PODER JUDICIÁRIO
TRIBUNAL REGIONAL FEDERAL DA 6ª REGIÃO

ESTUDO TÉCNICO PRELIMINAR - ETP COMPLETO 0329067

(para contratação de serviços e/ou aquisição de bens permanentes e de consumo por licitação)

Guia de suporte ao preenchimento do ETP: 15238786

ID (PAC):

Não se aplica, pois a contratação não foi incluída no PAC-23.

A. Descrição sucinta do objeto

Aquisição de *switches* do tipo Core e *software* de gerenciamento para atender às necessidades de funcionamento da rede de comunicação do Tribunal Regional Federal da 6ª Região.

B. Justificativa expressa para a contratação

A contratação é necessária para/porque *(expor a finalidade e os motivos da necessidade da contratação)*

O *Datacenter* que atende ao Tribunal Regional Federal da 6ª Região e suas Subseções Judiciárias foi reformado no ano de 2012 para atender às necessidades da Seção Judiciária de Minas Gerais. Assim, a atual infraestrutura de TI que atende ao TRF6 foi preparada para o funcionamento de uma Seccional, razão pela qual o recebimento de sistemas anteriormente centralizados no TRF1 como o PJe, o SEI, Acordo 58, SIREA, eSiest, bancos de dados, entre outros, representou um consumo de recursos não previstos quando das aquisições, conforme cenário de escassez reportado por meio dos autos 0000724-85.2022.4.06.8000.

Diante do crescimento dos sistemas do TRF6, alguns equipamentos já obsoletos e sem garantia contratual passaram a apresentar problemas relacionados ao aumento da carga, entre os quais a queda de desempenho, travamento e até danos físicos, como ocorreu com o Switch Core de tombo 46157. Por se tratar de equipamento de alta criticidade, o defeito do Core provocou a indisponibilidade total do PJe no período de 06 a 10/02/2023 e os serviços somente foram restabelecidos após o isolamento do equipamento, o que representou a perda da redundância e a sobrecarga correspondente do outro equipamento. Atualmente o equipamento se encontra com dois módulos danificados, o que representa a quebra da redundância

Destaca-se que um ativo de rede possui uma garantia de 05 anos e a recomendação de substituição após a vigência, nos termos da Resolução CJF nº 477/2018, em razão da obsolescência técnica ou funcional dos equipamentos. Por tal razão e considerando que os switches Core do *Datacenter* possuem mais de 10 anos de uso, além de não atenderem à demanda técnico-operacional, torna-se necessária a substituição urgente para adequação às necessidades de funcionamento do TRF6.

Há, ainda, um elemento essencial à infraestrutura: a disponibilidade. Todos os sistemas do TRF6 devem estar disponíveis para funcionamento em regime de 24 x 7 (vinte e quatro horas, sete dias por semana), o que pode acarretar em situações de falhas em horários sem acompanhamento por equipe especializada e, consequentemente, em atraso para o início do atendimento. Considerando que os sistemas e serviços de TI do TRF6 sustentam a área finalística da instituição, torna-se cada vez mais importante que estejam hospedados em ambiente de infraestrutura tecnológica que garanta a disponibilidade e integridade das informações.

Por tudo exposto, busca-se com a presente contratação:

a) Atualizar o parque tecnológico do TRF6;

b) Obter serviços de alta disponibilidade;

c) Aumentar a velocidade de operação entre os equipamentos;

d) Otimizar o desempenho da rede de dados;

e) Garantir a estabilidade operacional das comunicações do TRF6 e suas subseções judiciárias;

f) Permitir o crescimento futuro da rede de dados;

g) Incrementar os requisitos de segurança de operação.

A não contratação implicará *(expor as consequências advindas da não contratação)*

A não contratação poderá ensejar a parada dos sistemas de TI caso os equipamentos que integram a infraestrutura do *Datacenter* do TRF6 não suportem a demanda ou mesmo a piora da performance atual dos sistemas como o PJe e SEI.

C. Alinhamento da demanda com diretrizes e metas institucionais

- Resolução CNJ nº 370, de 28 de janeiro de 2021 - Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
- Resolução CJF nº 685, de 15 de dezembro de 2020 - Plano Estratégico de Tecnologia da Informação da Justiça Federal

Macrodesafio:

Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados

Objetivos Estratégicos da Justiça Federal:

1) Aperfeiçoar e assegurar a efetividade dos serviços de TI para a Justiça Federal

Indicadores	Metas
1 - Índice de satisfação dos clientes internos com os serviços de TI.	1 - Atingir, até 2025, 85% de satisfação dos clientes internos de TI.
2 - Índice de satisfação dos clientes externos com os serviços de TI.	2 - Atingir, até 2026, 80% de satisfação dos clientes externos de TI.

D. Proposta de solução

D.1. Alternativas de solução disponíveis no mercado

Solução nº	Descrição das alternativas de solução disponíveis no mercado	Fontes de consulta (órgãos públicos que adotaram a solução, fornecedores etc.)	Link das consultas (doc. SEI)
01	PREGÃO 265/2021 - Aquisição de aquisição de elementos ativos de rede de comunicação de dados, compostos por switches, sistema de segurança unificado, interfaces GBIC, pontos de acesso e equipamentos de telefonia VoIP, para integrar a infraestrutura de comunicação de dados das unidades do INPE.	INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS - INPE	0309686

02	PREGÃO 33/2022 - Aquisição de appliances de comutação de dados / switches e seus respectivos licenciamentos, servidores de configuração, equipamentos complementares de comunicação de dados, além do serviço de instalação, configuração, suporte técnico e garantia da fabricante de todos os itens adquiridos, para atender o PJMT.	TRIBUNAL DE JUSTIÇA DE MATO GROSSO - TJMT	0309691
03	PREGÃO 20220003 - Registro de preços para futuras e eventuais contratacões para Instalação, configuração e manutenção preventiva e corretiva com fornecimento de roteadores, switches, solucões para redes sem fio, acessórios, treinamentos e servicos especializados em redes, contemplando utilização de equipamentos obrigatoriamente todos novos e de primeiro uso.	EMPRESA DE TECNOLOGIA DA INFORMAÇÃO DO CEARÁ	0309696
04	PREGÃO 08/2022 - Contratação de solução de Firewall de próxima Geração para segurança da informação de perímetro que possibilite a visibilidade e controle de tráfego e aplicações em camada 7, prevenção contra ataques e ameaças avançadas e modernas, filtro de dados, VPN e controle granular de banda de rede, compreendendo fornecimento de equipamentos (appliances) e suas respectivas licenças de suporte e atualização.	CENTRO LOGÍSTICO DO MATERIAL DA MARINHA	0311141
05	PREGÃO 029/2022 - Aquisição de solução de visibilidade e detecção de ameaças do tráfego de rede, para reduzir o risco de cyber ataques e ampliar a visibilidade da Defensoria Pública do Estado do Pará.	DEFENSORIA PÚBLICA DO ESTADO DO PARÁ	0311169
06	PREGÃO 02/2023 - Contratação de empresa especializada para fornecimento, em lote único, de Solução contendo Switch de Acesso 24 e 48 portas, Controlador/gerenciador Wlan e Pontos de Acessos (AP), Solução de controle de acesso (NAC), incluindo o serviço de instalação e configuração da solução, software de erência, suporte e garantia por 5 anos e treinamento.	DEPARTAMENTO DE TRÂNSITO DO DISTRITO FEDERAL	0311179
07	PREGÃO 22/2022 - Contratação de expansão da infraestrutura de rede (cabeada e wireless) com garantia e suporte do fabricante, e renovação do suporte e garantia de equipamentos e softwares já existentes, para atender às dependências do Tribunal de Contas do Estado de Rondônia (Sede, Anexo III e Escola de Contas).	TRIBUNAL DE CONTAS DO ESTADO DE RONDÔNIA	0311184
08	PREGÃO 76/2022 - Aquisição de Switches, conforme condições, quantidades, exigências e estimativas estabelecidas.	COMPLEXO HOSPITALAR UNIVERSITÁRIO DA UNIVERSIDADE FEDERAL DO PARÁ	0311189
09	PREGÃO 17/2022 - Escolha da proposta mais vantajosa de uma solução unificada para a renovação da infraestrutura de ativos de rede LAN, Local Area Network, com ferramentas de gerenciamento centralizado e de controles de segurança, para os escritórios da ANCINE localizados no Rio de Janeiro/RJ e Brasília/DF, incluindo serviços de instalação, transferência de tecnologia prática (hands-on), garantia, suporte técnico e serviços continuados pelo prazo de 60 (sessenta) meses.	AGÊNCIA NACIONAL DO CINEMA - ANCINE	0311200
10	PREGÃO 13/2022 - Escolha da proposta mais vantajosa para a aquisição de soluções de rede para o Sistema de Inteligência do Exército (SIEx), conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.	CENTRO DE INTELIGÊNCIA DO EXÉRCITO - CIE	0311212

D.2. Estimativa de preços das alternativas de solução

Itens	**Quantidades**	**Estimativa de Preços das Soluções (R$)**										
		INPE	TJMT	Gov-CE	CL Marinha	DPE PA	DETRAN DF	TCE RO	UFPA	ANCINE	CIEX	
Switch Core Datacenter SFP	2	252.500,00	226.674,17	269.332,75		291.794,18						2
Switch Core UTP 48p PoE	4			32.039,58			30.692,14	59.464,25	130.000,00	88.185,88	60.990,00	6
Transceiver GBIC 10G	24	2.740,00		1.301,61	4.899,50	4.515,14			10.000,00			
Transceiver GBIC 25G	12	3.900,00				7.289,81						
Software de Gerência	1			75.092,78		35.939,36	22.447,65				43.100,00	6
Instalação e Configuração	1		46.500,74			217.886,93	123.760,00			92.000,00		1
Treinamento	1			13.016,08			27.341,52					2
TOTAL GERAL												

D.3. Razões da escolha da melhor solução (justificar técnica e economicamente o que o levou a escolher a solução)

As solução nºs 01 e 07 tratam de aquisições para substituições de equipamentos com vidas úteis expiradas, vinculados às r processo de renovação. Por se tratar de um processo gradual de substituição de equipamentos, tornou-se necessária a pré-definição do fab mantivesse a integração completa.

As soluções nºs 02, 03, 08, 09 e 10 detalham as aquisições completas de redes de comunicação dos respectivos órgãos. Trata permite a substituição completa dos equipamentos e que, consequentemente, demanda um maior tempo para implantação, além de um inv do número de bens envolvidos.

A solução nº 04 segue a mesma lógica de substituição gradual apresentada através da solução nº 01, porém o objeto é segurança da informação.

A solução nº 05 também representa um modelo de contratação da necessidade completa, porém com objeto voltado para a informação.

A solução nº 06 adota a proposta de uma aquisição completa de equipamentos de rede e inova ao apontar que "a marca est dos quatro quadrantes da Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure", proposta pela Gartner.

Os ativos das redes de dados do TRF6 e suas subseções judiciárias já ultrapassaram o período de vida útil previsto, razão pela devem ser substituídos como forma de garantir a estabilidade, segurança e controle das comunicações. Trata-se de um processo que der para a execução, pois a quantidade de equipamentos envolvidos se aproxima das 500 unidades. Assim, a substituição de toda a rede de cor em prazo que pode ser superior ao de funcionamento dos equipamentos.

Considerando-se que o TRF6 já se encontra com um switch Core com problema, pois o bem de tombo 46157 se enc danificados, e que um projeto de reestruturação da rede de dados deve incluir o acesso wi-fi corporativo, uma aquisição completa se m tempo e custos necessários. A situação é extremamente crítica até que seja realizada a troca dos equipamentos, uma vez que n comunicação e um eventual dano ao Core 2 pode provocar a indisponibilidade da rede de dados e a parada de todos os serviços e sistema bancos Oracle, Portal, entre outros.

Por tudo exposto, a melhor solução decorre da aquisição dos equipamentos necessários à substituição urgente dos swit garantir a confiabilidade das operações. A aquisição parcial permitirá a manutenção do funcionamento dos serviços e sistemas do disponibilidade da rede de comunicação, e o aumento de desempenho e controle dos ativos, em virtude da evolução tecnológica dos equipa

Destaca-se que a aquisição dos equipamentos deve prever a utilização em um posterior projeto de substituição dos equipame assim como o software de gerência. Assim, todos os equipamentos e softwares a serem adquiridos poderão ser integrados ao projeto final de comunicação.

D.4. Justificativas para o parcelamento ou não da solução

Justifica-se o não parcelamento do objeto, em razão da interdependência entre o fornecimento dos bens e os serviços que contratação, considerando-se a sua natureza específica e o caráter continuado de funcionamento dos bens.

O fracionamento da solução objeto poderia expor a risco a qualidade e a disponibilidade do ambiente tecnológico da JF6, já delimitar as responsabilidades, tarefas e ações caso haja mais de um fornecedor dentro do processo de execução dos serviços.

D.4.1. Aplicação de cotas a microempresas (ME) e empresas de pequeno porte (EPP)(somente para bens de natureza divisível)

Não se aplica, em virtude da impossibilidade de divisão da prestação de serviços.

E. Requisitos da solução escolhida

E.1. Requisitos qualitativos e quantitativos (e análise das contratações anteriores)

NECESSIDADES DE NEGÓCIO

1. ESPECIFICAÇÕES

1.1. Switch Core Datacenter SFP

1.1.1. Os switches tipo Leaf podem ser oferecidos em modelos fixos ou modulares;

1.1.2. Não deverá haver Stacking entre os switches, garantindo encaminhamento line -rate;

1.1.3. Deverá ser ofertado um modelo de switch específico para a rede de Datacenter, conforme classificação do fabricante, com características e capacidade de Software Defined Network;

1.1.4. Deverá permitir formar domínio de agregação de link virtual;

1.1.5. Possuir fonte de alimentação redundante interna AC bivolt, com seleção automática de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz);

1.1.6. As fontes deverão permitir a sua conexão a circuitos elétricos distintos possuindo alimentação independente;

1.1.7. Possuir ventiladores redundantes;

1.1.8. Deverá suportar OpenFlow ou similar;

1.1.9. Deverá possuir no mínimo 48 portas 1/10/25Gbps atendendo ao padrão Ethernet SFP+/SFP28 sem bloqueio (line-rate), totalmente licenciadas;

1.1.10. A mudança de velocidade das portas deverá ser feita de forma automática, de acordo com o transceiver instalado, e não por grupo de portas;

1.1.11. Implementar, em hardware, o protocolo VXLAN, conforme padronizado na RFC 7348, permitindo a criação e a extensão de segmentos de redes virtuais através da camada de redes;

1.1.12. Implementar funcionalidade Route Reflector para BGP;

1.1.13. Deverá implementar Equal -Cost Multi Path (ECMP) para os múltiplos links de conexão entre os switches;

1.1.14. Deverá possuir buffer de no mínimo 40MB;

1.1.15. Possuir no mínimo 32GB de memória RAM;

1.1.16. Possuir no mínimo 128GB para armazenamento (memória Flash ou SSD);

1.1.17. Deverá possuir capacidade de comutação de no mínimo 3,5 Tbps;

1.1.18. Latência máxima não superior a 1(um) microssegundos para comutação de pacotes de 64 bytes;

1.1.19. Deverá possuir capacidade mínima de encaminhamento de 1,2 (um virgula dois) bpps;

1.1.20. Possuir porta de gerenciamento Ethernet 10/100/1000BASE-T;

1.1.21. Possuir no mínimo 1 (uma) porta USB permitindo upgrade de firmware através dessa porta;

1.1.22. Deverá suportar MACSEC em line-rate para segurança link a link;

1.1.23. O switch deverá ser um equipamento homologado pela Agência Nacional de Telecomunicações (ANATEL);

1.1.24. Deverá oferecer suporte a FPGA ou EPLD para upgrade de software;

1.1.25. Deve implementar os protocolos de gerência de rede SNMPv2c e SNMPv3 gerando traps para servidor externo;

1.1.26. Deve possuir capacidade para pelo menos 500.000 endereços MAC;

1.1.27. Deve implementar pelo menos 3000 vlans;

1.1.28. Suportar Jumbo frames de no mínimo 9018 Bytes;

1.1.29. Deverá suportar, pelo menos, 1.000.000 (um milhão) de rotas IPV4 na tabela de roteamento;

1.1.30. Deverá suportar pelo menos 600.000 (seiscentas mil) rotas IPV6 na tabela de roteamento;

1.1.31. Deverá suportar,pelo menos 2.000 (duas mil) Listas de Controle de Acesso.

1.1.32. Deverá permitir autenticação para acesso local ou remoto ao equipamento usando base de usuários e permissões em um Servidor de Autenticação/Autorização do tipo TACACS e RADIUS.

1.1.33. Deve implementar protocolo de roteamento dinâmico OSPF conforme padronizado pelas RFCs 2328, 3101 ou 1587;

1.1.34. Deve implementar protocolo de roteamento BGPv4 conforme padronizado pelas RFCs 4271, 1997 e 2385;

1.1.35. Deve implementar o protocolo VRRP (Virtual Router Redundancy Protocol) ou similar;

1.1.36. Deve implementar Policy-Based Routing (PBR);

1.1.37. Suportar protocolo de roteamento dinâmico OSPFv3 para IPv6;

1.1.38. Deve implementar roteamento multicast PIM-SM e PIM-SSM para IPV4;

1.1.39. Deve implementar o protocolo IGMP nas versões v1 e v2;

1.1.40. Deve implementar o mecanismo IGMP Snooping nas versões v1 e v2;

1.1.41. Suporte aos mecanismos de QoS WRR ou WRED ou similar;

1.1.42. Deve implementar o protocolo de roteamento OSPF for IPv6;

1.1.43. Deve implementar o protocolo de roteamento BGP4 for IPv6;

1.1.44. Deve suportar mecanismo de Dual Stack para uso de IPv4 e IPv6;

1.1.45. Implementar protocolo BGP-EVPN conforme padronizado pela RFC 7432 ou atualizada;

1.1.46. Deve possuir planos de dados e de controle processados de forma separada;

1.1.47. Deve permitir configuração via Python, Ansible ou similar;

1.1.48. Os equipamentos ofertados devem ser compatíveis com uma futura expansão da rede em projeto de topologia segundo o modelo *spine and leaf*.

1.2. Switch Core UTP 48 portas PoE

1.2.1. Possuir, no mínimo, 48 portas Ethernet 10/100/1000 Base-T com autosensing de velocidade e com conectores RJ-45 para conexão de acesso;

1.2.2. Todas as 48 portas devem operar simultaneamente em conjunto com as 4 portas de uplink;

1.2.3. As portas de uplink devem suportar pelo menos 40 Gbps de banda;

1.2.4. Deve ser entregue com no mínimo 4 portas de uplink com velocidade de 1/10G SFP+;

1.2.5. As portas de uplink poderão ser fornecidas através de módulos;

1.2.6. Todas as portas Ethernet 10/100/1000 devem suportar configuração Half-Duplex (10/100) e Full-Duplex, com a opção de negociação automática;

1.2.7. As interfaces 10/100/1000 devem obedecer às normas técnicas IEEE802.3 (10BaseT), IEEE802.3u (100BaseTX), 802.3ab (1000BaseT) e IEEE802.3x (Flow Control);

1.2.8. Todas as portas Ethernet 10/100/1000 devem suportar autoconfiguração de crossover (Auto MDIX);

1.2.9. Deve implementar IEEE 802.3at PoE+ e IEEE 802.3af POE;

1.2.10. Possuir capacidade de associação das portas de acesso em grupo de, no mínimo, 8 (oito) portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad LACP;

1.2.11. Deve ser possível criar pelo menos 24 grupos LACP;

1.2.12. Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas;

1.2.13. Implementar VLANs por porta e VLANs compatíveis com o padrão IEEE 802.1q;

1.2.14. Implementar mecanismo de seleção de quais vlans serão permitidas através de trunk 802.1q.

1.2.14.1. Deve ser permitida a configuração da seleção de forma dinâmica;

1.2.15. Possuir porta de console para ligação direta de terminal RS-232 para acesso à interface de linha de comando. Poderá opcionalmente ser fornecida porta de console com interface USB;

1.2.16. Possuir porta Ethernet 10/100 Base-T dedicada para gerenciamento out-of-band;

1.2.17. Possuir porta USB compatível com flash drives para cópias de arquivos de configuração e arquivos de sistema operacional. Deve vir acompanhado de uma fonte de alimentação AC bivolt, automática de tensão (na faixa de 100 a 240 Volts) e frequência (de 50/60 Hz);

1.2.18. Suportar fonte de alimentação redundante interna AC bivolt, com seleção automática de tensão (na faixa de 100 a 240 Volts) e frequência (de 50/60 Hz);

1.2.18.1. As fontes deverão possuir alimentação independente, a fim de permitir a sua conexão a circuitos elétricos distintos;

1.2.18.2. Deve permitir troca da fonte redundante sem interrupção do funcionamento do switch;

1.2.18.3. Cada fonte deve possuir potência disponível para POE com, no mínimo, 740 (setecentos e quarenta) Watts de potência;

1.2.18.4. Em caso de o equipamento reiniciar, deve-se manter a potência POE+ durante o processo de reinício, tal característica é vital para reduzir indisponibilidade de dispositivos do departamento de engenharia de televisão como controladores de câmera, etc;

1.2.18.5. Deve possuir mecanismo capaz de energizar dispositivos PoE sem esperar o fim do carregamento do sistema operacional, permitindo uma alimentação mais rápida dos dispositivos conectados;

1.2.19. Possuir LEDs para a indicação do status das portas e atividade, além do modo duplex. Implementar os padrões

abertos de gerência de rede SNMPv1 (RFC 1157), SNMPv2 (RFC 1901 a 1907) e SNMPv3 (RFC 2273 a 2275);

1.2.20. Implementar pelo menos os seguintes níveis de segurança para SNMP versão 3:

1.2.20.1. Sem autenticação e sem privacidade (noAuthNoPriv);

1.2.20.2. Com autenticação e sem privacidade (authNoPriv);

1.2.20.3 Com autenticação e com privacidade (authPriv) utilizando algoritimo de criptografia AES 256-bit.

1.2.21. Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;

1.2.22. Possuir armazenamento interno das mensagens de log geradas pelo equipamento;

1.2.23. Possuir capacidade de exportar as mensangens de log geradas pelo equipamento para um servidor syslog externo;

1.2.24. Permitir o controle da geração de traps SNMP, possibilitando definir quais tipos de alarmes geram traps; Implementar nativamente pelo menos 2 grupos RMON (Alarms e Events);

1.2.25. Implementar os protocolos LLDP (IEEE 802.1AB) e LLDP-MED;

1.2.26. Suportar a coleta de informações de fluxos Layer 2, IPv4 e IPv6 através de IPFIX ou NetFlow;

1.2.27. Deve coletar informações referentes a 100% dos pacotes que trafegam no equipamento. Implementar Telnet e SSH para acesso à interface de linha de comando;

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

1.2.29. Ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface), SNMP, Telnet, SSH, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes;

1.2.30. Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP, e cópia segura e autenticada através de SCP (Secure Copy Protocol);

1.2.31. Suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES. Permitir que a sua configuração seja feita através de terminal assíncrono;

1.2.32. Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação. Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos;

1.2.33. Permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo switch e em outro switch do mesmo tipo conectado à mesma rede local;

1.2.34. Deve ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente;

1.2.35. Permitir o espelhamento do tráfego de portas que residem em um dado módulo para uma porta que reside em módulo diferente do switch;

1.2.35.1. Devem ser suportadas pelo menos duas sessões simultâneas de espelhamento;

1.2.35.2. O espelhamento não pode interferir no funcionamento normal do equipamento.

1.2.36. Deve ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;

1.2.37. Implementar funcionalidade de separação do tráfego de voz e dados em uma mesma porta de acesso (Voice VLAN), sem a necessidade de utilização de 802.1q;

1.2.38. Deve responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA);

1.2.39. Deve suportar no mínimo as seguintes operações de teste: ICMP echo, TCP connect (em qualquer porta TCP do intervalo 1-50000 que o administrador especifique), UDP echo (em qualquer porta UDP do intervalo 1-50000 que o administrador especifique);

1.2.40. O switch deve suportar pelo menos 5 (cinco) destas operações de testes simultaneamente:

1.2.40.1. Permitir a atualização de software sem perda de pacotes;

1.2.40.2. Suportar facilidades de programabilidade através de NETCONF/YANG;

1.2.40.3. Suportar scripts de configuração em Python;

1.2.40.4. Implementar o protocolo NTPv3 e NTP v4 (Network Time Protocol, versão 3 e versão 4).

1.2.40.5. Deve ser suportada autenticação entre os peers.

1.2.41. Implementar DHCP Client, DHCP Relay, DHCP Server em múltiplas VLANs;

1.2.42. Implementar roteamento estático;

1.2.43. Implementar o roteamento nível 3 entre VLANs;

1.2.44. Suportar o protocolo VRRP (RFC 2338) ou HSRP de redundância de gateway;

1.2.45. Possuir capacidade para pelo menos 32.000 endereços MAC na tabela de comutação;

1.2.46. Implementar, no mínimo, 1000 vlans simultaneamente;

1.2.47. Implementar, no mínimo, 4.000 entradas de roteamento IPv4;

1.2.48. Possuir capacidade de comutação de, no mínimo, 330 Gbps (Gigabits por segundo) incluindo as interfaces dedicadas para empilhamento;

1.2.49. Possuir uma taxa de encaminhamento de no mínimo 230 de Mpps (Milhões de pacotes por segundo) incluindo as interfaces dedicadas para empilhamento;

1.2.50. Suportar Jumbo frames de, no mínimo, 9198 Bytes;

1.2.51. Possuir porta dedicada de empilhamento com capacidade de 160 (cento e sessenta) Gbps (Gigabits por segundo) de banda agregada de empilhamento. Este valor deve ser adicional à capacidade de comutação do switch;

1.2.52. Deve ser fornecido um cabo de empilhamento por switch;

1.2.53. Suportar empilhamento através da porta dedicada, com capacidade de empilhamento de no mínimo 8 switches;

1.2.54. Suportar atualização automática de versão do sistema operacional dos switches que participam do empilhamento através da porta dedicada;

1.2.55. Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor

de Autenticação/Autorização do tipo TACACS+ e RADIUS;

1.2.56. Suportar filtragem de pacotes (ACL - Access Control List) para IPv4 e IPv6;

1.2.57. Proteger a interface de comando do equipamento através de senha;

1.2.58. Implementar o protocolo SSH V2 para acesso à interface de linha de comando;

1.2.59. Suportar a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet, SSH e SNMP;

1.2.60. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH;

1.2.61. Possibilitar o estabelecimento do número máximo de MACs que podem estar associados a uma dada porta do switch;

1.2.62. Deve ser possível bloquear o tráfego excedente e enviar um trap SNMP caso o número de endereços MAC configurados para a porta seja excedido;

1.2.63. Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino e flags TCP;

1.2.64. Permitir a associação de um endereço MAC específico a uma dada porta do switch, de modo que somente a estação que tenha tal endereço possa usar a referida porta para conexão. Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;

1.2.65. Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;

1.2.66. Permitir controlar e auditar quais comandos os usuários e grupos de usuários podem emitir em cada elementos de rede, independente do método de gerenciamento;

1.2.67. Possuir suporte a mecanismo de proteção da “Root Bridge” do algoritmo “Spanning-Tree” para defesa contra ataques do tipo “Denial of Service” no ambiente nível 2;

1.2.68. Possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta do switch esteja colocada no modo “Fast Forwarding” (conforme previsto no padrão IEEE 802.1w);

1.2.69. Possuir controle de broadcast, multicast e unicast por porta, podendo definir uma porcentagem limite de banda e pacotes por segundo;

1.2.70. Possuir análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC;

1.2.71 Possuir método de segurança que utilize uma tabela criada pelo mecanismo de análise do protocolo DHCP, para filtragem de tráfego IP que possua origem diferente do endereço IP atribuído pelo Servidor de DHCP, essa filtragem deve ser por porta. Implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN. Implementar padrão IEEE 802.1q (Vlan Frame Tagging). Implementar padrão IEEE 802.1p (Class of Service) para cada porta;

1.2.72. Implementar padrão IEEE 802.3ad. Implementar o protocolo de negociação Link Aggregation Control Protocol (LACP). Implementar padrão IEEE 802.1w (Rapid spanning Tree Protocol). Implementar padrão IEEE 802.1s (Multi-Instance Spanning-Tree);

1.2.73. Os processos de Autenticação, Autorização e Accounting associados a controle de acesso administrativo ao equipamento, TACACS+, devem ser completamente independentes dos processos AAA no contexto 802.1x, RADIUS;

1.2.74. Implementar controle de acesso por porta, usando o padrão IEEE 802.1x (Port Based Network Access Control). Devem ser atendidos, no mínimo, os seguintes requisitos:

1.2.74.1. Implementar funcionalidade que designe VLAN específica para o usuário, nos seguintes casos: A estação não tem cliente 802.1x (suplicante); As credenciais do usuário não estão corretas (falha de autenticação);

1.2.74.2. Implementar associação automática de VLAN da porta do switch através da qual o usuário requisitou acesso à rede (Assinalamento de Vlan);

1.2.74.3. Implementar associação automática de ACL da porta do switch através da qual o usuário requisitou acesso à rede (Downloadable ACL);

1.2.74.4. Implementar “accounting” das conexões IEEE 802.1x.

1.2.75. O switch (cliente AAA) deve ser capaz de enviar, ao servidor AAA, pelo menos as seguintes informações sobre a conexão:

1.2.75.1. Nome do usuário;

1.2.75.2. Switch em que o computador do usuário está conectado;

1.2.75.3. Porta do switch utilizada par acesso;

1.2.75.4. Endereço MAC da máquina utilizada pelo usuário;

1.2.75.5. Endereço IP do usuário;

1.2.75.6. Horários de início e término da conexão;

1.2.75.7. Bytes transmitidos e recebidos durante a conexão.

1.2.76. Deve ser possível definir, por porta, o intervalo de tempo para obrigar o cliente a se reautenticar (reautenticação periódica);

1.2.77. Deve ser possível forçar manualmente a reautenticação de um usuário conectado a uma porta do switch habilitada para 802.1x;

1.2.78. Suportar a autenticação 802.1x via endereço MAC em substituição à identificação de usuário, para equipamentos que não disponham de suplicantes;

1.2.79. Suportar a configuração de 802.1x utilizando autenticação via usuário e MAC simultaneamente na mesma porta do switch;

1.2.80. Deve suportar a autenticação 802.1x através do protocolo EAPOL;

1.2.81. Implementar o serviço de DHCP Server em múltiplas VLANS simultaneamente, para que possa atribuir endereços IP aos clientes 802.1x autenticados e autorizados;

1.2.82. Deve ser suportada a autenticação de múltiplos usuários em uma mesma porta;

1.2.83. Deve ter tratamento de autenticação 802.1x diferenciado entre “Voice Vlan” e “Data LAN”, na mesma porta para que um erro de autenticação em uma Vlan não interfira na outra;

1.2.84. Deve ser suportada a atribuição de autenticação através do navegador (Web Authentication) caso a máquina que

esteja utilizando para acesso à Rede não tenha cliente 802.1x operacional, o portal de autenticação local do switch deve utilizar protocolo seguro tal como HTTPS;

1.2.85. Deve implementar o mecanismo mudança de autorização dinamica, Radius “Change of Authorization”, conforme descrito na RFC 5176;

1.2.86. Deve implementar autenticação e encriptação MACSEc através dos algoritmo 128-bit Advanced Encryption Standard (AES) em todas as portas e velocidades obedecendo a norma técnica IEEE 802.1AE;

1.2.87. Implementar mecanismo de controle de multicast através de IGMP Snooping de IGMPv1 (RFC 1112), IGMPv2 (RFC 2236) e IGMPv3 (RFC 3376);

1.2.88. Implementar em todas as interfaces do switch o protocolo IGMP Snooping (v1, v2 e v3), não permitindo que o tráfego multicast seja tratado como broadcast no switch;

1.2.89. Suportar roteamento multicast PIM (Protocol Independent Multicast) nos modos “sparse- mode” (RFC 2362);

1.2.90. Implementar priorização de tráfego através do protocolo IEEE 802.1p;

1.2.91. Possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego “real-time” (voz e vídeo). Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino. Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nivel 2) e DSCP ("Differentiated Services Code Point"- nivel 3), conforme definições do IETF (Internet Engineering Task Force);

1.2.92. Suportar funcionalidades de QoS de “Traffic Shaping” e “Traffic Policing”;

1.2.93. Deve ser possível a especificação de banda por classe de serviço;

1.2.94. Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como:

1.2.94.1. Transmissão do pacote sem modificação;

1.2.94.2. Transmissão com remarcação do valor de DSCP;

1.2.94.3. Descarte do pacote.

1.2.95. Suportar mapeamento de prioridades nível 2, definidas pelo padrão IEEE 802.1p, em prioridades nível 3 (IETF DSCP – Differentiated Services Code Point definido pela Internet Engineering Task Force) e vice-versa;

1.2.96. Suporte aos mecanismos de QoS WRR (Weighted Round Robin) ou SRR (Shaped Round Robin);

1.2.97. Suporte aos mecanismos de QoS WRED (Weighted Random Early Detection) ou WTD (Weighted Tail Drop);

1.2.98. Implementar pelo menos oito filas de prioridade por porta de saída (egress port). Implementar IPv6;

1.2.99. Permitir a configuração de endereços IPv6 para gerenciamento;

1.2.100. Permitir consultas de DNS com resolução de nomes em endereços IPv6;

1.2.101. Implementar ICMPv6 com as seguintes funcionalidades:

1.2.101.1. ICMP request;

1.2.101.2. ICMP Reply;

1.2.101.3. ICMP Neighbor Discovery Protocol (NDP); ICMP MTU Discovery".

1.2.102. Implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH, TFTP, SNMP, SYSLOG, HTTP, HTTPS e DNS sobre IPv6;

1.2.103. Implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6;

1.2.104. Implementar roteamento estático para IPv6;

1.2.105. Suportar roteamento dinâmico RIPng para IPv6;

1.2.106. Suportar protocolo de roteamento dinâmico OSPFv3 para IPv6;

1.2.107. Os equipamentos ofertados devem ser compatíveis com uma futura expansão da rede em projeto de topologia segundo o modelo *spine and leaf*.

1.3. Transceiver GBIC 10GB SR

1.3.1. Atender ao padrão SFP+;

1.3.2. Atender o padrão 10 Gigabit Ethernet IEEE802.3ae, 850nm, MMF, até 400mt;

1.3.3. Deve possuir conector do tipo LC;

1.3.4. Deve atender ao padrão 1OGBASE-SR;

1.3.5. Deve ser compatível com os switches ofertados.

1.4. Transceiver GBIC 25GB SR

1.4.1. Atender ao padrão SFP28;

1.4.2. Atender o padrão 25 Gigabit Ethernet IEEE802.3by, 850nm, MMF, até 300m;

1.4.3. Deve possuir conector do tipo LC;

1.4.4. Deve atender ao padrão 25GBASE-SR;

1.4.5. Deve ser compatível com os switches ofertados.

1.5. Software de gerência

1.5.1. Deve gerenciar todos os dispositivos IPs do Datacenter do TRF6;

1.5.2. Deve permitir a integração da gerência da rede em uma única ferramenta de gerenciamento, de forma centralizada;

1.5.3. Deve possuir arquitetura cliente servidor, com interface WEB ou java podendo ser acessível através de browser WEB padrão;

1.5.4. Todas as licenças necessárias para o funcionamento da solução devem ser fornecidas;

1.5.5. Deve permitir que, no mínimo, 5 usuários administrativos acessem esta ferramenta de gerenciamento simultaneamente;

1.5.6. A ferramenta deve possibilitar a configuração de diferentes perfis de administradores. Deve ser possível ainda criar usuários com perfil de administração e outros de apenas visualização;

1.5.7. Deve permitir o gerenciamento de configurações, desempenho e falhas na rede;

1.5.8. Deve permitir sua instalação em pelo menos uma das plataformas abaixo:

1.5.8.1. Windows em versões 32 ou 64 bits;

1.5.8.2. Linux Debian 11 ou superiores nas plataformas 32 ou 64 bits;

1.5.8.3. Appliance virtual Hyper-V.

1.5.9. O software de gerenciamento deve suportar o protocolo SNMP de gerenciamento de versão 1, 2 e 3;

1.5.10. A solução de gerenciamento fornecida deve ser capaz de gerenciar ou monitorar equipamentos de outros fabricantes, pelo menos de forma básica;

1.5.11. Deve permitir o descobrimento de equipamentos presentes em uma ou mais sub-redes, a fim de garantir uma auditoria constante na infraestrutura de TI;

1.5.12. Deve permitir a criação de topologias/mapas da infraestrutura de rede através de protocolos de descobrimento;

1.5.13. O mapa deve permitir a identificação de problemas na infraestrutura de rede através de mudança de cores;

1.5.14. Permitir a visão agrupada da topologia conforme configuração do usuário;

1.5.15. O software deve permitir a criação, edição, remoção de VLANs nos dispositivos e associação das portas as mesmas;

1.5.16. Deve permitir a identificação do status das portas dos dispositivos up ou down, tecnologia e velocidade das portas;

1.5.17. Deve permitir a configuração de alarmes quando algum trap/evento ocorrer na rede;

1.5.18. A ferramenta deve permitir a configuração gráfica de um servidor SMTP externo para o envio de informações de gerenciamento da ferramenta;

1.5.19. Deve permitir envio de e-mail ou execução de um script ou programa integrado com a ferramenta para alertas;

1.5.20. A ferramenta deve permitir o gerenciamento dos dispositivos através de uma página WEB;

1.5.21. Permitir a localização de um dispositivo da rede baseado nos argumentos endereço IP, endereço MAC, username ou sub-rede;

1.5.22. A solução deverá prover recursos de "troubleshooting" capaz de mostrar por meio do RMON, dados presentes nos switches como performance ou estatísticas de utilização;

1.5.23. Deve permitir o gerenciamento das configurações de filas e priorização de tráfego dos dispositivos da rede;

1.5.24. A ferramenta deve permitir a configuração gráfica de rate limit nos equipamentos gerenciados;

1.5.25. A ferramenta deve permitir a configuração estática e dinâmica da funcionalidade MAC Locking ou Port Security, para executar o LOCK de MAC Address na rede;

1.5.26. A ferramenta deve permitir a configuração gráfica de vários métodos de autenticação, atendendo, no mínimo, a configuração da autenticação MAC ou autenticação IEEE 802.1X;

1.5.27. A ferramenta deve permitir o inventário detalhado de atributos dos dispositivos da rede, atendendo, no mínimo, números seriais, versão do sistema operacional e memória;

1.5.28. A ferramenta deve permitir o armazenamento das configurações dos dispositivos;

1.5.29. A ferramenta deve permitir o agendamento da função de armazenamento de configuração de determinados elementos da rede.

1.5.29.1. O agendamento deve ter periodicidade mínima de um dia;

1.5.30. A ferramenta deve permitir a comparação da configuração atual do dispositivo com a configuração armazenada na ferramenta;

1.5.31. Deve permitir o upgrade do sistema operacional ou Boot Prom dos dispositivos, unitariamente e para um grupo de dispositivos, inclusive podendo agendar um dia e horário para que este upgrade aconteça automaticamente;

1.5.32. A ferramenta deve permitir a execução de reboot dos dispositivos;

1.5.33. A ferramenta deve permitir restaurar a configuração armazenada. Deve ser possível ainda aplicar essa configuração em um equipamento em processo de substituição;

1.5.34. A ferramenta deve ser capaz de coletar e exibir informações de Sflow/Netflow recebidas de pelo menos 01 (um) equipamento de rede;

1.5.35. Relatórios: a solução de gerenciamento deve incluir:

1.5.35.1. Dashboards da rede cabeada, com capacidades de detalhamento;

1.5.35.2. Detalhes de identidade e informações de acesso;

1.5.35.3. Relatórios customizados para histórico e dados em tempo real;

1.5.35.4. Deve permitir integração com aplicações de terceiros;

1.5.35.5. Estatísticas de falhas reportadas pelos equipamentos de rede.

1.5.36. O software de gerência ofertado deve ser compatível com uma futura expansão da rede em projeto de topologia segundo o modelo *spine and leaf*.

1.6. Serviços de Instalação e Configuração dos Equipamentos e Migração das Operações

1.6.1. Os serviços de instalação física, configuração e documentação, deverão ser executados por equipe técnica da CONTRATADA.

1.6.2. O(s) profissional(is) técnico(s) da CONTRATADA responsável(is) pelos serviços descritos neste ITEM deve(m) possuir os certificados dos fabricantes das soluções respectivas.

1.6.3. A implantação deverá contemplar as seguintes fases:

1.6.3.1. Planejamento: nesta etapa a Contratada deverá realizar o planejamento do projeto, onde serão definidos os prazos por atividade, as pessoas, a estratégia de implantação do serviço, o plano de testes, a localização dos equipamentos na arquitetura da rede do orgão, bem como quaisquer outros itens que sejam necessários para a implantação do projeto. Devem-se considerar as janelas de manutenção do orgão, plano de rollback e o escopo

definido. Os responsáveis técnicos do orgão acompanharão e aprovarão o planejamento;

1.6.3.2. Documentação do projeto: Deverá ser entregue a documentação do projeto, conforme descrita a seguir, em formato e quantidade a serem acordados entre as partes e nos momentos especificados;

1.6.3.3. Plano de Requisitos de Infraestrutura: A CONTRATADA, antes de iniciar a execução das instalações deve levantar as necessidades de infraestrutura necessárias para instalação da configuração (espaço em rack, energização, refrigeração, tipo de conectorização, entre outros);

1.6.3.4. Plano de Implementação: A CONTRATADA, antes de iniciar a execução das configurações, deverá elaborar uma documentação técnica fundamentando todas as configurações que serão realizadas;

1.6.3.5. Plano de Migração: A CONTRATADA, antes de iniciar a execução das configurações, deverá analisar o ambiente do órgão para avaliar como será realizada a integração e a migração do ambiente atual de Produção.

1.6.4. Após a aprovação do planejamento deverá ser iniciado o processo de implantação, levando-se em consideração a disponibilidade das equipes envolvidas e cumprimento dos prazos pactuados:

1.6.4.1. Instalação física dos equipamentos (6 horas);

1.6.4.2. Configuração (3 horas);

1.6.4.3. Instalação em ambiente controlado (4 horas);

1.6.4.4. Etapa de testes e de funcionamento experimental (2 horas);

1.6.4.5. Migração (4 horas);

1.6.4.6. Validação do funcionamento em ambiente de produção (4 horas);

1.6.4.7. Documentação Final (48 horas).

1.7. Treinamento

1.7.1. Em até 15 dias corridos após a entrega da documentação da instalação (asbuilt), deverá ser ministrado o treinamento que será agendado baseado na disponibilidade da CONTRATANTE;

1.7.2. A transferência de conhecimento deverá ser ministrado pela contratada ou pelo fabricante;

1.7.3. A Contratada deverá fornecer todos os manuais dos equipamentos em formato digital em português brasileiro e/ou inglês;

1.7.4. A transferência de conhecimento deverá ter como ementa mínima:

1.7.4.1. Apresentação dos produtos fornecidos;

1.7.4.2. Visão geral da topologia e das tecnologias utilizadas;

1.7.4.3. Conceito, configuração, melhores práticas e diagnósticos de:

1.7.4.3.1. Gerência dos equipamentos;

1.7.4.3.2. Verificação da saúde da rede, configurações e inclusão de equipamentos de terceiros através da solução de gerência;

1.7.4.3.3. Futura integração a rede sem fio;

1.7.4.3.4. Roteamento;

1.7.4.3.5. Monitoramento utilizando telemetria;

1.7.4.3.6. QoS;

1.7.4.3.7. Voz e Vídeo na rede;

1.7.4.3.8. IPv6.

1.7.5. A transferência de conhecimento deve garantir que toda a informação gerada durante os processos de instalação/migração seja integral eformalmente apresentada à equipe da CONTRATADA, por meio de métodos expositivos, realização prática das atividades, apresentação de resumos, esquemas, relatórios ou qualquer outro documento que viabilize ou facilite a absorção da tecnologia do novo ambiente pela equipe da CONTRATADA;

1.7.6. É parte integrante do escopo de transferência do conhecimento a disponibilização de toda a documentação técnica, incluindo manuais de instalação, configuração e de usuário, relativa aos componentes integrantes da solução;

1.7.7. A transferência de conhecimento deverá ser realizada nas dependências da CONTRATADA em Belo Horizonte-MG ou por meio remoto, conforme a disponibilidade da CONTRATANTE, por técnicos com certificação(ões) técnica (s) emitida(s) pelo(s) fabricante(s) dos equipamentos;

1.7.8. A carga horária deverá ser de, no mínimo, 20 (vinte) horas, com duração máxima de 4 (quatro) horas por dia de segunda à sexta em horário comercial, e contar com até 6 (seis) participantes indicados pela CONTRATANTE;

1.7.9. A CONTRATADA assumirá todas as despesas e encargos inerentes à transferência de conhecimento, compreendendo as despesas com hospedagem, transporte e alimentação dos técnicos responsáveis pelo repasse e demais despesas/custos indiretos que incidirem sobre esta contratação;

1.7.10. Durante a transferência de conhecimento deverão ser fornecidos aos técnicos da CONTRATANTE todo material e documentação, preferencialmente em português, necessários à perfeita compreensão da solução instalada (slides, exemplos de implementação, documentação do projeto executado na CONTRATANTE, etc.) bem como alimentação compatível com a quantidade de pessoas envolvidas;

1.7.11. Ao término da transferência de conhecimento deverá ser realizada uma avaliação da atividade por parte da equipe da CONTRATANTE, que atribuirá as seguintes classificações:

1.7.11.1. A – Mais que Suficiente;

1.7.11.2. B – Suficiente; e

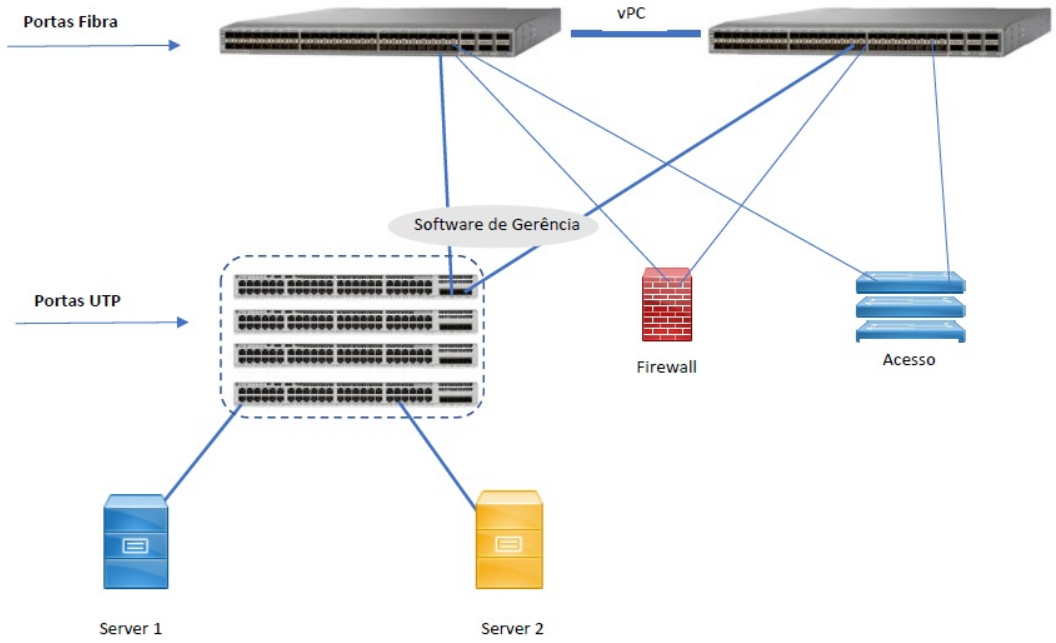
1.7.11.3. C – Insuficiente.

1.7.12. Caso 70% (cinquenta por cento) ou mais dos técnicos da CONTRATANTE avalie a transferência de conhecimento como insuficiente, a CONTRATADA deverá providenciar, sem ônus, outro período para a transferência de conhecimento;

1.7.13. Caso a CONTRATANTE considere a transferência de conhecimento suficiente ou mais que suficiente será gerado o termo de aceite da transferência de conhecimento em até 05 (cinco) dias.

2. TOPOLOGIA

2.1. A topologia de instalação seguirá ao desenho abaixo:



3. GARANTIA

3.1. Deve adquirir a garantia do fabricante, por um período mínimo de 05 (cinco) anos, considerando a reposição de peças danificadas, mão-de-obra de assistência técnica e suporte, com atendimento *on-site* e abertura de chamado em regime 24x7 (vinte e quatro horas por dia, sete dias por semana);

3.2. Deverá ser apresentado SKU ou número de série da garantia ofertada junto a proposta de preços;

3.3. Os serviços de reparo dos equipamentos especificados serão executados, quando necessário, onde se encontram instalados os equipamentos (ON-SITE), em horário comercial;

3.4. O prazo máximo para atendimento do chamado no local deve ser de até 4 horas após a sua abertura;

3.5. Comprovar junto a proposta final o tempo de atendimento no local, indicando a cidade do CONTRATANTE, por meio de documento ou relatório de ferramenta oficial do fabricante, ou ainda, através de declaração emitida pelo fabricante ou distribuidor autorizado.

3.6. A CONTRATADA e o Fabricante devem possuir Central de Atendimento tipo (0800) para abertura dos chamados de garantia;

3.7. O fabricante também deve oferecer canais de comunicação e ferramentas adicionais de suporte online como “chat”, “email” e página de suporte técnico na Internet com disponibilidade de atualizações e “hotfixes” de drivers, BIOS, firmware, sistemas operacionais e ferramentas de troubleshooting, no mínimo;

3.8. Durante o prazo de garantia será substituída sem ônus para o CONTRATANTE, a parte ou peça defeituosa, após a conclusão do respectivo analista de atendimento de que há a necessidade de substituir uma peça ou recolocá-la no sistema, salvo-se quando o defeito for provocado por uso inadequado;

3.9. Esta modalidade de cobertura de garantia deverá, obrigatoriamente, entrar em vigor a partir da data de recebimento definitivo dos equipamentos e serviços pelo órgão;

3.10. Possuir recurso disponibilizado via web, site do próprio fabricante (informar url para comprovação), que permita verificar os componentes entregues de fábrica e a garantia do equipamento, através da simples inserção do seu número de série do equipamento, sem necessidade de senhas de acesso;

3.11. Os equipamentos entregues serão verificados e devem constar as peças e softwares ofertados na proposta, para o devido aceite, a fim de garantir que todos os itens são integrados em fábrica e cobertos pela garantia do fabricante;

3.12. A substituição de componentes ou peças decorrentes da garantia não deve gerar quaisquer ônus para o CONTRATANTE. Toda e qualquer peça ou componente consertado ou substituído, fica automaticamente garantido até o final do prazo de garantia do objeto.

4. PRAZO DE ENTREGA

4.1. O prazo para entrega dos equipamentos e serviços será de no máximo 120 (cento e vinte) dias corridos, contados a partir do 1º (primeiro) dia útil subsequente ao recebimento da Ordem de Fornecimento.

4.1.1. A entrega deverá ser efetuada em horário de expediente normal deste Tribunal, mediante agendamento prévio através pelo telefone 31 - 3501-1201 ou e-mail suinf@trf6.jus.br, na Subsecretaria de Infraestrutura – SUINF, situada na Av. Álvares Cabral, nº 1.805, 5º andar, Bairro Santo Agostinho, Belo Horizonte/MG, no período das 09h às 18h, com a apresentação da correspondente nota fiscal, no prazo estipulado e nas quantidades indicadas nas notas de empenho.

4.1.2. Serão permitidas entregas e instalações parciais, sem prejuízo ao cronograma de entrega. O Termo de Recebimento Definitivo será emitido apenas após a efetiva entrega da solução com base nos quantitativos, métricas e características estabelecidos no Termo de Referência.

E.2. Critérios de sustentabilidade

Os itens pretendidos são sustentáveis? Indicar a resposta expressamente para cada item (SIM ou NÃO).
*Em caso de resposta **afirmativa** para um ou mais itens: indicar os critérios de sustentabilidade adotados para cada item.*
*Em caso de resposta **negativa** para um ou mais itens: justificar o afastamento dos critérios de sustentabilidade para cada item.*

A Contratada deverá adotar práticas de sustentabilidade ambiental na execução do objeto, quando couber, conforme disposto na Resolução CNJ 400/2021.

E.3. Critérios de acessibilidade

Não se aplica.

E.4. Demonstração de que o mercado atende aos requisitos mínimos

Requisito	ID da Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada outro órgão ou entidade Administração Pública Federal?	Solução 1	X		
	Solução 2			
	Solução 3			
	Solução 4			
	Solução 5			
	Solução 6			
	Solução 7			
	Solução 8			
	Solução 9			
	Solução 10			
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1		X	
	Solução 2			
	Solução 3			
	Solução 4			
	Solução 5			
	Solução 6			
	Solução 7			
	Solução 8			
	Solução 9			
	Solução 10			
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1		X	
	Solução 2			
	Solução 3			
	Solução 4			
	Solução 5			
	Solução 6			
	Solução 7			
	Solução 8			
	Solução 9			
	Solução 10			
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			
	Solução 3			
	Solução 4			
	Solução 5			
	Solução 6			
	Solução 7			
	Solução 8			
	Solução 9			
	Solução 10			
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			
	Solução 3			
	Solução 4			
	Solução 5			
	Solução 6			
	Solução 7			
	Solução 8			
	Solução 9			
	Solução 10			
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			
	Solução 3			
	Solução 4			
	Solução 5			
	Solução 6			
	Solução 7			
	Solução 8			
	Solução 9			
	Solução 10			

F. Descrição da solução como um todo

F.1. Resultados pretendidos com a solução escolhida

Atualizar o parque tecnológico do TRF6;

Obter serviços de alta disponibilidade;

Aumentar a velocidade de operação entre os equipamentos;

Otimizar o desempenho da rede de dados;

Garantir a estabilidade operacional das comunicações do TRF6 e suas subseções judiciárias;

Permitir o crescimento futuro da rede de dados;

Incrementar os requisitos de segurança de operação.

F.2. Contratações correlatas e/ou interdependentes

Não se aplica.

F.3. Adequações do ambiente do órgão impostas pela solução escolhida

Não se aplica.

F.4. Descrição integral da solução

Aquisição de *switches* do tipo Core, incluindo as GBICs para conexões óticas, e *software* de gerenciamento, além dos serviços de instalação e configuração dos equipamentos e treinamento para operação, para atender às necessidades de funcionamento da rede de comunicação do Tribunal Regional Federal da 6ª Região.

G. Declaração de viabilidade

Com base nas informações levantadas ao longo deste estudo técnico, declaramos que a solução apresentada é viável de prosseguir e ser concretizada, pois é a que melhor atende os requisitos técnicos e funcionais pretendidos pela área demandante.

H. Nome e assinatura dos responsáveis pela elaboração e pela revisão, supervisão e controle de qualidade do ETP

Responsável pela elaboração: *(servidor da unidade requisitante)*
Heli Lopes Rios - Diretor da SUINF
Responsável pela revisão, supervisão e controle de qualidade: *(diretor)*
Daniel Santos Rodrigues - Diretor da SECTI
Integrante Administrativo:
Bruno Vieira de Souza - Analista Judiciário

Documento assinado eletronicamente por **Heli Lopes Rios**, **Diretor(a) de Subsecretaria**, em 01/06/2023, às 19:33, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Daniel Santos Rodrigues**, **Diretor(a) de Secretaria**, em 01/06/2023, às 19:33, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.trf6.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0329067** e o código CRC **C59CF478**.