve ser instalável em rack padrão de 19", sendo que deverão ser fornecidos os respectivos Kit's de fixação;

6.1.19. O equipamento deve ser específico para o ambiente de Datacenter com comutação de pacotes de alto desempenho e arquitetura "non blocking".

6.1.20. Deve ser fornecido com pelo menos duas (2) fontes de alimentação redundante interna.

6.2. DISPONIBILIDADE

6.2.1. Empilhamento:

6.2.1.1. Deve suportar empilhamento sem ocupar portas dianteiras do switch, de forma que, no mínimo, 4 (quatro) switches operem como um único switch virtual.

6.2.1.2. O equipamento deverá ser fornecido com todos os módulos de empilhamento e cabos, e com qualquer tipo de licença necessária para realizar o empilhamento para atender ao projeto de rede do TRE-MA;

6.2.1.3. Deve suportar empilhamento através de portas 10 Gigabit Ethernet ou 40 Gigabit Ethernet padrão, permitindo o empilhamento de equipamentos que estejam em locais distintos, conectados através de fibra óptica;

6.2.1.4. Deve suportar empilhamento redundante, através da ligação do último switch da pilha ao primeiro switch da pilha.

6.2.1.5. Deve permitir empilhamento com o switch tipo 4;

6.2.2. Deve suportar a criação de grupos de agregação de link contendo portas em unidades diferentes da pilha;

6.2.3. Deve implementar agregação de links dinâmico (LACP), com suporte à criação de até 128 grupos. Deve ser possível a formação de grupos com até 16 portas;

6.2.4. Deve suportar atualização de software em serviço (In Service Software Upgrade - ISSU);

6.3. SWITCHING

6.3.1. Deve suportar o modo de comutação cut-through ou ser wire-speed;

6.3.2. Deve possuir tabela para no mínimo 128.000 endereços MAC;

6.3.3. Deve suportar o mínimo 4094 VLANs;

6.3.4. Deve implementar Jumbo frames com tamanho de até 10000 bytes;

6.3.5. Deve implementar MSTP;

6.3.6. Deve implementar IEEE 802.3ad Link Aggregation;

6.3.7. Deve implementar Rapid STP (RSTP, IEEE 802.1w);

6.3.8. Deve implementar Ethernet Virtual Bridging (EVB);
6.3.9. Deve implementar Virtual Ethernet Port Aggregator (VEPA);
6.3.10. Deve Implementar Transparent Interconnection of Lots of Links (TRILL) ou IEEE 802.1aq Shortest Path Bridging (SPB-M);
6.3.11. Deve implementar os protocolos de Data Center Bridging:
6.3.12. Priority Flow control (PFC);
6.3.13. Data Center Bridging Exchange (DCBX);
6.3.14. Deve implementar FCoE;
6.3.15. Deve suportar o modo FCF;

6.4. ROTEAMENTO
6.4.1. Deve implementar roteamento estático IPv4 e IPv6;
6.4.2. Deve implementar RIP e RIPv2;
6.4.3. Deve implementar RIPng;
6.4.4. Deve implementar BFD (Bidirectional Forwarding Detection);
6.4.5. Deve implementar Equal-Cost Multipath (ECMP);

6.5. QoS
6.5.1. Deve implementar 8 filas de porta;
6.5.2. Deve implementar WFQ (Weighted Fair Queueing), SP (Strict Priority);
6.5.3. Deve implementar Weighted Random Early Discard (WRED)
6.5.4. Deve implementar rate-limiting com granularidade de 64 kbps;

6.6. SEGURANÇA
6.6.1. Deve implementar autenticação 802.1x de múltiplos usuários por porta, simultaneamente.
6.6.2. Deve implementar segurança orientada por identidade e controle de acesso por usuário através de ACLs que permitam ou negue o acesso do usuário aos recursos de rede específicos, com base na identidade do usuário.
6.6.3. Atribuição VLAN automática, automaticamente atribui os usuários para a VLAN apropriada, com base em suas identidades.
6.6.4. Deve implementar accounting RADIUS;
6.6.5. Deve implementar TACACS+ ou HWTACACS;
6.6.6. Deve implementar proteção contra-ataques de ARP;
6.6.7. Deve implementar proteção contra IP spoofing (IP source guard);
6.6.8. Deve implementar SNMP v1, v2 e v3;
6.6.9. Deve implementar detecção de ataques maliciosos e enviar um aviso quando uma anomalia potencial, causada pelos ataques mal-intencionado, for detectado.
6.6.10. Deve suportar o isolamento de portas e VLANs, de forma que uma porta ou VLAN isolada não possa enviar tráfego para outra porta isolada do mesmo switch;
6.6.11. Deve implementar segurança do gerenciamento do switch em métodos de acesso CLI, GUI ou MIB, através de SSHv2, SSL e SNMPv3
6.6.12. Deve implementar autenticação baseado em porta ou endereço MAC;
6.6.13. Deve implementar autenticação utilizando navegadores web, possibilitando que clientes que não possuem cliente 802.1x possam autenticar;
6.6.14. Deve suportar port-security.

6.7. GERENCIAMENTO
6.7.1. Deve permitir instalação simplificada “Zero-touch provisioning” através de processo baseado em DHCP com a solução de software de gerenciamento;
6.7.2. O equipamento ofertado deve permitir múltiplos arquivos de configuração;
6.7.3. Deve suportar espelhamento remoto;
6.7.4. Deve implementar Secure File Transfer Protocol;
6.7.5. Deve implementar LLDP;
6.7.6. Deve implementar LLDP-MEd;
6.7.7. Deve implementar SNTP v4;
6.7.8. O equipamento ofertado deve Implementar Sflow ou Netflow;
6.7.9. Deve implementar RFC 1213 MIB II;
6.7.10. Deve implementar RFC 2096 IP Forwarding Table MIB;
6.7.11. Deve implementar RFC 2571 SNMP Framework MIB;
6.7.12. Deve implementar RFC 2572 SNMP-MPD MIB;
6.7.13. Deve implementar RFC 2573 SNMP-Notification MIB;
6.7.14. Deve implementar RFC 2574 SNMP USM MIB;
6.7.15. Deve implementar RFC 2737 Entity MIB (Version 2);
6.7.16. Deve implementar RFC 3414 SNMP-User based-SM MIB;
6.7.17. Deve implementar RFC 3415 SNMP-View based-ACM MIB;
6.7.18. Deve implementar RFC 2668 802.3 MAU MIB;
6.7.19. Deve implementar RFC 3418 MIB for SNMPv3;
6.7.20. Deve ser fornecido com a versão de software mais completa e
6.7.21. Deve ser fornecido com todas as licenças de software nece

funcionalidades disponíveis para o equipamento;

6.7.22. O equipamento ofertado deve possuir certificado de homologação na Anatel, de acordo com a resolução n° 242;

6.8. GARANTIA E SUPORTE

6.8.1. O equipamento ofertado deverá possuir garantia do fabricante na modalidade on-site pelo período mínimo de 60 (sessenta) meses para reposição de peças, mão de obra e atendimento. O prazo máximo para atendimento do chamado deve ser de até o próximo dia útil após a sua abertura. Durante o período da garantia o prazo máximo para o reparo de equipamentos defeituosos a condição normal de funcionamento deverá ser de até 07 (sete) dias úteis.

6.8.2. Caso a garantia padrão do fabricante seja inferior a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante ("part number"), incorporada à solução.

6.8.3. O fabricante deve possuir canais de comunicação e ferramentas adicionais para suporte técnico online como "chat" e "e-mail" em seu site da internet com disponibilidade ainda de área para cadastro da solução de hardware ofertada, possibilitando assim que a CONTRATANTE possa receber de forma proativa, durante todo período da garantia as notificações de atualizações e correções ("hotfix") da solução;

6.8.4. A empresa fabricante do equipamento deverá dispor de um número telefônico tipo 0800 para suporte técnico e abertura de chamados técnicos.

6.8.5. Para efeito de comprovação da garantia, suporte, dos níveis de atendimento e solução exigidos para os equipamentos, deverá ser comprovada a existência da assistência técnica local no domicílio da contratante e na modalidade on-site, devendo essa ser realizada por meio de documentação oficial do fabricante dos produtos e de domínio público, através de catálogos, folder impressos ou da internet, devendo constar o endereço URL na mesma. Caso não seja comprovada por um dos meios citados anteriormente, será possível a comprovação através da apresentação de documentação expressa do fabricante dos equipamentos, indicando a referida assistência técnica que será responsável pelo atendimento e manutenção durante o período de garantia dos produtos ofertados.

7. SOLUÇÃO DE GERENCIAMENTO DE ATIVOS DE REDE E ANÁLISE DE TRÁFEGO

7.1. LICENCIAMENTO

7.1.1. Licenciamento da SOLUÇÃO DE GERENCIAMENTO DE ATIVOS REDE, contemplando o quantitativo mínimo de 100 (cem) dispositivos, independentemente do tipo do dispositivo;

7.2. CARACTERÍSTICAS TÉCNICAS MÍNIMAS

7.2.1. Gerenciamento de Ativos

7.2.1.1. Caso a Solução gerenciamento de ativos de rede seja fornecida em appliance físico (hardware) ou virtual que demande sistema operacional, a contratada deverá fornecer o hardware, licenças de software (ex: licenças Microsoft, Linux, etc..), e garantias necessárias a todo conjunto com suporte e evolução desses itens durante todo período de garantia contratado.

7.2.1.2. Deve possuir portal web que permita o acesso integral à ferramenta através de um browser padrão;

7.2.1.3. Deve permitir a customização página principal do sistema, permitindo a inclusão alarmes, estatísticas de desempenho;

7.2.2. Análise de tráfego

7.2.2.1. Deve suportar o monitoramento de equipamentos de rede geradores de fluxos de dados baseados em protocolos NetStream v5/v9, NetFlow v5/v9, e sFlow v5.

7.2.2.2. Deve possuir interface gráfica de monitoramento de rede.

7.2.2.3. Deve fornecer informações em tempo real sobre o consumo de banda da rede utilizado por usuários e aplicativos.

7.2.2.4. Deve possibilitar o monitoramento de rede nas camadas 4 a 7.

7.2.2.5. Deve possibilitar a verificação do fluxo de dados da rede através da emissão de relatórios baseados na coleta de fluxos, análise e processamento dos dados da rede.

7.2.2.6. Deve possuir a capacidade de definir os dados recebidos pelo software de monitoramento, como estes dados devem ser interpretados e como serão apresentados para os administradores de rede.

7.3. CONTROLE ADMINISTRATIVO

7.3.1. Deve implementar controle de acesso baseado em privilégios, permitindo a criação de grupos de operadores com limitação de quais equipamentos e quais serviços da plataforma poderão ser usados;

7.3.2. Deve permitir a autenticação dos operadores através de base local e através de RADIUS e LDAP;

7.3.3. Deve permitir restringir a partir de quais endereços IP o operador poderá utilizar o sistema;

7.3.4. Deve executar o registro das ações executadas pelos operadores nos equipamentos gerenciados, para efeito de auditoria;

7.4. GERENCIAMENTO DE RECURSOS

7.4.1. Deve permitir a descoberta de elementos de rede através da faixa de endereços IP, tabela ARP e tabela de roteamento;

7.4.2. Deve permitir a configuração, monitoramento, adição e gerência de um dispositivo e também de um grupo de dispositivos;

7.4.3. Deve permitir a visualização dos equipamentos por tipo de dispositivo e sub-rede IP;

7.4.4. Deve permitir importar uma lista de dispositivos através de um arquivo;

7.4.5. Deve gerar o mapa e permitir a visualização da topologia física

7.4.6. Deve permitir a customização dos mapas de topologia d

dispositivos e links;

7.4.7. Deve permitir a visualização do painel frontal dos equipamentos gerenciados;

7.4.8. Deve permitir a criação de mapas do ambiente físico do data center, permitindo a criação de racks de equipamentos e a adição dos dispositivos gerenciados aos racks, de forma a se criar uma representação gráfica do ambiente no software de gerenciamento

7.4.9. Deve permitir, através da interface gráfica, executar cliente ssh e telnet para acesso à interface CLI do equipamento;

7.4.10. Deve permitir visualização de estatísticas de utilização do equipamento contemplando no mínimo utilização de memória e de CPU;

7.4.11. Deve permitir a visualização de informações dos dispositivos e componentes instalados, trazendo no mínimo, informações como fabricante, modelo, número de série, versão de hardware e software e outras informações que sejam disponibilizadas pelo equipamento gerenciado.

7.4.12. Deve permitir a localização de endereço IP e de endereço MAC na infraestrutura de rede, exibindo a qual dispositivo, porta e VLAN o dispositivo está conectado. Deve ser capaz de distinguir uma porta de usuário de um dispositivo de rede e exibir apenas resultados referentes a estações de trabalho ou terminais.

7.5. GERÊNCIA DE CONFIGURAÇÃO E MUDANÇA

7.5.1. Deve permitir a visualização do histórico dos arquivos de configuração dos dispositivos;

7.5.2. Deve permitir visualizar, comparar, aplicar e fazer o backup da configuração dos dispositivos gerenciados;

7.5.3. Deve permitir atualizar o software do dispositivo gerenciado;

7.5.4. Deve possibilitar a exclusão de arquivos da memória flash dos dispositivos gerenciados;

7.5.5. Deve permitir a criação de modelos de configuração para serem aplicados aos dispositivos gerenciados. Deve permitir criar modelos de parte da configuração e da configuração inteira do dispositivo;

7.5.6. Deve permitir o agendamento de backups da configuração dos dispositivos gerenciados;

7.5.7. Deve permitir a criação de relatórios de histórico de backups e atualizações de software;

7.5.8. Deve permitir a criação de regras de verificação de configuração e comparar com a configuração dos dispositivos gerenciados. Deve gerar relatório da verificação;

7.6. GERENCIAMENTO DE FALHAS

7.6.1. Deve suportar operação como servidor syslog, permitindo a recepção de mensagens Syslog dos dispositivos;

7.6.2. Deve possuir capacidade de gerar alarmes a partir de traps SNMP e mensagens Syslog;

7.6.3. Deve possuir mecanismo de análise de causa do problema para a supressão de eventos que são apenas sintoma da falha;

7.6.4. Deve possuir painel único de visualização dos alarmes e a partir desta tela verificar detalhes específicos de um alarme;

7.6.5. Deve possui a capacidade de enviar emails e mensagens via SMS para um administrador em caso de algum evento especificado de acordo com o nível de criticidade, dia da semana e horário;

7.7. GERENCIAMENTO DE DESEMPENHO

7.7.1. Deve possuir capacidade de monitorar o desempenho dos equipamentos gerenciados;

7.7.2. Deve possuir capacidade de monitorar a utilização de CPU, utilização de Memória, tempo de resposta e Disponibilidade;

7.7.3. Deve permitir ao administrador escolher quais monitores de desempenho devem ser configurados para ativar um alarme;

7.7.4. Deve permitir a visualização em tempo real de ítens monitorados;

7.8. GERÊNCIA DE LISTAS DE CONTROLE DE ACESSO

7.8.1. Deve permitir a visualização e configuração de listas de controle de acesso (ACL) nos equipamentos gerenciados e compatíveis;

7.8.2. Deve permitir a criação de templates ACLs para a distribuição em diversos equipamentos;

7.8.3. Deve permitir a criação de ACLs baseadas em endereço IP de origem e destino, endereço MAC de origem e destino, porta TCP/UDP e horário de ativação;

7.8.4. Deve possuir a capacidade de importar ACLs configuradas nos equipamentos gerenciados;

7.8.5. Deve possuir capacidade de avaliar o impacto de regras de ACL no desempenho da rede, sugerir e aplicar modificações para reduzir o efeito destas regras no desempenho da rede;

7.8.6. Deve possuir "wizard" de aplicação de ACLs em diversos equipamentos avaliando quais equipamentos suportam estas ACLs;

7.9. GERÊNCIA DE VLANS

7.9.1. Deve possuir capacidade de configurar VLANs globalmente e individualmente por switch gerenciado compatível;

7.9.2. Deve possuir capacidade de configurar interface vlan ou interfaces virtuais, adicionar portas de acesso e do tipo trunk;

7.9.3. Deve possuir capacidade de visualizar os dispositivos que fazem parte de uma VLAN no mapa de topologia;

7.10. ANÁLISE DE TRÁFEGO

7.10.1. Deve suportar o monitoramento de tráfego para equipamentos que não são capazes de gerar fluxos de dados, através do espelhamento de tráfego em uma porta de switch ou roteador e utilizando um aplicativo ou servidor dedicado a esta função.

7.10.2. Deve possibilitar a visualização, adição, modificação e remoção dos dispositivos geradores de fluxo monitorados.

7.10.3. Deve permitir a visualização de, no mínimo, as seguintes cara

7.10.3.1.- Endereço IP

7.10.3.2.- Nome do dispositivo
7.10.3.3.- Descrição do equipamento
7.10.3.4.- Comunidade SNMP
7.10.3.5.- Porta SNMP
7.10.3.6.- Estatísticas sobre Netstream ou sFlow

7.10.4. Deve permitir a classificação de aplicações baseadas nas camadas de rede 4 e 7.
7.10.5. Deve permitir o uso de expressões regulares para identificar uma aplicação através da pesquisa dentro do cabeçalho dos pacotes IP.
7.10.6. Deve permitir a criação de grupos baseados em categorias para agrupar protocolos ou aplicações com características semelhantes.
7.10.7. Deve fornecer relatórios e estatísticas de tráfego baseadas em Type of Service (TOS) e MPLS
7.10.8. Deve permitir a visualização de estatísticas de tráfego em interfaces dentro de uma instância VPN.
7.10.9. Deve suportar o envio de pacotes de pesquisa visando obter proativamente estatísticas de tráfego nos equipamentos monitorados.
7.10.10. Deve permitir a configuração de filtros para definir quais fluxos de dados recebidos pelo software serão analisados ou descartados.
7.10.11. Deve suportar a configuração de filtros de fluxo de dados baseados em, no mínimo, endereço IP de origem e destino, número de porta e protocolo
7.10.12. Deve suportar a configuração de filtros de fluxo de dados baseados em, pelo menos, os protocolos TCP, UDP, ICMP e IPv6 ICMP

7.11. AUDITORIA E RELATÓRIOS

7.11.1. Deve fornecer gráfico com as sessões estabelecidas entre todos os dispositivos IP ou hosts configurados durante a última hora.
7.11.2. Deve possibilitar a visualização gráfica das estatísticas de sessões de origem dos dispositivos IP ou hosts gerenciados
7.11.3. Deve possibilitar a visualização gráfica das estatísticas de sessões de destino dos dispositivos IP ou hosts gerenciados
7.11.4. Deve fornecer relatórios com quantidade de sessões identificando, pelo menos, os 10 dispositivos IP ou hosts de origem e destino com a maior quantidade de sessões ativas e a taxa máxima de sessões por segundo.
7.11.5. Deve fornecer gráfico para visualização do número total de sessões por minuto estabelecidas por um host ou dispositivo IP
7.11.6. Deve fornecer relatório com a quantidade total de sessões por minuto durante um período determinado e a taxa média de sessões por segundo durante este período para um host ou dispositivo IP.
7.11.7. Deve fornecer gráfico para visualização da taxa média em Mbps de um determinado tipo de tráfego entre todas as interfaces de rede monitoradas por um período de, pelo menos, 1 uma hora.
7.11.8. Deve fornecer gráfico para visualização dos 10 tipos de aplicações com maior volume de tráfego de entrada e de saída nas interfaces monitoradas em, pelo menos, 1 hora.
7.11.9. Deve fornecer relatórios de análise de tráfego que demonstrem a taxa média de tráfego de entrada e saída para todas as interfaces de rede monitoradas. Deve ser possível identificar, através destes relatórios, as estatísticas de utilização de um link, além do volume médio, mínimo e máximo do tráfego monitorado.

7.12. RELATÓRIOS

7.12.1. Deve possuir capacidade de gerar relatórios de:
7.12.2. - Ativos de Rede
7.12.3. - Estado dos dispositivos e Links
7.12.4. Deve possuir capacidade de gerar relatórios de dispositivos com as seguintes informações:
7.12.4.1.- Lista total de portas e lista de portas disponíveis
7.12.4.2. - Inventário dos equipamentos
7.12.4.3.- Informações sobre os dispositivos ativos
7.12.4.4.- Erros durante o processo de descoberta
7.12.4.5.- Topologia
7.12.5. Deve possuir capacidade de gerar relatórios de conexão com as seguintes informações:
7.12.5.1.- Estatísticas de disponibilidade de dispositivos
7.12.5.2.- Estatísticas de disponibilidade de links

7.13. CARACTERÍSTICAS GERAIS

7.13.1. Deve suportar a utilização de sistemas de banco de dados relacional Microsoft SQL Server, Oracle ou MySQL;
7.13.2. Deve permitir a instalação e utilização em sistemas operacionais Windows e Linux;
7.13.3. Deve suportar o gerenciamento de redes wireless, contemplando a configuração, monitoramento e topologia de dispositivos WLAN, permitindo o gerenciamento integrado de redes sem fio e cabeada na mesma plataforma, nativamente ou através de plug-in. A funcionalidade de gerenciamento de WLAN não necessita ser fornecida inicialmente;
7.13.4. Deve possuir capacidade e estar licenciado para gerenciamento de máquinas e switches virtuais ou switches;
7.13.5. O software de gerencia deve integrar a rede com plataformas VMware, Microsoft Hyper-V ou Citrix para a migração de VMs entre servidores físicos;
7.13.6. Deve possuir capacidade e estar licenciado para visualização d

7.14. ALTA DISPONIBILIDADE

7.14.1. Deve suportar balanceamento de carga entre até 5 servidores de análise de tráfego. Todas as licenças necessárias para esta funcionalidade devem ser fornecidas.

7.15. INSTALAÇÃO

7.15.1. Deve suportar instalação em sistemas operacionais Windows e Linux

7.15.2. Deve suportar o acesso através de um Web Browser convencional

7.15.3. Deve suportar a integração com a plataforma de gerenciamento de rede do mesmo fabricante.

7.15.4. GARANTIA E SUPORTE

7.15.5. Garantia e suporte do fabricante para a solução de software ofertada pelo período mínimo de 60 (sessenta) meses, incluindo a evolução para novas versões devendo o atendimento ser na modalidade 24x7 (vinte quatro horas por dia, sete dias da semana), com tempo de resposta máximo em 4 (quatro) horas.

7.15.6. Caso a garantia padrão do fabricante seja inferior a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante ("part number"), incorporada à solução.

7.15.7. O fabricante deve possuir canais de comunicação e ferramentas adicionais para suporte técnico online como "chat" e "e-mail" em seu site da internet com disponibilidade ainda de área para cadastro da solução de software ofertada, possibilitando assim que a CONTRATANTE possa receber de forma proativa, durante todo período da garantia as notificações de atualizações e correções ("hotfix") da solução;

7.15.8. A empresa fabricante da solução de software deverá dispor de um número telefônico tipo 0800 para suporte técnico e abertura de chamados técnicos.

7.15.9. A comprovação da modalidade da garantia deverá ocorrer através de documentação do fabricante de domínio público, não sendo aceita documentação emitida pelo fornecedor ou centro de distribuição para fins de comprovação que por ventura conflitem com catálogos, manuais, folders oficiais impressos ou da internet (devendo constar o endereço URL para folders da web). Caso não seja comprovada por um dos meios citados anteriormente, será possível a comprovação através da apresentação de documentação expressa do fabricante dos softwares, indicando o período de garantia dos produtos ofertados.

8. IMPLANTAÇÃO E TRANSFERÊNCIA DE TECNOLOGIA DA SOLUÇÃO DE GERENCIAMENTO DE ATIVOS DE REDE E ANÁLISE DE TRÁFEGO

8.1. CARACTERÍSTICAS GERAIS

8.1.1. Os serviços serão realizados em horário mais conveniente para o cliente, a fim de não impactar as atividades dos usuários, presencialmente nas dependências da CONTRATANTE ou remotamente conforme necessidades da CONTRATANTE;

8.2. IMPLANTAÇÃO

8.2.1. Instalação e configuração de 1 (uma) instância do serviço controle de acesso, contemplando configurações básicas para acesso à rede, dimensionamento, configuração de armazenamento;

8.2.2. Configuração de autenticação em Active Directory para usuários corporativos;

8.2.3. Configuração de autenticação de visitantes com portal de autosserviço para criação de usuários;

8.2.4. Configuração de no mínimo 50 (cinquenta) dispositivos de rede para autenticação na solução.

8.3. TRANSFERÊNCIA DE TECNOLOGIA

8.3.1. O treinamento deverá ser no realizado na modalidade workshop com tarefas práticas hands-on, visando assim a melhor fixação dos temas abordados com foco direto na explicação da tecnologia da solução como também nas rotinas de configuração, gerenciamento, administração e operação da mesma devendo ter duração mínima de 24 (vinte e quatro) horas onde será abordado no mínimo os seguintes tópicos:

8.3.2. Configuração de Active Directory como base de autenticação;

8.3.3. Configuração de autenticação de usuários corporativos;

8.3.4. Configuração de autenticação de usuários visitantes;

8.3.5. Configuração de portal de autosserviço;

8.3.6. Configuração de autenticação e autorização com RADIUS.

8.3.7. TREINAMENTO BÁSICO DE ADMNISTRAÇÃO DE SWITCHES HANDS-ON

8.3.7.1. O fornecimento desse item deverá contemplar 01 (um) voucher oficial do fabricante no Treinamento Básico de Administração dos Switches para 03 (três) profissionais da contratante;

8.3.7.2. O voucher deverá ter validade de pelo menos 12 (doze) meses;

8.3.7.3. O treinamento deverá ser de acordo com o calendário de treinamento do fabricante e ministrado em centro oficial de treinamento do mesmo ou remotamente, utilizando tecnologia de ensino a distância;

8.3.7.4. Deverá ser ministrado por profissional devidamente credenciado junto ao fabricante e apto a entregar o respectivo;

8.3.7.5. O treinamento deverá compreender a explicação da tecnologia da solução como também das rotinas de configuração, gerenciamento, administração e operação da mesma;

8.3.7.6. O treinamento deverá ter carga horária mínima de 24 (vinte e quatro) horas, ministrado no período de 08:00 às 12:00 e das 14:00 às 18:00.

9. SOLUÇÃO DE ANÁLISE DE PERFIL E CONTROLE DE ACESSO

9.1. LICENCIAMENTO

9.1.1. Licenciamento da SOLUÇÃO DE ANÁLISE DE PERFIL E CONTROLE DE ACESSO, contemplando o quantitativo mínimo de 1.000 (um mil) dispositivos, usuários corporativos ou autenticação, seja por dispositivo ou usuário;

9.1.2. Caso a solução ofertada necessite de licenciamento específico para credenciamento dos dispositivos, usuários (corporativos ou visitantes), deverá ser fornecido o quantitativo solicitado para ambos, de forma que a solução realize a análise de perfil e o controle de acesso dos 1.000 (um mil) dispositivos ou usuários (corporativos ou visitantes) simultâneos.

9.2. MÓDULO DE ANÁLISE DE PERFIL DE DISPOSITIVO

9.2.1. Deve implementar funcionalidade de classificação automática criando perfis de dispositivos, de forma a descobrir, classificar e agrupar os dispositivos conectados na rede;

9.2.2. Deve categorizar os dispositivos em pelo menos 3 níveis:

9.2.2.1. Por tipo de dispositivo (ex. Computador, Smartdevice, impressora, etc.);

9.2.2.2. Por sistema operacional (ex. Windows, Linux, MacOS, etc.);

9.2.2.3. Versão do sistema operacional (ex. Windows 7, Windows 2008 Server, etc.);

9.2.3. Deve ser capaz de gerar gráficos das categorias separando os dispositivos conforme suas características;

9.2.4. Deve suportar a coleta de informações, para classificação, usando no mínimo:

9.2.4.1. DHCP;

9.2.4.2. HTTP User-Agent;

9.2.4.3. MAC OUI;

9.2.4.4. ActiveSync plugin;

9.2.4.5. SNMP;

9.2.4.6. Subnet Scanner;

9.2.4.7. IF-MAP;

9.2.4.8. Cisco Device Sensor;

9.2.4.9. MDM;

9.2.4.10. TCP Fingerprinting.

9.2.5. Deve possuir dicionário de categorias de dispositivos pré-configurado e mecanismo de atualização do mesmo;

9.2.6. Deve suportar a integração com, no mínimo, as seguintes soluções de MDM de mercado AirWatch, MobileIron, JAMF, SOTI, XenMobile, SAP Afaria, MaaS 360 devendo comprovar a compatibilidade em documentação oficial do fabricante;

9.2.7. Deve permitir priorização na ordem de criação dos perfis com no mínimo as seguintes características:

9.2.7.1. Agente proprietário;

9.2.7.2. HTTP User-Agent;

9.2.7.3. SNMP;

9.2.7.4. DHCP;

9.2.7.5. MAC OUI.

9.2.8. A solução de análise de perfil de usuários deverá permitir consultas a sua base, pela solução de controle de acesso para validação de dispositivos com base no seu perfil.

9.3. MÓDULO DE CONTROLE DE ACESSO DE DISPOSITIVOS E USUÁRIOS

9.3.1. A Solução deverá dar suporte a no mínimo as seguintes bases de dados:

9.3.1.1. Microsoft Active Directory;

9.3.1.2. Kerberos;

9.3.1.3. Diretórios LDAP;

9.3.1.4. Novell eDirectory;

9.3.1.5. OpenLDAP;

9.3.1.6. Sun Directory Server;

9.3.1.7. PostgreSQL;

9.3.1.8. Oracle 11g;

9.3.1.9. MariaDB;

9.3.1.10. MSSQL;

9.3.1.11. Servidores de Token;

9.3.1.12. Base de dados SQL interna;

9.3.1.13. Lista interna estática de hosts.

9.3.2. Deve suportar "Single Sign-on" (SSO) através de SAML v2.0;

9.3.3. Deve implementar gerenciamento e aplicação de políticas de autorização de acesso de usuários com base em:

9.3.3.1. Atributos do usuário autenticado;

9.3.3.2. Hora do dia, dia da semana;

9.3.3.3. Tipo de dispositivo utilizado;

9.3.3.4. Localização do usuário;

9.3.3.5. Tipo de autenticação utilizada.

9.3.4. Deve permitir a visualização de todas informações relativas a cada transação e autenticação em uma única tela, a solução deverá trazer no mínimo as seguintes informações:

9.3.4.1. Data e Hora;

9.3.4.2. Mac Address do dispositivo;

9.3.4.3. Classificação do dispositivo;

9.3.4.4. Usuário;

9.3.4.5. Equipamento que requisitou a autenticação (origem);

9.3.4.6. Método de autenticação utilizado;

9.3.4.7. Fonte de autenticação utilizada para validação;
9.3.4.8. Perfil de acesso aplicado;
9.3.4.9. Atributos de entrada do protocolo utilizados na requisição (ex. RADIUS);
9.3.4.10. Informações de resposta da solução para o elemento de rede;
9.3.4.11. Alertas em caso de falha;
9.3.4.12. LOGS já filtrados para a requisição em análise.

9.3.5. Deve possuir Dashboard customizável, onde deve permitir a visualização de no mínimo as seguintes informações:
9.3.5.1. Lista com últimos Alertas do sistema;
9.3.5.2. Gráfico com todas as requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ ou HWTACACS e Autenticações Web;
9.3.5.3. Gráfico com o status das autenticações aceitas e rejeitadas nos últimos 7 dias;
9.3.5.4. Gráfico com a categorização dos dispositivos classificados pela solução, divididos de acordo com as categorias de classificação;
9.3.5.5. Últimas falhas de autenticação;
9.3.5.6. Gráfico com as requisições de avaliação de postura dos dispositivos, divididos em:
9.3.5.7. Saudáveis (dentro das políticas estabelecidas);
9.3.5.8. Não saudáveis (que estão fora das políticas estabelecidas);
9.3.5.9. Lista com as últimas autenticações;
9.3.5.10. Lista com as últimas autenticações com sucesso;
9.3.5.11. Utilização de CPU do sistema, no mínimo nos últimos 30 minutos;

9.3.6. Deve possuir base de regras e categorias de dispositivos pré-configurada e mecanismo de atualização da mesma;
9.3.7. Deve suportar a integração com no mínimo as seguintes soluções de MDM de mercado AirWatch, MobileIron, JAMF, SOTI, XenMobile, SAP Afaria, MaaS 360 devendo comprovar a compatibilidade em documentação oficial do fabricante;
9.3.8. Deve suportar autenticações via OAuth2, Facebook, Twitter, LinkdIn, Office365 e Google Apps;
9.3.9. Deve possuir recursos integrados de AAA: RADIUS, TACACS+, HWTACACS e Kerberos;
9.3.10. Deve possuir suporte aos seguintes recursos:
9.3.10.1. RADIUS;
9.3.10.2. RADIUS CoA;
9.3.10.3. TACACS+ ou HWTACACS;
9.3.10.4. Web authentication;
9.3.10.5. SAML v2.0;
9.3.10.6. EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS);
9.3.10.7. PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public);
9.3.10.8. TTLS (EAP-MSCHAPv2, EAP-GTC, EAP- TLS, EAP-MD5, PAP, CHAP);
9.3.10.9. EAP-TLS;
9.3.10.10. PAP, CHAP, MSCHAPv1, MSCHAPv2, and EAP-MD5;
9.3.10.11. Windows machine authentication;
9.3.10.12. MAC address authentication (dispositivos sem suporte a 802.1X);
9.3.11. Deve suportar verificação de vulnerabilidade através de varredura de portas;
9.3.12. Deve suportar à aplicação de políticas em ambiente com múltiplos fornecedores de Wireless, cabeado e VPN;
9.3.13. Deve possuir CA integrada, para geração de certificados para os dispositivos que forem se autenticar na rede;
9.3.14. Deve suportar à integração com plataforma de terceiros usando HTTP/RESTful API;
9.3.15. Deve permitir que a solução faça consultas em bases SQL, com o objetivo de buscar informação a serem utilizadas durante o processo de autenticação dos usuários;
9.3.16. Deve possuir suporte a administração através de IPv6;
9.3.17. Deve possuir ferramenta para gerenciar os processos de credenciamento, autenticação, autorização e contabilização de usuários visitantes através de portal web seguro;
9.3.18. Deve implementar a criação de grupos de autorizadores com privilégios distintos de criação de credenciais temporárias e atribuição de permissões de acesso aos clientes;
9.3.19. Deve permitir realizar a autenticação dos autorizadores em base externa do tipo Microsoft Active Directory ou LDAP e atribuir o privilégio ao autorizador de acordo com o seu perfil;
9.3.20. Deve implementar as funcionalidades de geração de lotes de credenciais aleatórias, temporárias, pré-autorizadas;
9.3.21. Deve implementar a importação e exportação da relação de credenciais temporárias através de arquivos txt ou csv;
9.3.22. Deve permitir a configuração do tempo de validade das credenciais, baseando-se na criação da conta ou no primeiro login da conta;
9.3.23. Deve permitir que o visitante crie sua própria credencial temporária (autosserviço) através de portal web, com ou sem a necessidade de um autorizador;
9.3.24. Deve permitir a customização do formulário de criação de credenciais, a ser preenchido pelo autorizador ou pelo visitante em caso de autosserviço, especificando quais informações cadastrais dos visitantes são obrigatórias ou opcionais;
9.3.25. Deve permitir a customização do nível de segurança da senha temporária que será gerada ao visitante, especificando a quantidade mínima de caracteres e o uso senha;

9.3.26. Deve exigir que o usuário visitante aceite o "Termo de uso da rede" a cada login ou apenas no primeiro login;
9.3.27. Deve permitir o envio das credenciais aos usuários registrados através de mensagens SMS (Short Message Service), e-mail ou impressão local.

9.4. GARANTIA E SUPORTE
9.4.1. Garantia e suporte do fabricante para a solução de software ofertada pelo período mínimo de 60 (sessenta) meses, incluindo a evolução para novas versões devendo o atendimento ser na modalidade 24x7 (vinte quatro horas por dia, sete dias da semana), com tempo de resposta máximo em 4 (quatro) horas.
9.4.2. Caso a garantia padrão do fabricante seja inferior a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante ("part number"), incorporada à solução.
9.4.3. O fabricante deve possuir canais de comunicação e ferramentas adicionais para suporte técnico online como "chat" e "e-mail" em seu site da internet com disponibilidade ainda de área para cadastro da solução de software ofertada, possibilitando assim que a CONTRATANTE possa receber de forma proativa, durante todo período da garantia as notificações de atualizações e correções ("hotfix") da solução;
9.4.4. A empresa fabricante da solução de software deverá dispor de um número telefônico tipo 0800 para suporte técnico e abertura de chamados técnicos.
9.4.5. A comprovação da modalidade da garantia deverá ocorrer através de documentação do fabricante de domínio público, não sendo aceita documentação emitida pelo fornecedor ou centro de distribuição para fins de comprovação que por ventura conflitem com catálogos, manuais, folders oficiais impressos ou da internet (devendo constar o endereço URL para folders da web). Caso não seja comprovada por um dos meios citados anteriormente, será possível a comprovação através da apresentação de documentação expressa do fabricante dos softwares, indicando o período de garantia dos produtos ofertados.

9.5. IMPLANTAÇÃO DA SOLUÇÃO
A implantação deverá contemplar a instalação e configuração de todos os softwares e serviços necessários para o funcionamento completo da solução de Controle de Acesso.
9.5.1. Instalação e configuração de 1 (uma) instância do serviço controle de acesso, contemplando configurações básicas para acesso à rede, dimensionamento, configuração de armazenamento;
9.5.2. Configuração de autenticação em Active Directory para usuários corporativos;
9.5.3. Configuração de autenticação de visitantes com portal de autosserviço para criação de usuários;
9.5.4. Configuração de no mínimo 30 (trinta) dispositivos de rede para autenticação na solução;
9.5.5. Configuração de portal de autosserviço;
9.5.6. Configuração de autenticação e autorização com RADIUS.
9.5.7. TREINAMENTO BÁSICO DA SOLUÇÃO DE CONTROLE DE ACESSO HANDS-ON
9.5.7.1. O fornecimento desse item deverá contemplar 01 (um) voucher oficial do fabricante no Treinamento da Solução de Controle de Acesso para 01 (um) profissional da contratante;
9.5.7.2. O voucher deverá ter validade de pelo menos 12 (doze) meses;
9.5.7.3. O treinamento deverá ser de acordo com o calendário de treinamento do fabricante e ministrado em centro oficial de treinamento do mesmo ou remotamente, utilizando tecnologia de ensino a distância;
9.5.7.4. Deverá ser ministrado por profissional devidamente credenciado junto ao fabricante e apto a entregar o respectivo;
9.5.7.5. O treinamento deverá compreender a explicação da tecnologia da solução como também das rotinas de configuração, gerenciamento, administração e operação da mesma;
9.5.7.6. O treinamento deverá ter carga horária mínima de 40 (Quarenta) horas, ministrado no período de 08:00 às 12:00 e das 14:00 às 18:00;

10. ACCESS POINT (PONTO DE ACESSO) WLAN:
10.1. Ponto de Acesso 802.11ac – 4X4 UM-MIMO –Wave 2
10.2. Cada access point deverá ser fornecido com uma fonte POE;
10.3. O Ponto de Acesso deverá trabalhar no modo de controladora virtual com até 64 APs gerenciada via HTTP/HTTPS no cluster ou no modo de controladora/software com suporte a no mínimo de 1000 Ponto de Acesso no mesmo grupo ou vários grupos respeitando o número máximo de 1000 APs;
10.4. PONTO DE ACESSO INTERNO:
10.4.1. Equipamento de Ponto de Acesso para rede local sem fio, configurável via software, com funcionamento simultâneo nos padrões IEEE 802.11a/n/ac, 5GHz, e IEEE 802.11b/g/n, 2.4GHz;
10.4.2. Os pontos de acesso deverão possuir certificado emitido pelo "WIFI Alliance" comprovando os seguintes padrões, protocolos e funcionalidades:
10.4.2.1. IEEE 802.11a;
10.4.2.2. IEEE 802.11b;
10.4.2.3. IEEE 802.11g;
10.4.2.4. IEEE 802.11n;
10.4.2.5. IEEE 802.11ac Wave 2;
10.4.2.6. IEEE 802.11e WMM;
10.4.2.7. WPA®;
10.4.2.8. WPA2®;

10.4.2.9. EAP-TLS;
10.4.2.10. EAP-TTLS/MSCHAPv2;
10.4.2.11. PEAPv0/EAP-MSCHAPv2;
10.4.2.12. PEAPv1/EAP-GTC;
10.4.2.13. WMM®;
10.4.2.14. Short Guard Interval (SGI);
10.4.2.15. Packet Aggregation (A-MPDU);
10.4.2.16. DPI
10.4.2.17. 802.1x

10.4.3. Operar com canais de 40MHz e 80MHz;

10.4.4. Deve implementar funcionamento em modo gerenciado por controlador virtual ou controladora /software, para configuração de seus parâmetros wireless, gerenciamento das políticas de segurança, QoS e monitoramento de RF;

10.4.5. O ponto de acesso deverá ser gerenciado centralizado diretamente ou remotamente;

10.4.6. Implementar mecanismo de funcionamento para trabalhar para garantira redundância em arquitetura distribuída ou através de controladora;

10.4.7. Deve permitir, simultaneamente, usuários configurados nos padrões IEEE 802.11b, 802.11g, 802.11a, 802.11n e 802.11ac;

10.4.8. Implementar as seguintes taxas de transmissão:
10.4.8.1. IEEE 802.11 a/g: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps;
10.4.8.2. IEEE 802.11 b: 11; 5,5; 2 e 1 Mbps;
10.4.8.3. IEEE 802.11n: MSC0 – MSC31 (6.5 a 600Mbps);
10.4.8.4. IEEE 802.11ac: MCS0 - MCS9, NSS = 1 a 4 (6.5 a 1733 Mbps);

10.4.9. Possuir capacidade de selecionar automaticamente o canal de transmissão;

10.4.10. Permitir o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar a célula RF;

10.4.11. Possuir suporte a pelo menos 8 SSIDs por rádio;

10.4.12. Deve suportar no mínimo 512 clientes associados;

10.4.13. Permitir habilitar e desabilitar a divulgação do SSID;

10.4.14. Implementar padrão WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como, VoIP, vídeo, dentre outras;

10.4.15. Deve suportar roaming entre os Pontos de Acessos;

10.4.16. Possuir antenas integradas, compatíveis com as frequências de rádio dos padrões IEEE 802.11a/n/ac com ganho de, pelo menos, 4.4 dBi e IEEE 802.11/b/g/n com ganho de, pelo menos, 3.6 dBi, com padrão de irradiação omnidirecional (4x4 MIMO);

10.4.17. Suportar operação Wave 2 com 4x4 MIMO e no mínimo 4 streams simultâneo (multi user MIMO);

10.4.18. Possuir potência máxima de transmissão de, no mínimo, 18 dBm para IEEE 802.11a/b/g/n/ac;

10.4.19. Deve possuir sensibilidade de recepção de valor menor ou igual: a -92 dBm a 6Mbps no padrão 802.11g; e a -89 dBm a 6Mbps no padrão 802.11a, por canal de recepção;

10.4.20. Implementar a pilha de protocolos TCP/IP;

10.4.21. Possuir, no mínimo, 1(uma) interfaces IEEE 802.3 10/100/1000BaseT Ethernet, auto-sensing, com conectores RJ-45, para conexão à rede local;

10.4.22. Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet ou serial;

10.4.23. Possuir 1 (uma) porta de console para gerenciamento e configuração com conector RJ-45;

10.4.24. Possuir 1(uma) porta USB;

10.4.25. Deve suportar no mínimo 3(três) níveis de administração;

10.4.26. Deve suportar NTP Server;

10.4.27. Deve configurar-se automaticamente ao ser conectado na rede;

10.4.28. Possibilitar alimentação elétrica local e via padrão PoE ou PoE+;

10.4.29. Possuir estrutura que permita fixação do equipamento em teto e parede e fornecer acessórios para que possa ser feita a fixação;

10.4.30. Deve ser acompanhado de todos os acessórios necessários para operacionalização do equipamento, tais como: softwares, cabos de console, cabos de energia elétrica, documentação técnica e manuais (podendo ser em CD-ROM) que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;

10.4.31. Possuir suporte a trava padrão "Kensington security lock point" ou similar;

10.4.32. Implementar varredura de RF nas bandas 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, para identificação de Pontos de Acesso intrusos não autorizados (rogues) e interferências no canal habilitado ao ponto de acesso e nos demais canais configurados na rede WLAN, sem impacto no seu desempenho;

10.4.33. Deve implementar localização da AP mais próxima da AP intrusa identificada;

10.4.34. Deve suportar “White e Black list”;

10.4.35. Implementar autenticação via IEEE 802.1x;

10.4.36. Implementar autenticação via portal de visitante. O portal visitante deverá suportar customização de no mínimo logotipo, imagem principal e o termo de aceitação;

10.4.37. Implementar criptografia do tráfego local;

10.4.38. Implementar algoritmo de criptografia TKIP, AES e CCMP;
10.4.39. Deve possuir modo dedicado de funcionamento de análise de espectro das faixas de frequência de 2.4 e 5 GHz identificando fontes de interferência nessas faixas;
10.4.40. Deve possibilitar analise de espectro nos canais em que estiver provendo acesso, sem desconectar os usuários;
10.4.41. Deve disponibilizar informações gráficas de análise de espectro em conjunto com o controlador a controladora virtual ou no gerenciamento;
10.4.42. O equipamento ofertado deve possuir homologação junto à ANATEL com certificados disponíveis publicamente no endereço eletrônico desta agência, conforme a Resolução número 242.

11. SISTEMA DE GERENCIAMENTO DOS ACCESS POINTS

11.1. A solução wireless LAN deve ser baseada no IEEE 802.11 e deve possuir WFA certified para Dados e Voz.
11.2. A solução wireless LAN deve possuir uma arquitetura distribuída, eliminando assim, o tunelamento do tráfico garantindo a baixa latência e também a redundância da solução.
11.3. A solução de wireless LAN deve suportar implementação no formato Multi-site deployment com pontos de acesso espalhados por vários domínios de transmissão (VLAN) que podem operar em diferentes ambientes de RF.
11.4. A solução deve oferecer recursos avançados como Detecção / Prevenção de Intrusão e um Portal Convidados para gerenciar a conexão de convidados.
11.5. A solução de wireless LAN deve ser gerenciada de forma centralizada através controladora física ou virtual em alta disponibilidade.
11.6. A solução de wireless LAN deve possuir licenças compatíveis para gerenciar no mínimo 50 Access Points. A solução deve suportar futura ampliação de mais 4000 Access Points com a simples adição de licenças para essa finalidade.
11.7. Controle Acesso, Autenticação e Encriptação
  11.7.1. A solução wireless LAN deve suportar MAC based authentication.
  11.7.2. A solução wireless LAN deve suportar 802.1x based authentication.
  11.7.3. Implementar protocolo de autenticação para controle do acesso administrativo a solução com mecanismos de AAA;
  11.7.4. Deverá suportar os seguintes métodos EAP-PEAP, EAP-TLS e EAP-TTLS;
  11.7.5. A solução de rede sem fio deve ter a capacidade de utilizar atributos RADIUS para atribuir cada usuário / dispositivo autenticado, a uma regra específica. Dessa forma o perfil criado irá definir a VLAN, forma segurança e QoS através de funções e políticas QoS que podem ser diretamente integradas com as funções definidas nos servidores de autenticação existentes.
11.8. A solução de wireless LAN deve suportar os seguintes standards de encriptação: WPA2_AES, WPA2_TKIP, WPA_AES, WPA_TKIP, DYNAMIC_WEP, WPA_PSK_AES, WPA2_PSK_AES, WPA2_PSK_TKIP.
11.9. A solução de wireless LAN deve suportar os seguintes suplicantes para 802.1x : Windows 7, 10, MAC OS, IOS, Android, Chromebook.
11.10. A solução de wirelless LAN deve possuir gerenciamento de Convidados com base em um Portal Captive incorporado, fornecendo autenticação baseada na web para convidados e visitantes.
11.11. O Portal Captive deve permitir customização da página de apresentação.
11.12. O Portal Captive deve suportar os seguintes métodos de autenticação:
  11.12.1. Nome (username) e Senha (Password)
  11.12.2. Código de acesso
  11.12.3. Termo e condições de aceite
  11.12.4. Mídia Social, no mínimo facebook e google
11.13. A solução WLAN deve permitir o auto-registro de convidados. A solução também deve suportar a opção da liberação do acesso de convidado, através de um Sponsor definido quando o visitante preencher o cadastro de registro. A solução deverá vir equipada para no mínimo 500 visitantes simultâneos.
11.14. O modelo de licenciamento da solução de gerenciamento de convidados deve basear-se na quantidade de dispositivos.
11.15. A solução de gerenciamento de convidados deve permitir definir um período de validade para um dispositivo autenticado.
11.16. A solução de wireless LAN deve implementar strict guests traffic isolation.
11.17. A solução WLAN deve suportar BYOD aplicando as características corporativas em dispositivos particulares/terceiros (on-boarding) sem necessidade de componentes adicionais.
11.18. O processo de on-boarding para dispositivos particulares deve ser baseado no perfil corporativo do funcionário.
11.19. A aplicação do BYOD deve permitir configurar o período de permanência do dispositivo e o máximo de dispositivos por conta.
11.20. O modelo de licenciamento para o BYOD deve ser baseado no número de dispositivos.
11.21. Gerenciamento RF
  11.21.1. A solução WLAN deve permitir ajustes RF automático e manual de canal e potência.
  11.21.2. A solução de WLAN deve suportar Short Guard Interval.
  11.21.3. A solução WLAN deve conectar o clinte na melhor banda e canal (2.4GHz / 5GHz) considerando o número de clientes associados em cada banda e a utilização.
  11.21.4. Se nenhuma banda / canal (2.4GHz / 5GHz) estiver sobrecarregado ou número máximo de clientes associados, o AP deve, por padrão, orientar um novo cliente para a ba
  11.21.5. Em caso a banda de 5GHz no limite de clientes, o AP dev

automaticamente.

11.21.6. Quando um novo cliente se conectar à rede, o novo cliente deve ser orientado para o AP que possui o menor número de clientes associados, permitindo balanceamento de carga inteligente / dinâmico.

11.21.7. A solução WLAN deve suportar analise do ambiente, a fim de identificar interferências / rogue APs e detecção de ataques a rede sem fio.

11.21.8. Essa função não deve ter impacto de performance quando ativado prioridades de voz ou vídeo (SIP e H.323).

11.22. Detecção de Intruso e Prevenção

11.22.1. A solução de WLAN deve suportar wIDS/wIPS sem necessidade de licenças e equipamentos adicionais.

11.22.2. A solução de WLAN deve ter capacidade de identificar interferências.

11.22.3. A solução de WLAN deve ser capaz de identificar e conter APs Piratas (Rogue APs).

11.22.4. A solução WLAN deve permitir a classificação um AP como um AP Pirata para melhor controle e administração.

11.22.5. A solução WLAN deve permitir criar políticas para detecção de ataques de AP.

11.22.6. A solução WLAN deve permitir criar políticas para detecção de ataques de clientes.

11.22.7. A solução WLAN deve poder criar “BlackList “de clientes da WLAN, manualmente ou automaticamente depois de um ataque ter sido detectado.

11.22.8. A solução WLAN deve permitir configurar a duração da “ blacklist “.

11.22.9. A solução WLAN deve permitir configurar o limite de tempo para falha de autenticação.

11.23. Qualidade de Serviço

11.23.1. A solução WLAN deve suportar Quality of Service (QoS) ajustado, permitindo as seguintes ações com base na identidade do usuário conectado:

11.23.2. Baseado em ACL (endereço IP de origem / destino e portas TCP / UDP) permitir / negar decisão;

11.23.3. Marcação prioritária de QoS e filas;

11.23.4. A solução LAN sem fio deve cumprir o padrão WMM 802.11e e deve suportar QoS (802.1p / DSCP) para o mapeamento da fila WMM.

11.23.5. A solução WLAN deve suportar Deep Packet Inspection (DPI) de tráfego permitindo que um administrador controle os aplicativos, incluindo não apenas o bloqueio de aplicativos, mas também permitindo priorizar e limitar as aplicações.

11.23.6. A solução de WLAN deve ser capaz de definir e garantir a largura de banda com base por SSID e também deve definir e garantir a largura de banda com base no perfil do usuário / dispositivo.

11.23.7. A solução WLAN deve permitir definir o número máximo de clientes por banda / rádio e por AP para um SSID específico.

11.23.8. A solução de WLAN deve suportar mecanismos de otimização de tráfego de transmissão.

11.23.9. Através do recurso de IGMP snooping da rede, a solução de WLAN deve ser capaz de otimizar o tráfego multicast convertendo o tráfego multicast para o tráfego unicast.

11.23.10. A solução Wlan deve suportar otimização de Multicast para alto trafego.

11.23.11. A solução de WLAN deve suportar WMM Automatic Power Save delivery (APSD) para conservar a bateria dos dispositivos dos clientes.

11.23.12. A solução de WLAN deve suportar por identificar por default trafico de Voz e Vídeo (SIP and H323) para priorização dos serviços citados.

11.24. Mobilidade

11.24.1. A solução WLAN deve suportar as capacidades de roaming de camada 2.

11.24.2. A solução WLAN deve suportar o roaming de camada 3 entre as APs.

11.24.3. A solução WLAN deve suportar Opportunistic Key Caching (802.11k).

11.24.4. A solução WLAN deve ser complaince ao padrão 802.11r

11.25. Gerenciamento

11.25.1. A solução WLAN deve ser através de gerenciamento centralizado baseado em uma GUI WEB incorporada e segura.

11.25.2. O gerenciamento centralizado deverá ser na forma de um dispositivo virtual que pode ser instalado em cima de qualquer um dos seguintes hypervisors: VMware ESXi, Microsoft HyperV e Oracle VirtualBox. O hardware será de responsabilidade da CONTRATANTE.

11.25.3. O gerenciamento centralizado deve ser capaz de gerenciar também os equipamentos com fio (switches) para uma abordagem de "gerenciamento unificado".

11.25.4. A solução WLAN deve ser capaz de descobrir automaticamente novas APS quando adicionadas.

11.25.5. A função de gerenciamento centralizado deve permitir exibir a topologia física da rede.

11.25.6. A função de gerenciamento centralizado deve permitir a configuração dos equipamentos e o backup em massa.

11.25.7. A função de gestão centralizada deve permitir o acesso a todos os recursos WIPS / WIDS.

11.25.8. O gerenciamento centralizado deve ter capacidade, com base em um arquivo de assinatura de aplicativos, uma visão na camada de aplicação (por exemplo, facebook.com, youtube.com, salesforce.com...), mesmo que os aplicativos sejam executados em cima dos protocolos HTTP ou HTTPS. Deve também permitir o controle e bloqueio dessas aplicações.

11.25.9. O gerenciamento centralizado deve permitir exibir a
determinada área ("Mapa de calor").

11.25.10. O gerenciamento centralizado deve permitir, antes da implantação, determinar a localização ideal de Pontos de Acesso (Planejamento de RF).

11.25.11. O gerenciamento centralizado deve implementar aplicativos de gerenciamento de Visitante com auto provisionamento e BYOD.

12. MODULO GBIC 10GB PARA ATÉ 300M

12.1. CARACTERÍSTICAS TÉCNICAS MÍNIMAS

12.1.1. Deve ser do tipo SFP+ de 10GBASE-SR com conector LC para distancias de no mínimo 300 (trezentos) metros;

12.1.2. Deve possuir compatibilidade integral com os Itens 3 (switch tipo 3) e 4 (switch tipo 4).

12.2. GARANTIA E SUPORTE

12.2.1. O equipamento ofertado deverá possuir garantia do fabricante do equipamento na modalidade on-site pelo período mínimo de 12 (doze) meses para reposição de peças, mão de obra e atendimento no local. No período da garantia o prazo máximo para o reparo de equipamentos defeituosos a condição normal de funcionamento deverá ser de até 07 (sete) dias úteis;

12.2.2. Caso a garantia padrão do fabricante seja inferior a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante (part number), incorporado ao equipamento;

12.2.3. Por questões de compatibilidade, gerência, suporte e garantia, deve ser do próprio fabricante ou estar em conformidade com a política de garantia do mesmo, não sendo permitida a integração de itens de terceiros que possam acarretar em perda parcial da garantia ou não realização da manutenção técnica pelo próprio fabricante quando solicitada.

13. MODULO GBIC 10GB PARA ATÉ 10KM

13.1. CARACTERÍSTICAS TÉCNICAS MÍNIMAS

13.1.1. Deve ser do tipo SFP+ de 10GBASE-LR com conector LC para distancias de no mínimo 10 (dez) quilômetros;

13.1.2. Deve possuir compatibilidade integral com os Itens 3 (switch tipo 3) e 4 (switch tipo 4).

13.2. GARANTIA E SUPORTE

13.2.1. O equipamento ofertado deverá possuir garantia do fabricante do equipamento na modalidade on-site pelo período mínimo de 12 (doze) meses para reposição de peças, mão de obra e atendimento no local. No período da garantia o prazo máximo para o reparo de equipamentos defeituosos a condição normal de funcionamento deverá ser de até 07 (sete) dias úteis;

13.2.2. Caso a garantia padrão do fabricante seja inferior a exigida, a proponente deverá informar em sua proposta o código de serviço de garantia do fabricante (part number), incorporado ao equipamento;

13.2.3. Por questões de compatibilidade, gerencia, suporte e garantia, deve ser do próprio fabricante ou estar em conformidade com a política de garantia do mesmo, não sendo permitida a integração de itens de terceiros que possam acarretar em perda parcial da garantia ou não realização da manutenção técnica pelo próprio fabricante quando solicitada.

2 – AVALIAÇÃO DE SOLUÇÕES

Foram realizadas provas de conceito (POC) com equipamentos de 3 fabricantes (HP, Alcatel e Aerohive) e consultados fornecedores para identificação das soluções que atendem à demanda dentro dos recursos disponíveis conforme doc. PAD nº 88960/2018 que contém e-mails sobre tratativas de provas de conceito e reuniões sobre o projeto de rede deste regional. Também foram avaliados os pregões nº 25/2018 da Universidade Federal do Amapá e o pregão nº 07/2019 da Polícia Federal que tem os mesmos objetos da demanda do TRE-MA.

Como a necessidade de negócio do TRE-MA é a substituição de equipamentos desprovidos de garantia e sem suporte prestado pelo fabricante optou-se como solução a substituição dos equipamentos que fazem a interconexão entre todos os prédios e o datacenter do TRE-MA. Acrescentamos aos requisitos opções de segurança de acesso. E como estratégia para a substituição fizemos reuniões com fornecedores e provas de conceito com os fornecedores de equipamentos de rede no mercado nacional (doc. PAD. Nº 88960/2019) e consultamos outras licitações que tinham o mesmo escopo da necessidade deste tribunal.

Também foi o doc. PAD nº 88448/2019 tem uma tabela do fabricante com todas as datas de enceramento de venda, fim de suporte de hardware, software e fim de suporte de peças dos equipamentos instalados no TRE-MA, onde se verifica que não há mais a possibilidade de contratação de suporte para os equipamentos. Portanto, dada a idade avançada dos equipamentos optamos pela substituição dos equipamentos com o objetivo de evitar interrupção dos serviços de comunicação da rede do TRE-MA.

A garantia de atualização e suporte técnico de 5(cinco) anos faz-se necessária em face da criticidade dos serviços de TI que serão assegurados, cuja disponibilidade contínua é essencial para o desempenho das atribuições administrativas e judiciais deste Tribunal. Ademais, privilegia-se também o Princípio da Economicidade, considerando que, ao adotarmos comportamento usual de mercado conforme doc. PAD nº 93221/2019 (demonstra que é uma prática de mercado e também o percentual do custo da garantia frente ao valor do produto. No caso específico, de 7% (sete por cento), a administração se desincumbe da necessidade de repetição de procedimento licitatório, com todos os seus custos envolvidos, tão logo ultrapassado o exercício financeiro.

Para a coleta de preços foi feita pesquisa em sistema de registro de preços e consulta por email/telefone para 03 (três) empresas especializadas conforme tabela abaixo e documento anexo:

Empresa	Observação
SmartWave Networks	Enviou proposta somente solução wifi
Plugnet Informática	Enviou proposta todos os itens
Lettel Distribuidora de Telefonia	Enviou proposta todos os itens
Fonmart Tecnologia	Enviou proposta todos os itens

Sendo assim, quanto aos custos avaliados temos:

Utilizamos como premissa para o cálculo do preço médio a utilização dos valores das licitações. Os valores muito díspares do valor das licitações eram retirados do cálculo do valor médio para fins de obtenção do coeficiente de variação e valor médio. Os valores de pesquisas feitas na internet com valores muito diferentes de valores de licitações também foram retirados do cálculo do valor médio e coeficiente de variação. A motivação da exclusão de valores de internet é não termos a garantia que os equipamentos atendessem todos os requisitos especificados, por conseguinte o valor médio poderia representar um equipamento que não atendesse a necessidade do TRE-MA.

ITEM	FONTE DE PREÇO	VALOR
1 - Switch Tipo 1 – Mínimo 8 portas par trançado L2	Plugnet informática	R$ 2.800,00
	Lettel Distrib	~~R$ 3.665,40~~[1]
	Fonmart	~~R$ 3.220,42~~[1]
	Site showdigital.com.br	~~R$ 1.156,15~~[1]
	Site netcomputadores.com.br	R$ 2.144,37
	Site atera.com.br	~~R$ 1.076,84~~[1]
	Site Oukeystore.com.br	R$ 1.599,99
	Pregão 7/2018 UFMG	R$ 1.697,41
	Pregão 76/2018 TRE-MG	R$ 1.702,00
Média		R$ 1.988,75
Quantidade		15
Total		**R$ 29.831,25**

1. Valores desconsiderados devido sua utilização gerar um coeficiente de variação maior que 25%.

ITEM	FONTE DE PREÇO	VALOR
2 - Switch Tipo 2 – Mínimo 24 portas par trançado incluindo 2	Plugnet informática	R$ 18.000,00
	Lettel Distrib	R$ 15.168,00
	Fonmart	R$ 25.763,49
	Site dreamshop.com.br	~~R$ 5.497,90~~[1]
	Site bits.com.br	~~R$ 5.085,26~~[1]
	Site Oukeystore.com.br	~~R$ 3.449,99~~[1]
	Site Oukeysto	

portas 10Gb	Site Oukeystore.com.br	~~R$ 3.899,99~~[1]
	Site Fouserv.com.br	~~R$ 9.499,00~~[1]
	Pregão 42/2017 UNILA	R$ 23.069,00
	Pregão 56/2017 Aeronáutica	~~R$ 42.000,00~~[1]
	Pregão 65/2018 UFPA	~~R$ 39.900,00~~[1]
	Pregão 25/2018 UNIFAP	R$ 16.000,00
Média		R$ 19.600,10
Quantidade		7
Total		**R$ 137.200,70**

2. Valores desconsiderados devido sua utilização gerar um coeficiente de variação maior que 25%.

ITEM	FONTE DE PREÇO	VALOR
3 - Switch Tipo 3 Mínimo 48 portas par trançado incluindo 2 portas 10Gb	Plugnet informática	R$ 25.000,00
	Lettel Distrib	R$ 26.465,00
	Fonmart	R$ 25.763,49
	Site Oukeystore.com.br	~~R$ 7.779,99~~[1]
	Site Oukeystore.com.br	~~R$ 6.499,99~~[1]
	Site Oukeystore.com.br	~~R$ 8.159,99~~[1]
	Site Oukeystore.com.br	~~R$ 8.799,99~~[1]
	Site Fouserv.com.br	~~R$ 16.999,00~~[1]
	Pregão 42/2017 UNILA	~~R$ 36.000,00~~[2]
	Pregão 54/2018 TJAC	~~R$ 65.000,00~~[1]
	Pregão 20/2018 IFEES	~~R$ 14.382,08~~
	Pregão 65/2018 UFPA	~~R$ 59.990,00~~[1]
	Pregão 25/2018 UNIFAP	R$ 19.750,00
	Pregão 7/2019 PF-PB	R$ 20.049,68[3]
Média		R$ 23.405,63
Quantidade		24
Total		**R$ 561.735,12**

1. Valores desconsiderados devido sua utilização gerar um coeficiente de variação maior que 25%.

2. Valor desconsiderado devido a licitação ser do ano de 2017.

3. Corresponde a divisão do valor de R$ 501.242,00 pela quantidade 25 do termo de homologação.

ITEM	FONTE DE PREÇO	VALOR
4 – Switch Tipo 4 – (SWITCH CORE)	Plugnet informática	R$ 150.000,00
	Lettel Distrib	R$ 114.747,50
	Fonmart	~~R$ 266.027,53~~[1]
	Pregão 47/2018 UFPI	R$ 165.760,00
	Pregão 2/2019 SENAC	R$ 112.413,94[2]
	Pregão 7/2019 PF-PB	R$ 174.040,00
Média		R$ 143.392,29
Quantidade		2
Total		**R$ 286.784,58**

1. Valores desconsiderados devido sua utilização gerar um coeficiente de variação maior que 25%.
2. Corresponde a divisão de R$ 224.827,88 pela quantidade 2 do termo de homologação.

ITEM	FONTE DE PREÇO	VALOR
5 – Switch Tipo 5 – (SWITCH CORE)	Lettel Distrib	R$ 114.747,50
	Fonmart	~~R$ 266.0270,53~~[1]
	Pregão 47/2018 UFPI	R$ 165.760,00
	Pregão 3/2018 IFMA	R$ 117.400,00
	Pregão 65/2018 UFPA	R$ 128.976,00
Média		R$ 131.720,88
Quantidade		2
Total		**R$ 263.441,76**

1. Valores desconsiderados devido sua utilização gerar um coeficiente de variação maior que 25%.

ITEM	FONTE DE PREÇO	VALOR
6 – Solução de gerenciamento de ativos de rede e análise de tráfego	Plugnet informática	R$ 180.000,00
	Lettel Distrib	R$ 78.000,00
	Fonmart	R$ 126.312,84
	Pregão 23/2018 Ministério da Agricultura	R$ 130.000,00

	Pregão 42/2017 UFLA	~~R$ 96.500,00~~[1]
Média		R$ 128.578,21
Quantidade		1
Total		**R$ 128.578,21**

1. Valor desconsiderado devido a licitação ser do ano de 2017.

ITEM	FONTE DE PREÇO	VALOR
6.1 – Treinamento básico de administração de switches hands-on	Plugnet informática	R$ 24.000,00
	Lettel Distrib	~~R$ 2.966,66~~[1]
	Fonmart	R$ 14.237,00
	Site trainnig.com.br	~~R$ 7.797,00~~[1]
	Site tecnoponta.com.br	~~R$ 2.576,00~~[1]
	Pregão 49/2018 Ministério da Defesa	R$ 25.995,00
	Pregão 346/2017 Infraero	~~R$ 23.314,00~~[2]
Média		R$ 21.410,67
Quantidade		3
Total		**R$ 64.232,01**

1. Valores desconsiderados devido sua utilização gerar um coeficiente de variação maior que 25%.

2. Valor desconsiderado devido a licitação ser do ano de 2017.

ITEM	FONTE DE PREÇO	VALOR
7 – Implantação e transferência de tecnologia da solução de gerenciamento de ativos de rede e análise de tráfego	Plugnet informática	R$ 70.000,00
	Lettel Distrib	R$ 89.000,00
	Fonmart	R$ 42.343,26
	Pregão 3/2018 INCRA	R$ 82.454,11
Média		R$ R$ 70.949,34
Quantidade		1
Total		**R$ 70.949,34**

ITEM	FONTE DE PREÇO	VALOR

8 – Solução de análise de perfil e controle de acesso	Plugnet informática	R$ 300.000,00
	Lettel Distrib	~~R$ 148.000,00~~[1]
	Fonmart	~~R$ 844.673,47~~[1]
	Pregão 34/2019 Senado	R$ 270.000,00
Média		R$ 285.000,00
Quantidade		1
Total		**R$ 285.000,00**

1. Valores desconsiderados devido sua utilização gerar um coeficiente de variação maior que 25%.

ITEM	FONTE DE PREÇO	VALOR
8.1 – Treinamento básico da solução de controle de acesso hands-on	Plugnet informática	R$ 18.000,00
	Lettel Distrib	~~R$ 2.966,66~~[1]
	Fonmart	R$ 14.237,00
	Site entelco.com.br	~~R$ 1.099,99~~[1]
	Pregão 34/2019 Senado Federal	R$ 10.277,78[2]
	Pregão 5/2018 TRE-MT	R$ 18.816,00[3]
Média		R$ 15.332,70
Quantidade		3
Total		**R$ 45.998,10**

1. Valores desconsiderados devido sua utilização gerar um coeficiente de variação maior que 25%.
2. O valor de R$ 61.666.66 (divisão de R$ 369.999.96 por 6 treinamentos no termo de homologação) para 6 pessoas resulta em R$ 10.277.78 como preço unitário.
3. O valor de R$ 75.264,00 para 4 pessoas resulta em R$ 18.816,00 como preço unitário.

ITEM	FONTE DE PREÇO	VALOR
9 – Modulo Gbic 10gb para até 300m	Plugnet informática	~~R$ 3.600,00~~[1]
	Lettel Distrib	R$ 1.185,00
	Fonmart	~~R$ 5.365,93~~[1]
	Site informatashop.com.br	~~R$ 3.006,00~~[1]
	Site netcomputadores.com.br	~~R$ 598,30~~[1]
	Site netcomputadores.com.br	~~R$ 932,28~~[1]
	Site aztech.com.br	~~R$ 411,12~~[1]

	Pregão 18/2018 TCE-MA	R$ 1.886,00
	Pregão 3/2018 INCRA	R$ 1.179,83
	Pregão 251/2017 UFSC	~~R$ 1.614,34~~[2]
	Pregão 22/2018 TJAM	R$ 1.915,00
Média		R$ 1.541,46
Quantidade		40
Total		**R$ 61.658,40**

1. Valores desconsiderados devido sua utilização gerar um coeficiente de variação maior que 25%.

2. Valor desconsiderado devido a licitação ser do ano de 2017.

ITEM	FONTE DE PREÇO	VALOR
10 – Modulo Gbic 10gb para até 10km	Plugnet informática	~~R$ 15.000,00~~[1]
	Lettel Distrib	R$ 3.160,00
	Fonmart	~~R$ 17.695,98~~[1]
	Site oukeystore.com.br	R$ 2.568,93
	Site netcomputadores.com.br	~~R$ 434,36~~[1]
	Site netcomputadores.com.br	~~R$ 704,27~~[1]
	Pregão 18/2018 TCE-MA	R$ 3.068,00
	Pregão 18/2018 Ministério de Infraestrutura	R$ 2.290,25
	Pregão 31/2018 MPU	R$ 1.842,40
Média		R$ 2.585,92
Quantidade		8
Total		**R$ 20.687,36**

1. Valores desconsiderados devido sua utilização gerar um coeficiente de variação maior que 25%.

ITEM	FONTE DE PREÇO	VALOR
	Plugnet informática	~~R$ 6.800,00~~[1]
	Lettel Distrib	R$ 4.345,00
	Fonmart	~~R$ 8.958,24~~[1]
	SmartWave Networks	R$ 3.591,00[3]
	Site oukeystore.com.br	~~R$ 2.399,99~~[1]

11 – Access point (ponto de acesso) wlan	Site oukeystore.com.br	R$ 3.499,99
	Site oukeystore.com.br	~~R$ 7.279,99~~[1]
	Site oukeystore.com.br	~~R$ 2.129,99~~[1]
	Site oukeystore.com.br	R$ 3.259,99
	Site Fouserv.com.br	~~R$ 1.719,00~~[1]
	Site Fouserv.com.br	~~R$ 2.899,00~~[1]
	Site Fouserv.com.br	~~R$ 1.699,00~~[1]
	Pregão 144/2017 Comando da Aeronáutica	~~R$ 2.369,41~~[2]
	Dispensa 681/2018 Comissão de Energia Nuclear	R$ 2.347,65
	Dispensa 21/2018 IFPR	~~R$ 1.750,00~~
Média		R$ 3.408,73
Quantidade		50
Total		**R$ 170.436,50**

1. Valores desconsiderados devido sua utilização gerar um coeficiente de variação maior que 25%.
2. Valor desconsiderado devido a licitação ser do ano de 2017.
3. O valor do fornecedor SmartWave resulta da soma dos 1 e 5 da sua proposta.

ITEM	FONTE DE PREÇO	VALOR
12 – Sistema de gerenciamento dos access points	Plugnet informática	R$ 40.000,00
	Lettel Distrib	R$ 48.490,00
	Fonmart	~~R$ 126.312,84~~[1]
	Pregão 47/2018 UTFPR	R$ 48.800,00
	Pregão 38/2017 IFECTAP	~~R$ 44.400,00~~[2]
	Pregão 34/2018 EBSERH	R$ 40.844,20
Média		R$ 44.533,55
Quantidade		1
Total		**R$ 44.533,55**

1. Valores desconsiderados devido sua utilização gerar um coeficiente de variação maior que 25%.
2. Valor desconsiderado devido a licitação ser do ano de 2017.

LOTE	ITEM	Qtde	Valor Médio	Total
	1. Switch Tipo 1 –	15	R$ 1.988,75	

	Mínimo 8 portas par trançado L2			
	2. Switch Tipo 2 – Mínimo 24 portas par trançado incluindo 2 portas 10Gb	7	R$ 16.600,10	**R$ 137.200,70**
	3. Switch Tipo 3 – Mínimo 48 portas par trançado incluindo 2 portas 10Gb	24	R$ 23.405,63	**R$ 561.735,12**
	4. Switch Tipo 4 – Mínimo 40 portas RJ45, incluindo 4 portas 10Gb, 2 portas 40 Gb, layer 3 (SWITCH CORE)	2	R$ 143.392,29	**R$ 286.784,58**
	5. Switch Tipo 5 – Mínimo 20 portas SFP+ 10Gb, 2 portas 40 Gb, layer 3 (SWITCH CORE)	2	R$ 131.720,88	**R$ 263.441,76**
01	6. Solução de gerenciamento de ativos de rede e análise de tráfego + Treinamento básico hands-on[1]	1	R$ 192.810,22	**R$ 192.810,22**
	7. Implantação e transferência de tecnologia da solução de gerenciamento de ativos de rede e análise de	1	R$ 70.949,34	**R$ 70.949,34**
	8. Solução de análise de perfil e controle de acesso + Treinamento básico hands-on[2]	1	R$ 330.998,10	**R$ 330.998,10**
	9. Modulo Gbic 10gb para até 300m	40	R$ 1.541,46	**R$ 61.658,40**
	10. Modulo Gbic 10gb para até 10km	8	R$ 2.585,92	**R$ 20.687,36**
02	1.Access point (ponto de acesso) wlan	50	R$ 3.408,73	**R$ 170.436,50**
	2. Sistema de gerenciamento dos access points	1	R$ 44.533,55	**R$ 44.533,55**
Total Geral				**R$ 2.171.066,88**

1. Corresponde a junção dos itens 6 e 6.1 com a soma de seus custos.

2. Corresponde a junção dos itens 8 e 8.1 com a soma de seus custos.

As quantidades previstas são as necessárias para a substituição de todos os equipamentos descontinuados instalados nos prédios sede e anexo deste Tribunal.

3 – ESCOLHA E JUSTIFICATIVA DA SOLUÇÃO

Para o atendimento da demanda especificada no Documento de O

4300/2019), opta-se pela aquisição e instalação dos itens que constam no item 2 – AVALIAÇÃO DA SOLUÇÃO, dada ser a solução mais adequada.

4 – NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE

Não há necessidade de adequação do ambiente.

II – SUSTENTAÇÃO DO CONTRATO

5 – DEFINIÇÃO DE RECURSOS HUMANOS E MATERIAIS

O atendimento deverá ser realizado por pessoal técnico especializado na instalação e configuração dos itens descritos no objeto da licitação. Todas as despesas necessárias para a prestação do serviço já devem estar incluídas no valor do contrato, tais como utilização de equipamentos, translado e estadia de técnicos da CONTRATADA.

6 – DEFINIÇÃO DAS ATIVIDADES DE TRANSIÇÃO E ENCERRAMENTO DO CONTRATO

Após o período de garantia deve ser realizado processo licitatório para renovação do suporte do software de backup e da assinatura dos agentes Linux.

7 – ELABORAÇÃO DE ESTRATÉGIA DE INDEPENDÊNCIA

Não se aplica.

III– ANÁLISE DE RISCOS

8 – IDENTIFICAÇÃO DOS RISCOS

1. *Fracasso da contratação.*
2. *A aquisição não atender as necessidades do TRE-MA.*
3. *Erro na especificação ou dimensionamento.*
4. *Seleção do fornecedor*
5. *Execução do objeto*

9 – IDENTIFICAÇÃO DAS PROBABILIDADES DE OCORRÊNCIA E DOS DANOS POTENCIAIS

1. Probabilidade média e dano alto
2. Probabilidade baixa e dano alto
3. Probabilidade baixa e dano alto
4. Probabilidade média e dano alto
5. Probabilidade baixa e dano alto

10 – DEFINIÇÃO DAS AÇÕES E RESPONSÁVEIS

1. Fracassar a contratação
    a. Ação: Comprometimento das unidades envolvidas para dar celeridade ao processo de contratação e se empenharem na obtenção do sucesso do processo. Responsável: Demandante.
    b. Revisão dos termos da contratação ou revisão da estratégia da contratação. Responsável: Demandante, técnico e administrativo.
2. Equipamentos não atenderem as necessidades do TRE-MA
    a. Ação: Definir requisitos que garantam a qualidade técnica da solução e homologá-las adequadamente. Responsável: Técnico.
3. Erro de especificação do produto
    a. Dimensionar os equipamentos contemplando as demandas considerando o funcionamento do TRE-MA com as perspectivas de longo e médio prazo. Contemplar soluções tecnológicas alinhadas com o mercado futuro. Responsável: Técnico.
4. Seleção do fornecedor
    a. Ação: Não especificar exigências que não possam ser atendidas por um conjunto de fornecedores. Responsável: Demandante, técnico e administrativo.
5. Execução do objeto
    a. Ação: Monitorar os prazos e notificar/informar a empresa em caso de descumprimento dos prazos e atendimento do edital da licitação. Responsável: Demandante e técnico.

IV– ESTRATÉGIA PARA A CONTRATAÇÃO

11 – NATUREZA DO OBJETO

Objeto de natureza comum, cujos padrões de desempenho e qualidade podem ser objetivamente definidos, por meio de especificações usuais de mercado.

12 - PARCELAMENTO DO OBJETO E FORMA DE ADJUDICAÇÃO

A contratação foi dividida em dois grupos, considerando a necessidade de perfeita integração/compatibilidade entre os itens de cada grupo, cujas funcionalidades são interdependentes (donde a inviabilidade de se contratar por itens separados). Com isso buscou-se também ampliar, na medida do possível à adequada execução do objeto, a competitividade no certame, que talvez restasse prejudicada se, por outro lado, a opção fosse por lote único.
Além disso, optamos por agrupar "fornecimento e instalação" em virtude de ser esta a prática de mercado e também em função do alto risco em se permitir que uma empresa forneça determinado item e outra o instale, criando assim problemas para a obtenção dos resultados esperados e obstáculos para a imputação de responsabilidades. Portanto, a forma de parcelamento escolhida busca tanto a adequada entrega e instalação dos itens – sem riscos para o conjunto da solução – e também a salvaguarda das respectivas garantias.

13 – MODALIDADE E O TIPO DE LICITAÇÃO

O objeto da contratação pretendida possui requisitos de desempenho e qualidade objetivamente definidos por meio de especificações usuais de mercado, razão por que se entende adequada a utilização da modalidade Pregão Eletrônico, tipo menor preço.

14 – CLASSIFICAÇÃO ORÇAMENTÁRIA

449039 - OUTROS SERVICOS DE TERCEIROS-PESSOA JURIDICA
449052 - EQUIPAMENTOS E MATERIAL PERMANENTE

15 – PRAZO DE GARANTIA

A garantia de atualização e suporte técnico será de no mínimo de 5 anos.

V – CONCLUSÃO DOS ESTUDOS PRELIMINARES

11 – DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

Declaramos a viabilidade da contratação com base nas informações levantadas neste documento.

Integrante Técnico	Integrante Demandante	Integrante Administrativo
_____ Sebastião da Silva Penha	_____ Lourencio Monteiro de Melo	_____ Marco Aurélio Martins Fernandes