# Estudo Técnico Preliminar 94/2021

## 1. Informações Básicas

Número do processo: 00094.000498/2020-61

## 2. INTRODUÇÃO

### Histórico de Revisões

| data | Versão | Descrição | Autor |
|---|---|---|---|
| 27/10/2020 | 1.0 | Finalização da primeira versão do documento | Robson Martins Guimarães da Silva |
| 05/05/2021 | 2.0 | Finalização da segunda versão do documento | Robson Martins Guimarães da Silva |
| 13/10/2021 | 3.0 | Finalização da terceira versão do documento | Marcelo Ferreira Pinheiro |
| 08/11/2021 | 4.0 | Finalização da quarta versão do documento | Marcelo Ferreira Pinheiro |

| 1 - INTROCUÇÃO |
|---|
| O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.<br><br>**Referência: Art. 11 da IN SGD/ME nº 1/2019.** |

## 3. Descrição da necessidade

| DAS NECESSIDADES |
|---|

| DEFINIÇÃO E IDENTIFICAÇÃO DAS NECESSIDADES |
|---|

| OBJETO |
|---|
| **Diante do exposto, este instrumento trata do processo de aquisição de 02 (dois) roteadores BGP (Border Gateway Protocol) com garantia de 60 (sessenta) meses, incluindo licenças perpétuas, suporte técnico por 12 (doze) meses,** |

**instalação e configuração dos equipamentos de modo que a Presidência da República do Brasil opere como Sistema Autônomo (AS), bem como a aquisição de solução/ferramenta de análise de tráfego e roteamento BGP para os objetos citados, com garantia de 60 (sessenta) meses, licenças perpétuas, suporte técnico por 12 (doze) meses, instalação, configuração, além de treinamentos especializados para ambas as soluções.**

**A segunda solução refere-se à implementação de um software/ferramenta de coleta e análise de tráfego para protocolo BGP, devendo essa ser baseada nas melhores tecnologias ou protocolos de medição de fluxo de tráfego e gerenciamento de ativos conectividade, como por exemplo, *Network Flows* (ex. NetFlow, sFlow, IPFIX, etc) e SNMP (*Simple Network Management Protocol*). A futura solução deverá contemplar também funções que possibilitem o monitoramento do consumo, desempenho e segurança dos links e demais ativos que suportam toda a infraestrutura de rede WAN (roteadores BGP) da Presidência da República.**

**A aquisição de uma solução destinada ao gerenciamento, coleta e análise de tráfego de rede BGP, se fez necessária desde o momento que a Presidência da República decidiu se tornar e operacionalizar seu Sistema Autônomo - AS, isso porque, quando uma instituição ou empresa se torna um AS, esta passa a ter, além dos diversos benefícios inerentes dessa condição, tais como, uma infraestrutura de rede mais robusta, o poder de contar com mais de um fornecedor de trânsito para garantia de redundância em caso de indisponibilidade ou intermitência de seus links, flexibilização na implementação de políticas de tráfego de dados, traz o ônus, que, na maioria das vezes, apresentasse como o maior desafio para os gestores.**

**A gestão de um Sistema Autônomo pode se tornar uma tarefa hercúlea, caso os gestores não possam contar com uma solução que permita a execução eficiente e ágil de processos para coleta e análises de dados, que servirão de insumos para a execução de ações de gerenciamento de incidentes e problemas, tanto proativos quanto reativos, bem como para a tomada de decisões, auxiliando os processos de futuras aquisições e implementações de medidas e mecanismos de segurança da informação.**

**Com relação as questões de segurança da informação, para ilustrar e facilitar o dimensionamento do impacto no caso da ocorrência de algum sinistro dessa natureza, tomemos como exemplo algumas notícias circulantes, no caso específico, com relação a ataques DDoS tem afetado o panorama nacional, considere os dados que são divulgados pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, tais como: - Segundo o relatório da NSFOCUS "2020 *Mid-Year DDoS Attack Landscape Report*", em 2020 o Brasil foi o 4º país que mais sofreu com ataques DDoS, ficando atrás somente de Japão, China e Estados Unidos. Já em 2021, de acordo com a Kaspersky, somente em abril, o Brasil foi alvo de mais de 60% dos ataques identificados pela companhia na América Latina.**

**Diante do exposto, a aquisição da solução/ferramenta busca apresentar dados analíticos que possam auxiliar na implementação de processos e métodos que possibilitem melhoras significativas nos processos de identificação, controle de segurança, mitigação de ocorrências de sinistros, diminuição de custos operacionais, além do planejamento de ações que visam o tratamento das seguintes questões:**

- **Segurança do roteamento BGP;**
- **Segurança do plano de controle da rede;**
- **Segurança contra ataques de negação de serviços;**
- **instabilidades do BGP;**
- **Engenharia de tráfego;**
- **Planejamento de capacidades;**
- **Reputação e conformidade.**

# 4. Área requisitante

| Área Requisitante | Responsável |
|---|---|
| Coordenação Geral de infraestrutura Tecnológica e Telecomunicações substituto | Adriano Franco Bezerra |

# 5. Descrição dos Requisitos da Contratação

**DEFINIÇÃO E ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO**

O objeto de estudo é a aquisição de 02 (dois) roteadores BGP (Border Gateway Protocol) com garantia de 60 (sessenta) meses, incluindo licenças perpétuas, suporte técnico por 12 (doze) meses, instalação e configuração dos equipamentos de modo que a Presidência da República do Brasil opere como Sistema Autônomo (AS), bem como a aquisição de solução/ferramenta de análise de tráfego e roteamento BGP para os objetos citados, com garantia de 60 (sessenta) meses, licenças perpétuas, suporte técnico por 12 (doze) meses, instalação, configuração, além de treinamentos especializados para ambas as soluções.

- **O contrato será executado conforme discriminado abaixo:**
- Os requisitos de negócio estão especificados no âmbito deste E.T.P.
- Requisitos de capacitação são aplicáveis quanto ao objeto em comento, conforme disposto neste E.T.P.
- Os requisitos legais estão compreendidos na Lei nº 10.520/2002 e no regulamento do pregão eletrônico (Decreto nº 10.024/2019), conjugados com as regras da Lei nº 8.666/93, de aplicação subsidiária, bem como no disposto no art. 5º do Decreto nº 7.174/2010 e no art. 25 da IN. SGD/ME nº 1/2019.
- Os requisitos temporais estão especificados no âmbito do item 1.12 deste E.T.P.
- Requisito Temporal 1 - Os equipamentos e a solução de análise BGP deverão ser entregues e instalados em até 120 (cento e vinte) dias a partir da data de assinatura do Contrato.
- Os requisitos de segurança são os requisitos específicos praticados pela Presidência da República, quanto ao acesso e a permanência de terceirizados nas dependências.
- Os requisitos sociais, ambientais e culturais deve estar aderente à Lei nº 12.305/ 2010 que Institui a Política Nacional de Resíduos Sólidos.
- Os requisitos de arquitetura tecnológica se encontram especificados no âmbito deste E.T.P.
- Os requisitos de projeto e implementação se acham contemplados no âmbito deste E.T.P.
- Os requisitos de implantação estão especificados no âmbito deste E.T.P.
- Em relação aos requisitos de garantia (a contratada deverá fornecer garantia para os itens ofertados), esta será de 60 (sessenta) meses, a partir do recebimento definitivo do objeto contratado.
- Os requisitos de experiência profissional da equipe não são aplicáveis quanto ao objeto em comento.
- Os requisitos de formação da equipe não são aplicáveis quanto ao objeto em comento.
- Os requisitos de metodologia de trabalho não são aplicáveis quanto ao objeto em comento.
- Os requisitos de segurança da informação estão especificados no âmbito deste ETP.
- Em relação aos requisitos de segurança da informação, a Contratada deverá garantir a segurança, bem como não divulgar ou fornecer a terceiros quaisquer dados e informações desta Presidência da República a que tiver acesso no curso da prestação dos serviços, a menos que autorizado formalmente e por escrito para tal.
- A contratada deverá celebrar o Termo de Confidencialidade da Informação e o Termo de Ciência, respectivamente, constantes do Termo de Referência.

**DESCRIÇÃO DO OBJETO – GRUPO 1**

**REQUISITOS DA AQUISIÇÃO**

A aquisição em comento pretende atender as seguintes características técnicas mínimas necessárias:

**INSTALAÇÃO**

O equipamento deverá ser montável em rack de 19’’, tendo sua altura máxima de 4RUs, devendo este vir acompanhado dos devidos acessórios necessários para sua instalação.

**FONTE DE ALIMENTAÇÃO**

O equipamento deve operar nas tensões entre 100 e 240 VCA / 60 Hz, selecionáveis automaticamente;

O equipamento deve possuir, no mínimo, 2 (duas) fontes de alimentação, operando na configuração N+1, ou seja, em caso de falha de uma das fontes o roteador deve permanecer suportando sua capacidade máxima;

A troca de fontes de alimentação deve ser hot-swappable;

Implementar de forma nativa mecanismo de monitoramento e detecção de falhas em suas fontes de alimentação individuais;

A fonte de energia deve vir acompanhada com cabo de energia com 1,80 metros de comprimento mínimo e tomada padrão NBR 14136;

O plugue do cabo de alimentação deverá seguir o padrão brasileiro, conforme estabelece a norma NBR 14136, ou, alternativamente, deverá ser fornecido adaptador para esse padrão.

**REFRIGERAÇÃO**

O Subsistema de ventilação deve ser redundante, operando na configuração N+1, ou seja, em caso de falha de um dos ventiladores o roteador deve permanecer suportando sua capacidade máxima;

O equipamento deve implementar de forma nativa mecanismo que viabilize detecção de falhas nos principais componentes do subsistema de ventilação;

O equipamento deve implementar de forma nativa mecanismos dos principais componentes do subsistema de ventilação bem como de seus parâmetros de funcionamento;

Deve ser capaz de adaptação automática da velocidade de rotação em função da temperatura do equipamento.

**CPU E MEMÓRIA**

Deverá possuir configuração de CPU e quantidade necessária de memória DRAM ou SDRAM e memória auxiliar que atenda, simultaneamente, a todas as funcionalidades exigidas nesta especificação, em conformidade com as recomendações do fabricante;

Deverá suportar o armazenamento de múltiplas imagens de *software* e configuração (mínimo de 2 imagens e 2 configurações);

Deverá permitir selecionar a imagem de *software* que será utilizada na próxima inicialização;

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;

Deverá permitir selecionar a configuração que será utilizada na próxima inicialização;

Os planos de encaminhamento (forwarding plane) e controle (control plane) devem ser completamente independentes;

**CONDIÇÕES DO AMBIENTE**

Deve operar em temperatura ambiente entre 10 e 40°C;

Deve ser destinado ao uso normal em ambiente tropical com umidade relativa na faixa de 20% a 80% (sem condensação), permitindo, por um curto período, funcionamento com umidade relativa de 5% a 85%.

Deve suportar temperatura ambiente de armazenamento entre 0 e 50°C.

**FERRAMENTAS DE ATUALIZAÇÃO E TRANSFERÊNCIA DE ARQUIVOS**

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

Deve ter a capacidade de atualização de *software* via FTP e via TFTP, em conformidade com a RFC 783 ou RFC 1350;

Deve permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (*Secure Copy*) ou SFTP ( *Secure FTP*).

**FERRAMENTAS DE CONFIGURAÇÃO**

Implementar Telnet e SSH para acesso à interface de linha de comando;

Ser configurável e gerenciável via CLI (*Command Line Interface*), SNMP, Telnet, SSH, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes;

Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP;

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;

Deve permitir a criação de versões de configuração e suporte a "*rollback*" da configuração para versões anteriores.

**FERRAMENTAS DE COLETA DE FLUXO**

Suportar protocolo de coleta de informações de fluxos que circulam pelo equipamento contemplando no mínimo as seguintes informações:

IP de origem/destino;

Parâmetro "*protocol type*" do cabeçalho IP;

Marcação de QoS, portas TCP/UDP de origem/destino; e

Interface de entrada do tráfego;

Deve ser possível especificar o uso de tal funcionalidade somente para tráfego de entrada, somente para tráfego de saída e também para ambos os sentidos simultaneamente, em cada uma das interfaces do equipamento;

A informação coletada deve ser automaticamente exportável em intervalos pré-definidos através de um protocolo IPFIX (NetFlow v9 ou SFlow ou JFlow ou HFlow) padronizado;

Deve ser possível definir uma taxa de amostragem para coleta de fluxos, sendo possível uma taxa configurável de 1:1 até 1: 10000 fluxos.

Deve suportar BGP *Flowspec*.

**CAMADA DE ENLACE**

Implementar VLANs por porta;

Implementar VLANs compatíveis com o padrão IEEE 802.1q;

Implementar mecanismo de seleção de quais VLANs serão permitidas através de trunk 802.1q:

Deve ser permitida a configuração dessa seleção de forma dinâmica;

Implementar, no mínimo, 128 VLANs simultaneamente;

Deverá implementar *link agreggation* padrão IEEE 802.3ad com suporte a LACP padrão IEEE 802.1ax, para interfaces 1Gbps e 10 Gbps;

Deverá implementar a funcionalidade de auto negociação de taxa de transmissão (10/100/1000) e de modo de transmissão (*half /full-duplex*) e Auto-MDIX (*Automatic Media Dependent Interface Crossover*) para portas Gigabit Ethernet.

Deverá suportar protocolos de controle de *loop*, tais como:

Padrão IEEE 802.1d (STP – *Spanning Tree*).

Padrão IEEE 802.1w (RSTP – *Rapid Spanning Tree*).

Padrão IEEE 802.1s (MSTP – *Multiple Spanning Tree*).

**CAMADA DE REDE**

Deve permitir o roteamento nível 3 entre as VLANs;

Deverá suportar jumbo *frames* (até 9012 *bytes*);

Deverá implementar a autonegociação;

Deve suportar a pilha de protocolos TCP/IP;

Deve suportar o protocolo roteável IPv4;

Deve suportar o protocolo roteável IPv6;

Deve implementar mecanismo de pilha dupla (IPv4 e IPv6), para permitir o funcionamento simultâneo dos protocolos IPv4 e IPv6;

Deve permitir a configuração de rotas estáticas para IPv4 e IPv6;

Deve suportar o protocolo BFD (*Bidirectional Forwarding Detection*);

Deverá implementar o protocolo de roteamento OSPF com, no mínimo, as seguintes características:

RFC 3101 - OSPF *Not-So-Stubby Area* (NSSA) *Option*;

RFC 3137 - OSPF *Stub Router Advertisement*.

RFC 2740 ou 5340 - OSPF for IPv6;

RFC 3623 - *Graceful* OSPF *Restart*;

RFC 5187 - OSPFv3 *Graceful Restart.*

Deverá implementar Capacidade de pelo menos 3 áreas OSPFv2;

Deverá implementar autenticação MD5 de sessões OSPFv2 e OSPFv3.

Deverá implementar o protocolo de roteamento BGP versão 4 com, no mínimo, as seguintes características:

RFC 3065 - Autonomous System Confederation for BGP;

RFC 2796 - BGP *Route Reflection - An Alternative to Full Mesh* IBGP;

RFC 1997 - BGP *Communities Attribute*;

RFC 2385 - *Protection of BGP Sessions via the* TCP MD5 *Signature Option*;

RFC 2439 - *BGP Route Flap Damping*;

RFC 3392 - Capabilities Advertisement with BGP-4;

RFC 4760 - Multi-Protocol Extensions for BGP-4;

RFC 2918 – *Route Refresh Capability for BGP-4*;

RFC 3065 - *Autonomous System Confederations for* BGP;

RFC 4271 - *A Border Gateway Protocol* 4 (BGP-4);

RFC 4456 - *BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP).*

*RFC 4724 – BGP Gracefull Restart*

*RFC 4360 - BGP BGP Extended Communities Attribute*

Implementar protocolo de roteamento Multiprotocol BGP com suporte a IPv6 ou BGP4+;

Deverá implementar autenticação MD5 entre os peers BGP;

Permitir limitar a quantidade de rotas recebidas por peer BGP;

Implementar o protocolo BFD para BGP, através de interfaces físicas e lógicas (inclusive túneis GRE);

Implementar roteamento baseado em políticas (Policy Based Routing) com suporte a IPv4 e IPv6, permitindo a definição de políticas de roteamento baseadas em endereços de origem e outras condições especiais;

Com a configuração máxima de memória suportada, deve suportar, no mínimo, 4.000.000 (quatro milhões) de rotas IPv4 e 300.000 (trezentas mil) rotas ou IPv6 simultaneamente na tabela RIB (*Routing Information Base*);

Deve suportar, no mínimo, 1.800.000 (um milhão e oitocentas) rotas IPv4 e rotas IPv6 simultaneamente na tabela FIB ( *Forwarding Information Base*);

Deve implementar o protocolo VRRP (Virtual Router Redundancy Protocol), em conformidade com o padrão RFC 3768, ou mecanismo similar de redundância de gateway;

Deve suportar mecanismo de autenticação MD5 entre os peers VRRP;

Deve implementar, no mínimo, 50 grupos VRRP ou de mecanismo similar de redundância de gateway simultaneamente;

Deverá implementar redistribuição controlada de rotas entre diferentes protocolos.

Deverá ser possível controlar os tipos de rotas que serão redistribuídas;

Permitir a virtualização das tabelas de roteamento VRF (*Virtual Routing and Forwarding*) ou VPN-INSTANCE ou MCE ( *Multi* CE);

Deve suportar a criação de, no mínimo, 10 tabelas de roteamento virtuais (VRF);

Deve suportar o protocolo MPLS (*Label Distribution Protocol*, *MPLS Virtual Private Network*, *MPLS QoS*, *MPLS Traffic Engineering*);

Implementar mecanismo de controle de *Multicast* através de:

RFC 1112 - *Host Extensions for IP Multicasting*;

RFC 2236 - *Internet Group Management Protocol*, *Version* 2;

RFC 3376 - *Internet Group Management Protocol*, *Version* 3;

RFC 2362 - *Protocol Independent Multicast - Sparse Mode* (PIM-SM);

RFC 3973 - *Protocol Independent Multicast - Dense Mode* (PIM-DM);

PIM-SM sobre VRF.

Deve implementar o NAT em conformidade com a RFC 1631 e RFC 3022;

Deve suportar traduções de endereços de rede IPv4 em IPv4 (NAT44) e traduções de endereços de rede IPv4 em IPv6 (NAT64) simultaneamente;

Deve possuir suporte à tradução de endereços de porta (*Port Address Translation* - PAT).

**PROTOCOLOS DE SERVIÇO**

Implementar o protocolo NTPv3 (*Network Time Protocol* versão 3) conforme definições da RFC 1305;

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

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

Deve suportar o padrão IEEE 802.1p para cada porta:

Possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p;

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;

Deverá suportar classificação e marcação de pacotes baseadas em VLAN ID;

Deve suportar a classificação, marcação e remarcação baseadas em CoS (*Class of Service*) para a camada de enlace;

Suportar funcionalidades de QoS de *Traffic Shaping* e *Traffic Policing*;

Deve ser possível a especificação de garantia de banda por classe de serviço;

Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como: transmissão do pacote sem modificação; transmissão com remarcação do valor de DSCP; e descarte do pacote.

Deve suportar a classificação, marcação e remarcação baseados em IP *Precedence* e DSCP (*Differentiated Services Code Point* ) para a camada de rede, em conformidade com os padrões RFC 2474 e RFC 2475;

Deverá implementar RFC 2598 *DiffServ Expedited Forwarding* (EF);

Deverá implementar RFC 2597 *DiffServ Assured Forwarding* (AF);

Deve suportar a classificação, marcação e remarcação baseadas em CoS (*Class of Service*) e DSCP, conforme definições do IETF (*Internet Engineering Task Force*);

Deverá implementar aplicação de políticas de QoS em todas as portas físicas do equipamento.

Implementar RTP (Real-Time Transport Protocol) e a compressão do cabeçalho dos pacotes RTP (IP RTP Header Compression).

**REQUISITOS DE GERÊNCIA**

Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de TRAPs;

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

Sem autenticação e sem privacidade (noAuthNoPriv);

Com autenticação e sem privacidade (authNoPriv);

Com autenticação e com privacidade (authPriv) utilizando algoritmo de criptografia AES.

Suportar SNMP sobre IPv6;

Deve suportar o protocolo de gerenciamento SNMP e MIB-II, em conformidade com os padrões RFCs 1157 e RFC 1213;

Implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento como: tráfego de interfaces, uso de CPU do processador, uso de memória, QoS, serviços, etc.;

Possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa;

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

Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas;

Deverá implementar Syslog Local e comunicação com Syslog Remoto;

Deverá permitir a criação de listas de acesso baseadas em endereços IP para limitar o acesso ao elemento de rede via Telnet ou SSH, possibilitando a definição dos endereços IP de origem das respectivas sessões. O acesso gerencial remoto aos equipamentos deverá ser provido através dos protocolos seguros SSHv2 e HTTPS.

Deve suportar o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs.

Deve ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada e/ou somente tráfego de saída.

**SEGURANÇA**

Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um servidor de Autenticação /Autorização do tipo TACACS e/ou RADIUS:

Deverá implementar RFC 2865 RADIUS *Authentication Dial In User Service*;

Deverá implementar RFC 2866 RADIUS *Accounting*;

Deverá implementar definição de grupos de usuários, com diferentes níveis de acesso;

Deverá permitir o controle dos comandos que cada usuário ou grupos de usuários poderão enviar;

Deve implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;

Deve permitir controlar e auditar quais comandos os usuários e grupos de usuários podem emitir;

Implementar mecanismos de AAA (*Authentication*, *Authorization* e *Accounting*) com garantia de entrega.

Todos os comandos de administração do equipamento, executados por qualquer dos meios de acesso: interface de console, Telnet, SSH, HTTP, HTTPS deverão ser individualmente autorizados e registrados (“Accounting”) por este protocolo de controle de acesso administrativo;

Implementar anti-spoofing para IPv4 e IPv6 através de verificação Reverse Path Forwarding (RPF).

**LISTAS DE ACESSOS**

Implementar filtragem de pacotes (ACL - *Access Control List*), para IPv4 e IPv6;

Implementar listas de controle de acesso (ACLs), para filtragem de pacotes, baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino e *flags* TCP;

Deverá implementar contadores para as listas de acesso;

Deverá implementar listas de acesso para o tráfego entrante e sainte;

Permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao equipamento via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH.

**FUNCIONALIDADES DE VPN**

Suportar serviços de VPN baseados no padrão IPSec (IP *Security Protocol*), compatível com IPv4 e IPv6;

Suportar serviços de VPN baseados no padrão IKE (*Internet Key Exchange*);

Implementar IKE v1 e v2;

Devem ser suportados, no mínimo, os algoritmos DES (56 bits), 3DES (168 bits), AES-128 e AES-256 para garantia de confidencialidade às conexões IPSEC;

Suportar criação de VPNs de acordo com o conjunto de padrões IPSEC em modo túnel;

Implementar a criptografia dos pacotes de forma totalmente transparente e automática, sem a alteração dos cabeçalhos incluindo endereços IP de origem e destino, e portas de origem e destino;

Suportar o tráfego protocolo GRE sobre IPSEC;

Suporte ao protocolo de Tunelamento GRE.

**REQUISITOS DE INTERFACE**

Deve possuir uma porta de console para o gerenciamento e configuração do equipamento, no padrão RS232, com conector RJ45 ou DB9 ou uma porta de console com interface USB;

Possuir no mínimo 06 (seis) interfaces Gigabit-Ethernet, no padrão **SFP** e 04 (quatro) interfaces XGigabit-Ethernet, no padrão **SFP +**;

Deve suportar módulos com interfaces compatíveis com os padrões IEEE 802.3ab (1000BASE-T), IEEE 802.3z (1000BASE-SX, 1000BASE-LX/LH) e IEEE 802.3ae (10GBASE-SR e10GBASE-LR).

Deve suportar módulos 1000BASE-X e 10GBASE-X, para comunicações 1Gbps e 10Gbps em distâncias de até 10km;

Deve ser fornecido os *transceivers* ópticos compatíveis e nas quantidades citadas abaixo:

04 (quatro) do tipo 1000BASE-T;

04 (quatro) do tipo 1000BASE-LX;

04 (quatro) do tipo 10GBASE-LR; e

04 (quatro) do tipo 10GBASE-SR;

Deve permitir a reinicialização de interfaces do equipamento sem afetar o funcionamento do mesmo.

**DESEMPENHO**

Deve suportar, no mínimo, 80 (oitenta) Gbps de throughput com todas as funcionalidades de roteamento e segurança ativas simultaneamente para um tráfego IMIX;

Deve suportar uma taxa de comutação de pacotes de no mínimo 60 (sessenta) Mpps considerando-se pacotes de 64 bytes.

**CARACTERÍSTICAS GERAIS DE *HARDWARE***

As capacidades de tráfego expressas neste documento se referem a taxas *wire-rate full-duplex* de entrada e saída simultaneamente;

Os equipamentos fornecidos deverão ter homologação da ANATEL e serem fabricados pelo mesmo fabricante;

Deve possuir LEDs de diagnóstico que forneçam informações de alimentação (*on*/*off*) e atividade do equipamento;

Deve possuir LEDs de diagnósticos que forneçam informações e atividades das portas.

Todas as funções *Layer* 2 e *Layer* 3 deverão ser executadas localmente pelo equipamento, não sendo permitido que estas funções sejam executadas em outros módulos externos ao equipamento, devendo inclusive a interface de configuração do equipamento ser única, dispensando assim a necessidade de configuração módulo a módulo;

Deverá implementar geração de logs sobre eventos no hardware, protocolos, módulos e interfaces;

Todos os requisitos, com exceção daqueles de capacidade (prefixos IP e MAC), deverão ser atendidos de forma concomitante, ou seja, a conformidade de um requisito não pode afetar a disponibilidade dos demais.

O equipamento deverá implementar, no momento da entrega, todas as características exigidas nesta especificação sem a necessidade de inclusão de nenhum componente, módulo ou dispositivo extras.

**SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO CONTRATADA - GRUPO 1:**

A CONTRATADA deverá instalar, configurar, interconectar, testar e documentar a Solução.

O escopo do serviço de instalação compreende:

Até 02 (dois) roteadores, rodando BGP, sendo um em cada site (ambos localizados em Brasília - Distrito Federal).

O planejamento da instalação compreende:

Reuniões de planejamento, que irão gerar um plano de instalação que deve ser validado conjuntamente entre CONTRATANTE e CONTRATADA;

Plano de testes da solução em funcionamento;

Agendamentos de datas, planejamento de entrada em funcionamento da nova solução; e

O plano de teste e o planejamento de entrada em funcionamento das soluções deverão ser elaborados e validados conjuntamente entre CONTRATANTE e CONTRATADA.

A instalação deve compreender:

A desembalagem, a montagem de todos os componentes que integram a Solução;

A instalação dos equipamentos montados em rack padrão, conforme o caso, a energização do equipamento;

A instalação dos softwares necessários para o funcionamento da solução;

Os equipamentos deverão ser adequados à estrutura elétrica nos data centers.

A configuração deve compreender:

Todas as atualizações de *firmware* ou qualquer outro *software* componente da solução, para a versão mais atualizada disponível e estável ou a última compatível;

Habilitação de licenças que porventura sejam adquiridas e recursos do equipamento que serão utilizados no projeto.

A integração compreende:

As verificações dos recursos e o seu perfeito funcionamento e integração com os demais, conforme as melhores práticas indicadas pelo fabricante;

A interconexão do(s) equipamento(s) à rede ethernet do CONTRATANTE;

A interconexão do(s) equipamento(s) aos links WAN dos provedores ativos na CONTRATANTE;

A configuração dos roteadores para roteamento BGP externo (com as operadoras) e interno;

Criação de filtros e devidos ajustes de BGP para o perfeito funcionamento da topologia;

Configuração dos roteadores para que participem do roteamento interno (iBGP).

A documentação compreende:

Relatório com todas as atividades desenvolvidas, desenhos da nova topologia e arquivos de configuração do novo ambiente.

O repasse de conhecimento compreende:

Carga horária mínima de 06 (seis) horas;

Os funcionários da CONTRATADA deverão possuir todo o ferramental necessário ao exercício das suas atividades;

Opcionalmente, a critério exclusivo do CONTRATANTE, poderá haver serviços fora dos horários, inclusive durante o período noturno. Nestes casos a empresa CONTRATADA deverá alocar a equipe técnica durante o transcorrer da tarefa sem qualquer ônus para o CONTRATANTE; e

Todo o processo de instalação e configuração realizado deverá ser documentado pela CONTRATADA sob a forma de relatório.

A interconexão do(s) equipamento(s) à rede ethernet do CONTRATANTE;

Configuração para que participem do roteamento interno (iBGP) com os roteadores BGP de borda;

O serviço deverá ser realizado por profissional certificado de nível profissional pelo fabricante da solução de roteamento;

A CONTRATANTE pode requerer operação assistida para a implementação/configuração dos equipamentos.

**DESCRIÇÃO DO OBJETO – GRUPO 2**

**REQUISITOS DA AQUISIÇÃO**

A solução/ferramenta é composta por um sistema de análise de fluxo BGP, FLOW, SNMP, alertas de DoS/DDoS e uso de roteadores para mitigação por *BLACKHOLE* e *FLOWSPEC*;

Requisitos Gerais:

Deve ser entregue para análise do tráfego de 02 (dois) roteadores;

Deve ser oferecida em formato de *Software*, para ser instalada dentro do ambiente de Data Center da Contratante, suportando Hypervisor ESXi 5.5 ou superior e ou KVM;

Deve permitir *query* SNMP (v1, v2c ou v3);

Deve prover o estado de comunicação da coleta de Flow, BGP e SNMP de cada roteador monitorado;

Deve gerar traps SNMP caso ocorra uma das seguintes situações: Ipflow perdidos, alertas do sistema, condições de sobrecarga, carga elevada de CPU ou memória;

Deve enviar alertas através de e-mails SMTP / SNMP traps e mensagens SYSLOG para dispositivos externos para anomalias graves, eventos do sistema ou outros problemas de tráfego;

Deve realizar backups de forma manual ou automatizada e recorrente da base de dados, incluindo a possibilidade de exportar os dados de backup para um servidor remoto através de SCP;

Deve armazenar e mostrar um log das trocas de configuração que mostrem quando e por qual usuário foram realizadas as mesmas;

Deve prover uma interface WEB sem que seja necessária instalação de cliente na máquina para visualização ou alteração de quaisquer configurações;

A interface WEB deve prover funções de busca para facilitar a navegação em grandes números de alertas, roteadores, interfaces e objetos configurados;

Deve prover um modo de acesso a CLI através de SSH;

Deve permitir múltiplos níveis de acesso e permissão, incluindo no mínimo: administrador, operador, usuário e bloqueado;

Deve permitir a criação de grupos de usuários distintos com diferentes permissões e visualizações segmentadas do tráfego capturado pela solução;

Deve prover serviços de autenticação de usuários por meio de uma base de autenticação local, por RADIUS, TACACS ou uma configuração combinada destes métodos.

Análise e Detecção:

A Análise/Detecção destina-se a coletar dados do tráfego da rede (através da captura de flow) analisá-los e fornecer informações para a planejamento, engenharia de rede e detecção de ataques DoS e DDoS;

Deve utilizar o recebimento de tráfego via fluxos de telemetria do tipo Netflow, sFlow, Jflow e IPFIX;

Deve funcionar de modo a não inserir um ponto de falha para a rede, funcionando em modo Offline;

Deve apresentar os dados coletados de BGP e fluxos de telemetria em interface via WEB (HTTPS);

Deve possuir no mínimo 1.000 (um mil) recursos monitorados (clientes, provedores, serviços) e permitir o crescimento da quantidade de recursos em até 20.000 (vinte mil) por meio de adição de licenças;

Deve aceitar informações de rotas BGP de todos os roteadores monitorados na rede e correlacionar esta informação com a obtida em IPflow, de modo que se possa criar objetos monitorados por ASN, AS path, comunidade e outros diferentes atributos dinâmicos BGP;

Deve permitir a criação de objetos de monitoração por, pelo menos: blocos CIDR IPv4 e/ou IPv6, BGP ASN, Comunidade BGP, Interface de Roteador e/ou combinação de anteriores;

Deve determinar a importância das anomalias baseado nos impactos que estas provocam na rede, com pelo menos 3 níveis de importância;

Deve permitir a detecção de ataques volumétricos DoS e DDoS de camadas 3 e 4 do modelo OSI;

Deve suportar a detecção e geração de alertas de anomalias por taxas excessivas de tráfego que excedam parâmetros configurados, para no mínimo estes parâmetros: Tráfego total (*Bytes* e/ou Pacotes), DNS, Amplificação de DNS (*Bytes* e/ou Pacotes), ICMP, Fragmentação de IP, IP`s privados, Amplificação em MS SQL RS (*Bytes* e/ou Pacotes), Amplificação NTP ( *Bytes* e/ou Pacotes), Amplificação SNMP (*Bytes* e/ou Pacotes), Amplificação SSDP (*Bytes* e/ou Pacotes), TCP NULL, TCP RST, TCP SYN, UDP;

Deve mostrar o impacto geral de uma anomalia assim como o impacto da mesma em cada interface envolvida através das taxas de bits e pacotes por segundo;

Deve mostrar uma caracterização básica da anomalia, apresentando no mínimo os seguintes componentes predominantes: blocos IPv4 e IPv6 (Origem e Destino), protocolos IP, portas dos protocolos IP (Origem e Destino) e flags TCP;

Deve identificar todos os roteadores monitorados afetados pela anomalia de rede e cada interface de entrada do mesmo que foi afetada;

Deve permitir que os usuários classifiquem uma anomalia, escolhendo entre uma lista de opções pré-definidas, por exemplo: possível ataque, falso positivo;

Deve ser capaz de prover um alerta se algum Peer BGP anuncia uma rota que é local da rede (BGP *Hijacking*);

A detecção rápida de ataques de alto volume e alta severidade poderá ser habilitada por objeto monitorado;

Deve enviar queries SNMP v1, v2c e v3 aos roteadores monitorados como mecanismo de validação da coleta de flow;

Deve correlacionar dados de IP flow de cada roteador de borda monitorado com a informação BGP obtida deste roteador e deve com isso gerar relatórios sobre atributos BGP, incluindo no mínimo: ASN`s Origem/Peer/, AS-Paths;

Deve apresentar relatórios de quantidade de tráfego entre interfaces monitoradas, podendo correlacionar este tráfego com recursos monitorados (por exemplo: clientes, provedores);

Deve apresentar informações de previsão de troca de conexão entre provedores Internet;

Deve prover no mínimo as seguintes informações de tráfego: tráfego médio, tráfego atual, tráfego máximo e percentual de 95% para a rede em geral, por roteador, por interface, por serviço, por aplicação ou por recurso a proteger;

Deve apresentar relatórios de tráfego entre provedores e outros recursos monitorados incluindo tráfego interno;

Deve permitir a configuração de sites VPN por blocos CIDR e prover um relatório de tráfego por Site VPN dentro de uma VPN (Virtual Private Network);

Deve apresentar relatórios de tráfego por tamanhos diferentes de pacotes, protocolos, portas TCP/UDP e tipo ICMP por VPN e Site VPN;

Deve ter permissão para extrair relatórios com, no mínimo, as seguintes informações: endereços IP com maior consumo de tráfego, protocolos e aplicações;

Deve apresentar relatórios de tabelas de rotas de um roteador específico para um período particular de tempo nos últimos 3 meses, filtrado por comunidade BGP, Asregex e/ou prefixo (exato, menor ou maior);

Deve prover informações de fluxos para o período mais recente de coleta, por roteador, interface ou objeto administrado;

Além de assinaturas, a solução deve prover visão de estatísticas mundiais da Internet, com dados de roteamento e segurança coletadas de sua própria rede colaborativa. Com dados de utilização mundial de protocolos, métricas de BGP mundiais, visão global de instabilidade de rotas BGP, além de uma visão global, atualizada em tempo real dos ataques DDoS que ocorrem ao redor do mundo;

Deve prover identificação por país para origens de tráfego de entrada e saída;

Deve identificar invasores DDoS baseado em indicadores de endereço IP proveniente de base própria;

Deve poder enviar ACL's inteligentes aos roteadores BGP monitorados a fim de descartar tráfego quando gerado alerta de DOS /DDOS, em formato FLOWSPEC (ACL sobre BGP), em roteadores que suportem esta funcionalidade, a fim de poder descartar, aplicar RATE-LIMIT, ou permitir um certo padrão de tráfego específico formado por camadas 3 e 4 OSI;

Estes padrões de mitigação por FLOWSPEC devem permitir selecionar tráfego através de:

IP de origem e ou destino, porta tcp e ou udp de origem e ou destino, tamanho do pacote, *flag* do pacote, *tos* do pacote, uma ou mais opções detalhadas;

A mitigação por BLACKHOLE ou FLOW-SPEC no ROTEADOR suportado, poderá ser aplicada independentemente por objeto, podendo ser automatizada baseado no nível do alerta.

**SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO CONTRATADA - GRUPO 2:**

Todos os componentes de *software* que integram a solução/ferramenta deverão ser fornecidos pela CONTRATADA e deverão estar plenamente implementados ao final do serviço de instalação;

Todo serviço de instalação, configuração e atualização da solução/ferramenta será de total responsabilidade da CONTRATADA.

O serviço de instalação da solução/ferramenta deverá ser realizado por profissionais especializados, certificados pelo fabricante da Solução a ser entregue pela CONTRATADA.

O serviço de instalação da Solução compreenderá, no mínimo, a configuração da solução/ferramenta adquirida com as funcionalidades indicadas pela CONTRATANTE, bem como a integração desta com os 02 (dois) roteadores BGP, disponibilidade em produção pelo CONTRATANTE;

A CONTRATADA deve executar o processo de integração da nova solução com os ativos computacionais envolvidos, respeitando o cronograma de instalação e fazendo a devida compatibilidade técnico-operacional, garantindo desta forma que o ambiente atual possa ser integrado à nova solução. Qualquer problema ou incompatibilidade é de responsabilidade da CONTRATADA e por ela deve ser resolvido;

A CONTRATADA deverá entregar um Plano de Instalação da solução no prazo máximo de 05 (dias) dias úteis, contados a partir da data do Termo de Aceite de Entrega, contendo, no mínimo:

cronograma descrevendo as atividades de instalação, indicando prazos e respectivas datas de início e término;

lista de recursos de tecnológicos de *hardware* e *software* que serão utilizados;

procedimentos que serão seguidos para a realização dos testes de funcionamento em produção e outras informações adicionais requeridas pela Presidência da República;

A CONTRATANTE avaliará o Plano de Instalação fornecido pela CONTRATADA no prazo máximo de 05 (cinco) dias corridos, contados a partir da data de entrega do referido plano. Caso o Plano de Instalação não seja aceito pela CONTRATANTE, a CONTARTADA terá prazo de 05 (cinco) dias corridos, a partir da data de comunicação do fato, para efetuar os ajustes necessários para a apresentação de um novo Plano de Instalação. Nesse caso, a CONTRATANTE terá novo prazo de 05 (cinco) dias corridos, a partir da data de entrega, para avaliar o novo plano;

A solução deverá ser instalada pela CONTRATADA no prazo de até 30 (trinta) dias corridos contados a partir da aprovação do Plano de Instalação pela CONTRATANTE, dentro do horário comercial e em dias úteis. Havendo acordo de ambas as partes, a instalação poderá ocorrer fora do horário comercial e em dias não úteis;

Faz parte da instalação e é responsabilidade da CONTRATADA a configuração e customização da solução;

A CONTRATADA deve executar o processo de integração da nova solução com os ativos computacionais envolvidos, respeitando o cronograma de instalação e fazendo a devida compatibilidade técnico-operacional, garantindo desta forma que o ambiente atual possa ser integrado à nova solução. Qualquer problema ou incompatibilidade é de responsabilidade da CONTRATADA e por ela deve ser resolvido;

O licenciamento será de uso permanente, isto é, tipo perpétuo. Em caso do prazo de *subscription* encerrar, a solução deve continuar a funcionar sem nenhuma interrupção no serviço;

Não será necessário o fornecimento de equipamentos e licenças adicionais para permitir a virtualização da solução. Será utilizada a infraestrutura de virtualização mantida pelos recursos tecnológicos da CONTRATADA;

A CONTRATADA deverá disponibilizar o acesso direto à base de dados de conhecimento do fabricante da solução que contenha informações de assistência, orientação para instalação, desinstalação, configuração, atualização de software, aplicação de correções (*patches*), diagnóstico, avaliações e resolução de problemas, e demais atividades relacionadas à correta operação, e funcionamento da solução.

**TREINAMENTO TÉCNICO – GRUPOS 01 e 02**

Treinamento para até 16 (dezesseis) participantes localizados na Presidência da República, em Brasília, devendo esses serem distribuídos da seguinte forma:

08 (oito) participantes para o treinamento do Item 1 do Lote 1 - ROTEADOR DE BORDA BGP, e

08 (oito) participantes para o treinamento do item 1 do Lote 2 - FERRAMENTA DE ANÁLISE DE TRÁFEGO E ROTEAMENTO BGP;

O(s) instrutor(es) deverão possuir certificação técnica comprovada, emitida pelo fabricante da solução, nas configurações dos referidos equipamentos ou versões do software da solução (ferramenta) adquirida;

Cada treinamento deverá ter duração mínima de 30 (trinta) horas, a ser ministrado por videoconferência, em horário comercial, com carga horária de, no máximo, 4 (quatro) horas diárias;

Os treinamentos devem iniciar em até 15 (quinze) dias úteis após a instalação dos equipamentos, componentes e softwares das soluções;

Os treinamentos devem ser de natureza teórica e prática, devendo abranger todos os equipamentos, componentes e softwares das soluções ofertadas, em seus aspectos mais relevantes, além de focar em suas funcionalidades direcionadas ao protocolo de roteamento dinâmico BGP (Border Gateway Protocol) para comunicação de sistemas autônomos (AS);

A CONTRATADA será responsável pelo fornecimento de todo material didático pedagógico individual necessário para a execução dos treinamentos;

O conteúdo programático dos treinamentos deverão ser definidos previamente pela CONTRATANTE em conjunto com a CONTRATADA e deverão abordar, no mínimo, os principais aspectos relativos às soluções adquiridas e de suas implantações no caso específico da Presidência da República;

A CONTRATADA deverá fornecer certificado individual de conclusão com aproveitamento do curso em até 05 (cinco) dias úteis após o encerramento dos treinamentos;

Os treinamentos deverão ocorrer em período e horário definido pela CONTRATANTE, respeitando as especificações contidas neste item;

A qualidade dos treinamentos ministrados deverão sofrer avaliações por seus participantes ao final do mesmo e, caso seja considerada insuficiente, a CONTRATADA deverá providenciar a realização de nova turma, até o alcance dos objetivos do treinamento, sem ônus adicional para a Presidência da República;

Para a consecução da parte prática dos treinamentos deverão ser utilizados equipamentos similares aos ofertados, quando for o caso, além de todos os softwares que fizerem parte das soluções.

**SERVIÇO DE SUPORTE TÉCNICO**

**GRUPO 01**

O serviço de suporte técnico será prioritariamente na modalidade remoto (24x7x365) nos equipamentos, pelo período de 12 (doze) meses da solução contratada;

A CONTRATADA deverá fornecer apoio técnico para tarefas de auditoria e análise de logs;

Os casos de necessidade de suporte ON-SITE deverão ser combinados conforme a gravidade do problema, sendo que os custos deverão ser de responsabilidade da CONTRATADA;

Os chamados para atendimento ON-SITE deverão ser abertos com antecedência mínima de 01 (um) dia útil;

A CONTRATADA deverá possuir sistema de chamados via WEB que possibilite, no mínimo:

Abertura, acompanhamento, listagem e fechamento de chamados, a qualquer momento, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana. Os chamados devem estar sempre atualizados ao final do dia;

Armazenar e gerar os relatórios das atividades executadas associadas ao chamado. Caso haja alguma indisponibilidade no sistema de abertura de chamados, deverão ser enviados relatórios dos chamados abertos, ao final do dia, com seus respectivos assentamentos;

Sanar dúvidas relacionadas ao funcionamento dos equipamentos e softwares envolvidos na solução.

Configuração e suporte de protocolos de roteamento internos (IGPs) e externos (EGPs) em IPv4 e em IPv6;

Configuração de endereçamento e recursos de VPN dinâmicas com IPSEC, GRE e algoritmos de criptografia e protocolos quando solicitado;

Configuração e suporte de Listas de Controle de Acesso (ACL);

Configuração e suporte do protocolo VRRP ou protocolo similar de redundância de gateway para alta disponibilidade;

Configuração de regras aplicáveis à solução ofertada para funcionamento com Sistema Autônomo (ASN);

Análise e suporte no acesso à Internet, sites remotos, serviços de rede oferecidos aos servidores e aos usuários do CONTRATANTE que dependem dos links WAN;

Apoio técnico em configurações de alta disponibilidade, redundância e gerência dos roteadores;

Identificação e resolução de problemas em *software* e *hardware;*

A CONTRATADA deverá indicar, na assinatura do contrato, os procedimentos para abertura do chamado de suporte técnico;

A CONTRATADA deverá possuir estrutura de suporte com atendimento em português do Brasil e chamada direta gratuita (DDG) 0800 ou número com custo de ligação local na cidade de Brasília;

Todos os chamados, bem como as providências adotadas, deverão ser armazenados em sistema para controle, rastreamento e consulta de chamados efetuados junto à CONTRATADA;

A CONTRATADA deverá atender às solicitações técnicas abertas pela CONTRATANTE em regime contínuo de 24x7 (vinte e quatro horas por dia, sete dias por semana);

O atendimento será realizado por profissionais especializados e deverá cobrir todo e qualquer defeito apresentado, incluindo o fornecimento e a substituição de peças e/ou componentes, ajustes, reparos e correções necessárias para o correto funcionamento do equipamento ou da solução;

Não sendo possível o reparo do equipamento no local em que está instalado ou dentro do prazo de solução da prestação do serviço, deverá ser providenciada imediatamente a substituição temporária por outro equipamento do mesmo fabricante, com configurações iguais ou superiores às do inicialmente instalado, até que o equipamento defeituoso retorne em perfeitas condições de funcionamento;

No caso da substituição temporária do equipamento em parte ou no todo, deverá ser justificada tal necessidade ao Gestor do contrato, por escrito, no prazo máximo de 01 (um) dia corrido, anexando documentação comprobatória contendo informações dos equipamentos envolvidos, para providências de autorização de saída do equipamento e de atualização dos dados patrimoniais, após constatar tal necessidade;

O equipamento a ser removido ficará sob responsabilidade da CONTRATADA, ficando esta responsável pelo seu transporte, guarda e acondicionamento;

O equipamento colocado em substituição ficará instalado até a devolução do equipamento consertado, que não poderá ultrapassar o prazo máximo de 30 (trinta) dias corridos;

Sendo impossível o reparo do equipamento ou cumprimento do prazo máximo para conserto (item anterior), a CONTRATADA realizará sua substituição definitiva, nas mesmas condições e prazos previstos acima;

No caso de troca de equipamento, o serviço de suporte técnico será responsável pela manutenção das configurações do equipamento.

**GRUPO 02**

O serviço de suporte técnico será prioritariamente na modalidade remoto (24x7x365) para solução/ferramenta de análise de tráfego e roteamento BGP, pelo período de 12 (doze) meses da solução contratada;

A CONTRATADA deverá fornecer apoio técnico para tarefas de auditoria, análise de logs e confecção de relatórios gerenciais;

Os casos de necessidade de suporte ON-SITE deverão ser combinados conforme a gravidade do problema, sendo que os custos deverão ser de responsabilidade da CONTRATADA;

Os chamados para atendimento ON-SITE deverão ser abertos com antecedência mínima de 01 (um) dia útil;

A CONTRATADA deverá possuir sistema de chamados via WEB que possibilite, no mínimo:

Abertura, acompanhamento, listagem e fechamento de chamados, a qualquer momento, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana. Os chamados devem estar sempre atualizados ao final do dia;

Armazenar e gerar os relatórios das atividades executadas associadas ao chamado. Caso haja alguma indisponibilidade no sistema de abertura de chamados, deverão ser enviados relatórios dos chamados abertos, ao final do dia, com seus respectivos assentamentos;

Sanar dúvidas relacionadas ao funcionamento da solução/ferramenta e demais *softwares* envolvidos;

A CONTRATADA deverá indicar, na assinatura do contrato, os procedimentos para abertura do chamado de suporte técnico;

A CONTRATADA deverá possuir estrutura de suporte com atendimento em português do Brasil e chamada direta gratuita (DDG) 0800 ou número com custo de ligação local na cidade de Brasília;

Todos os chamados, bem como as providências adotadas, deverão ser armazenados em sistema para controle, rastreamento e consulta de chamados efetuados junto à CONTRATADA;

A CONTRATADA deverá atender às solicitações técnicas abertas pela CONTRATANTE em regime contínuo de 24x7 (vinte e quatro horas por dia, sete dias por semana);

O atendimento será realizado por profissionais especializados e deverá cobrir todo e qualquer defeito apresentado, incluindo ajustes, reparos e correções necessárias para o correto funcionamento da solução/ferramenta;

# 6. Demais Requisitos da Solução de TIC

**DEMAIS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO**

- **DA JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO**
  - Justificativa (Art. 15 da IN. SGD/ME nº 1/2019):

Considerando a natureza *sui generis* da Presidência da República como órgão da estrutura governamental do Brasil, seus requisitos de comunicação podem exigir níveis de segurança, de controle e de qualidade acima da média e dos padrões que costumam ser contratados por boa parte dos órgãos governamentais. Assim, a Presidência da República decidiu adotar a estratégia de se tornar *Autonomous System*, passando de mera usuária a partícipe no controle e planejamento de suas comunicações de dados e voz no Sistema de Internet Global.

Como parte deste planejamento e controle, diversas melhorias e incrementos de qualidade de serviço vêm sendo implantados pela Diretoria de Tecnologia no âmbito da infraestrutura de redes e de telecomunicações de dados. Tal conjunto engloba a readequação dos meios de provimento de interligação da Presidência da República com a Internet. Considerando que tal interligação precisa ser provida a diversos sites que compõem a área de atendimento dos serviços de Tecnologias da Informação e Telecomunicação, fornecidos pela Diretoria de Tecnologia com padrões de qualidade e segurança elevados.

Neste sentido, objetiva-se neste processo a aquisição de equipamentos de redes, como roteadores WI-FI, switches e roteadores, para adequar e modernizar a infraestrutura de rede IP, substituir equipamentos antigos ou de longo tempo de uso, sem peça de reposição, sem suporte técnico e sem garantia.

## DA CLASSIFICAÇÃO DOS BENS COMUNS

- **Bens Comuns:**

A natureza do objeto a ser adquirido enquadra-se na classificação de bens comuns, nos termos do parágrafo único do art. 1° da Lei 10.520/02.

- **DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR**

Como critério de aceitabilidade de preços, serão considerados como máximos os preços estimados da planilha, tanto global quanto unitários.

O critério de julgamento da proposta é o do menor preço do total por grupo

As regras de desempate entre propostas são as discriminadas no edital.

- **DOS CRITÉRIOS DE HABILITAÇÃO**:
  - As exigências de habilitação jurídica e de regularidade fiscal e trabalhista são as usuais para a generalidade dos objetos, conforme disciplinado no edital.
  - Os critérios de qualificação econômica a serem atendidos pelo fornecedor serão:
  - certidão negativa de falência expedida pelo distribuidor da sede do licitante;
  - balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta;
  - no caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade;
  - é admissível o balanço intermediário, se decorrer de lei ou contrato/estatuto social;
  - comprovação da boa situação financeira da empresa mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), obtidos pela aplicação das seguintes fórmulas:
  - LG = (Ativo Circulante + Realizável a Longo Prazo) / (Passivo Circulante + Passivo Não Circulante);
  - SG = (Ativo Total) / (Passivo Circulante + Passivo Não Circulante);
  - LC = Ativo Circulante / Passivo Circulante
- As empresas que apresentarem resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar patrimônio líquido de 10% (dez por cento) do valor estimado da contratação ou do item pertinente;
- A comprovação da qualificação econômico-financeira, conforme o caso, poderá ser substituída pela consulta ao SICAF, nos casos em que a empresa estiver habilitada no referido sistema, conforme o disposto nos artigos 6º, inciso III, 10 a 16 e 21, inciso III, da Instrução Normativa SEGES/MP nº 3, de 2018.

- **Os critérios de qualificação técnica a serem atendidos pelo fornecedor serão:**

- Comprovação de aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis com o objeto desta licitação, ou com o item pertinente, mediante a apresentação de atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado.
- Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a serviços executados com as seguintes características mínimas:
- Os critérios de qualificação técnica para o grupo 1 a serem atendidos pelo fornecedor serão:
    - Comprovação de aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis com o objeto desta licitação, ou com o item pertinente, mediante a apresentação de atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado.
- Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a serviços executados com as seguintes características mínimas:
    - O licitante deve apresentar atestado de capacidade técnica em seu nome, fornecido por pessoa jurídica de direito público ou privado, comprovando o fornecimento, instalação, configuração, garantia e suporte técnico para o objeto da presente licitação ou outro roteador que possua no mínimo as seguintes quantidade de rotas simultaneamente na tabela FIB (Forwarding Information Base):

        - rotas IPv4  800.000 (oitocentos mil);

        - rotas IPv6 100.000 (cem mil) ;

- O licitante deve apresentar atestado da mesma forma do item acima para as conexão EBGP com no mínimo a configuração de  02 (dois) ASN distintos.

- Nos atestados, devem estar explícitos: a empresa ou órgão que está fornecendo o atestado, o responsável pelo setor encarregado do objeto em questão, os equipamentos administrados com suas respectivas descrições (versão, capacidade, etc.);
- No caso de atestados emitidos por empresa da iniciativa privada, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa proponente. Serão considerados como pertencentes ao mesmo grupo empresarial da empresa proponente, empresas controladas ou controladoras da empresa proponente, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da empresa proponente.
- A exigência dos atestados se justifica pela necessidade de obtenção de garantias de experiência e qualidade comprovada da contratada na prestação dos serviços em comento, devido a complexidade técnica da aquisição e serviços, e as exigências dos requisitos de segurança. O art. 30, inciso II, da Lei 8.666/93, autoriza expressamente a administração a exigir da licitante a comprovação de que já executou objeto compatível, em prazo, com o que está sendo licitado.
- Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

- **DA ENTREGA E DOS CRITÉRIOS DE ACEITAÇÃO DO OBJETO**

Os equipamentos adquiridos deverão ser entregues e instalados em até 120 (cento e vinte) dias a partir do recebimento da Solicitação de Fornecimento/Ordem de Serviço.

A entrega dos equipamentos deverá ser realizada, em remessa única, no seguinte endereço: Almoxarifado Central da Presidência da República, situado na Avenida N-2, Palácio do Planalto, CEP 70150-900, em Brasília-DF.

Os bens serão recebidos provisoriamente no prazo de 15 (quinze) dias, pelo(a) responsável pelo acompanhamento e fiscalização do Contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

Após o recebimento provisório, a instalação deverá ser realizada pela Contratada, em conjunto com o corpo técnico da Presidência da República, dentro do prazo estabelecido no Termo de Referência.

Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 15 (quinze) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

Os bens serão recebidos definitivamente, após instalação, configuração e implantação, conforme especificações técnicas no Termo de Referência, mediante parecer do(a) responsável pelo acompanhamento e fiscalização do Contrato, em até 15 (quinze) dias após a execução do serviço por parte da Contratada.

Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.

O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da contratada pelos prejuízos resultantes da incorreta execução do Contrato.

A garantia dos bens e o suporte será de, no mínimo, 60 (sessenta) meses, a partir do recebimento definitivo do objeto contratado.

# 7. Necessidades de Negócios da Solução

| NECESSIDADES DE NEGÓCIO |
|---|

- **Necessidades identificadas:**

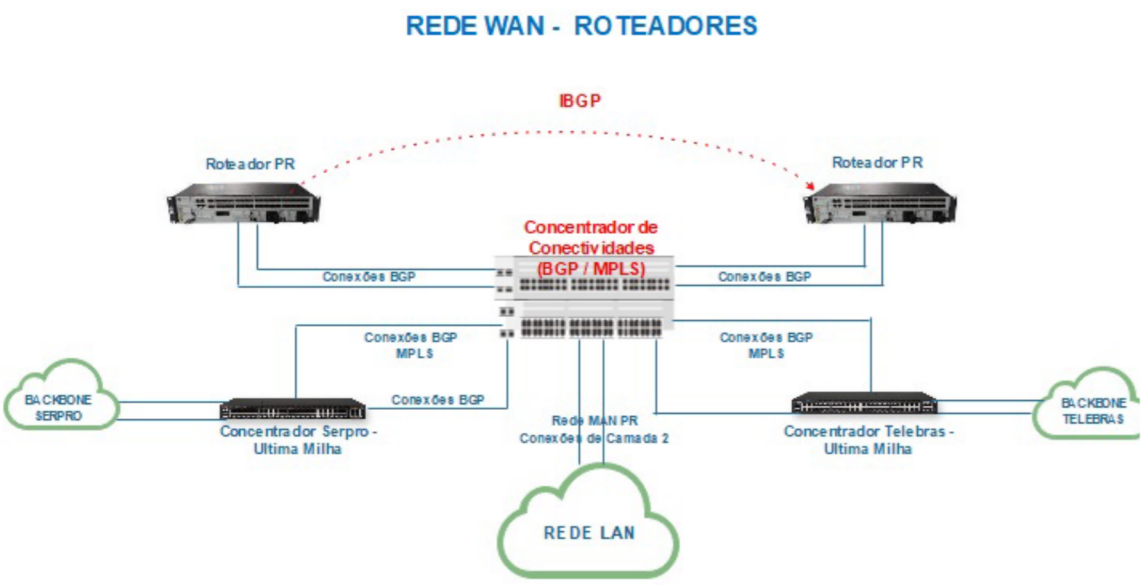
As funções finalísticas exercidas pela Presidência da República exigem o provimento contínuo de acesso pleno e informações de relevância nacional e internacional, as quais muitas vezes são divulgadas e acessadas por meio das m mídias eletrônicas. Em adição, grande parte dos sistemas de informação que são utilizados para a realização de ativida meio e da área fim da Presidência da República são realizadas com o uso da Internet.

Considerando a natureza *sui generis* da Presidência da República como órgão da estrutura governamental do Brasil, seus r comunicação podem exigir níveis de segurança, de controle e de qualidade acima da média e dos padrões que co contratados por boa parte dos órgãos governamentais. Assim, a Presidência da República decidiu adotar a estratégia d *Autonomous System*, passando de mera usuária a partícipe no controle e planejamento de suas comunicações de dad Sistema de Internet Global.

Como parte deste planejamento e controle, diversas melhorias e incrementos de qualidade de serviço vêm sendo impla Diretoria de Tecnologia no âmbito da infraestrutura de redes e de telecomunicações de dados. Tal conjunto engloba a r dos meios de provimento de interligação da Presidência da República com a Internet. Considerando que tal interligaçã provida a diversos sites que compõem a área de atendimento dos serviços de Tecnologias da Informação e Telec fornecidos pela Diretoria de Tecnologia com padrões de qualidade e segurança elevados, propõe-se novo processo de co Serviço de Comunicação Multimídia (SCM) contemplando o tráfego de dados, voz e vídeo, provido com tecnologia do t */MPLS* (Virtual Private Network - Multiprotocol Label Switching) ou semelhante, para atendimento aos es representações regionais, Link de Provimento de Acesso a Internet com proteção de ataque contra negação de serviço, pr equipamentos e serviços necessários à implantação dos acessos aos concentradores e *Link de Provimento de Acess* eventual em todo Território Nacional, para o atendimento de deslocamentos presidenciais quando solicitado.

Em virtude da necessidade de que esse provimento seja ininterrupto, torna-se necessário que em parte dos sites (prédios/ Presidência da República haja atendimento redundante. Parte destes locais é atendido atualmente por meio da interlig INFOVIA, provida por meio de contratação com o SERPRO, sem que haja, em futuro próximo, qualquer outra forma de redundante eficiente e adequado em qualidade e capacidade que não seja por meio de nova contratação.

Diante disso, trata-se da aquisição de 2 (dois) roteadores BGP (*Border Gateway Protocol*), conjuntamente com u /ferramenta de análise de tráfego e roteamento BGP, com o objetivo de implementar e melhor gerir uma arquitetura de de equipamentos na interconexão da rede interna da Presidência da República com a redes externas, atendida pelos Conectividade IP, MPLS, MetroEthernet, de diversos provedores, atendimento de VPN´s, conforme demonstrado na figura




Demanda dos potenciais gestores e usuários da solução: A demanda foi motivada mediante oficialização contida no Documer Oficialização da Demanda (DOD) acostado aos autos do processo nº 00094.000498/2020-61. A presente solução possui como p gestores integrantes da Coordenação de Redes de Longa Distância e Telecomunicações (CORET) e como usuários diversos set Presidência da República, em atendimento à necessidade de controle de recursos dispendidos com telecomunicações.

Estimativa da demanda máxima atual e futura: a demanda consiste na aquisição de nova solução tecnológica e informacional en evolução das necessidades relacionadas ao negócio.

## 8. Levantamento de Mercado

**ANÁLISE DE SOLUÇÕES**

- **Grupo1 - Para o objetivo desejado, verificam-se 3 (três) possíveis solução demanda:**
- **Solução 01 - Aquisição** de roteadores BGP (*Border Gateway Protocol*) com garantia de 60 (sessenta) meses.

Está opção **considera a aquisição de roteadores BGP.** Com a aquisição, esta solução viabiliza a manutenção, operação e gerenciamento direto dos técnicos especializados da Presidência da República nos equipamentos adquiridos, possibilitando a pronta tomada de decisão e ação em eventos de riscos ou falhas.

Está opção viabiliza a adoção da Topologia de Rede proposta no **Item 7. Necessidades de Negócios da Solução** deste E.T.P., com a dupla abordagem de equipamentos de redes, possibilitando a desativação do aluguel de 01 roteador do atual contrato de conexão de Internet (Contrato nº 27/2020 - Telebrás).

- **Solução 02 - Utilização do Firewall como roteadores BGP (*Border Gateway Protocol*).**

Está opção considera o uso do Firewall exercendo as funções de roteadores BGP.

O Firewall da Presidência da República é um Firewall UTM, que possibilita a configuração de algumas funções de roteador. Contudo o hardware não foi projetado para executar todas as funcionalidades específicas requerida por um roteador BGP, mas que eventualmente poderia ser utilizados como um backup em caso de falhas, o que será superado com a adoção da Topologia de Rede proposta no **Item 7. Necessidades de Negócios da Solução** deste E.T.P.

- **Solução 03 - Aluguel de roteadores BGP (*Border Gateway Protocol*) das empresas contratadas.**

Está opção já vem sendo utilizado dentro dos Contratos de conexão de Internet (Contrato nº 54/2017 e nº 27/2020 - Telebrás). Contudo, esta solução tem inviabilizado a manutenção, operação e gerenciamento direto dos técnicos especializados da Presidência da República no equipamento, o que restringe a decisão e tomada de ação em eventos de riscos ou falhas.

Está opção não viabiliza a adoção da Topologia de Rede proposta no **Item 7. Necessidades de Negócios da Solução** deste E.T. P., com a dupla abordagem de equipamentos de redes, pois o atual Contrato apenas prevê o aluguel de 01 roteador.

- **Grupo2 -** Para o objetivo desejado, verificam-se 03 (três) possíveis modalidades de contratação da demanda:
- **Solução 01 –** Modalidade SaaS *Subscription*: **locação** de *software*/ferramenta de análise de tráfego de roteamento BGP, com garantia para 60 (sessenta) meses, como um serviço com período de uso pré-definido (*Software as a Service* ).

**Essa modalidade de SaaS –** *Software* como **serviço locado**, é uma forma de distribuição e comercialização de software /aplicação, onde o fornecedor da solução se responsabiliza por toda a estrutura necessária à disponibilização do sistema (servidores, conectividade, segurança lógica), e o cliente/usuário utiliza o *software* como um serviço com propósitos específicos que estarão disponíveis para os usuários localmente, nas suas instalações físicas.

Com essa modalidade de locação decreta-se que as atividades referentes a gestão da ferramenta, guarda e manipulação das bases de dados com informações sensíveis e sigilosas (informações de roteamento, logs de segurança, etc), ficarão sob responsabilidade da equipe técnica da Presidência da República.

A característica principal dessa modalidade de serviço é a não aquisição do *software* e das licenças de modo definitivo, vitalício, mas sim o direito pelo uso destas a partir de pagamentos recorrentes, normalmente mensal ou anual. Após o encerramento do período de uso, previamente definido em contrato, o acesso à ferramenta é imediatamente interrompido, bem como as funcionalidades da solução são totalmente descontinuadas, não podendo ser utilizadas nem de modo parcial/limitada, pois a infraestrutura (servidores e software envolvidos), anteriormente disponibilizada, é completamente removida pelo contratado.

- **Solução 02 – Modalidade SaaS *Cloud*: locação** de software/ferramenta de análise de tráfego de roteamento BGP, com garantia para 60 (sessenta) meses, com um serviço em nuvem (*Software as a Service - Cloud*).

**A modalidade SaaS *Cloud* –** é também uma forma de distribuição e comercialização de software/aplicação por locação, mas difere-se da modalidade descrita na Solução 01, onde o fornecedor da solução se responsabiliza por toda a estrutura necessária à disponibilização do sistema (servidores, conectividade, base da dados, com informações sigilosas, segurança física e lógica), e o cliente/usuário utiliza o *software* como um serviço com propósitos específicos que estarão disponíveis para os usuários **via internet**, em ambiente externo.

A característica principal dessa modalidade de serviço é a não aquisição do *software* e das licenças vitalícias, mas sim o direito pelo uso destas a partir de pagamentos recorrentes, normalmente mensal ou anual. Após o encerramento do período de uso, previamente definido em contrato, o acesso à ferramenta é imediatamente interrompido, bem como as funcionalidades da solução são totalmente descontinuadas, não podendo ser utilizadas nem no modo parcial/limitada.

**Solução 03 -** Modalidade *On Premise*: **aquisição** do software/ferramenta de análise de tráfego de roteamento BGP, com garantia para 60 (sessenta) meses, para ser disponibilizado/instalado na infraestrutura local, como um produto com licenciamento perpétuo.

Na modalidade *On Premise*, após a aquisição do produto, neste caso um software/ferramenta, este terá seus componentes instalados e disponibilizados localmente, isto é, totalmente nas dependências físicas da contratante. Além de que, toda a responsabilidade de gestão, monitoramento, o controle e a supervisão sob os cuidados diretos da equipe técnica interna.

Por se tratar da aquisição de um produto, ao final do contrato, o *software*/ferramenta adquirido estará ainda cumprindo a sua função inicial, apenas deixará de receber atualizações de segurança, pacotes de correções e implementação de novas funcionalidades.

Além de tudo até aqui exposto, preconiza-se como melhor prática que, soluções ou ferramentas que se utilizam tecnologias de amostragem de fluxos de pacotes (*flows*), SNMP, e demais informações geradas pelo protocolo BGP, sejam disponibilizadas localmente no ambiente, isto é, na origem onde estas informações estão sendo coletadas, a fim de manter a integridade dos dados, mitigar atrasos entre o tempo de propagação do conteúdo até o seu destino (*delay*) e questões relacionadas à segurança da informação, uma vez que os dados coletados para análise não devem ser transportados em meios públicos, mesmo sendo previamente criptografados.

## IDENTIFICAÇÃO DAS SOLUÇÕES

| Id | Descrição da solução - Grupo1 |
|---|---|
| 1 | **Aquisição** de roteadores BGP (*Border Gateway Protocol*) com garantia de 60 (sessenta) meses. |
| 2 | **Utilização** do Firewall como roteadores BGP (*Border Gateway Protocol*). |
| 3 | **Aluguel** de roteadores BGP (*Border Gateway Protocol*) das empresas contratadas. |

## ANÁLISE COMPARATIVA DAS SOLUÇÕES

| Id | Descrição da solução - Grupo1 |
|---|---|
| 1 | **Aquisição** de roteadores BGP (*Border Gateway Protocol*) com garantia de 60 (sessenta) meses. |
| 2 | **Utilização** do Firewall como roteadores BGP (*Border Gateway Protocol*). |
| 3 | **Aluguel** de roteadores BGP (*Border Gateway Protocol*) das empresas contratadas. |

Em análise comparativa referente ao **Grupo1, a Solução 1** é a opção viável para Presidência da República, pois viabiliza a adoção da Topologia de Rede proposta no **Item 7. Necessidades de Negócios da Solução** deste E.T.P., com a dupla abordagem de equipamentos de redes, bem como viabiliza a manutenção, operação e gerenciamento direto dos técnicos especializados da Presidência da República nos equipamentos adquiridos, possibilitando a pronta tomada de decisão e ação em eventos de riscos ou falhas.

A **Solução 2 não é tecnicamente viável**, pois a solução de Firewall não suportaria a necessidade da Presidência da República, pois não foi projetado para executar todas as funcionalidades específicas requerida por um roteador BGP, mas que eventualmente poderia ser utilizados como um *backup* em caso de falhas, o que será superado com a adoção da Topologia de Rede proposta no **Item 7. Necessidades de Negócios da Solução** deste E.T.P.

A **Solução 3 não viabiliza a adoção da Topologia de Rede** proposta no **Item 7. Necessidades de Negócios da Solução** deste E.T.P., com a dupla abordagem de equipamentos de redes e não viabiliza a manutenção, operação e gerenciamento direto dos técnicos especializados da Presidência da República no equipamento, o que restringe a decisão e tomada de ação em eventos de riscos ou falhas.

| Requisito | Solução | Sim | Não | Não se aplica |
|---|---|---|---|---|
| A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública? | Solução 1 | X | | |
| | Solução 2 | | X | |
| | Solução 3 | X | | |
| A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software) | Solução 1 | | | X |
| | Solução 2 | | | X |
| | Solução 3 | | | X |
| A Solução é composta por software livre ou software público? (quando se tratar de software) | Solução 1 | | | X |
| | Solução 2 | | | X |
| | Solução 3 | | | X |
| A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG? | Solução 1 | | | X |
| | Solução 2 | | | X |
| | Solução 3 | | | X |
| A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital) | Solução 1 | | | X |
| | Solução 2 | | | X |

| | | | | |
|---|---|---|---|---|
| | Solução 3 | | | X |
| 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 | | | X |
| | Solução 3 | | | X |

| Id | Descrição da solução - Grupo2 |
|---|---|
| 1 | **Locação** de *software*/ferramenta de análise de tráfego de roteamento BGP, com garantia para 60 (sessenta) meses, como um serviço com período de uso pré-definido (Modalidade *Software as a Service - Subscription*). |
| 2 | **Locação** de software/ferramenta de análise de tráfego de roteamento BGP, com garantia para 60 (sessenta) meses, com um serviço em nuvem (Modalidade *Software as a Service - Cloud*). |
| 3 | **Aquisição** do software/ferramenta de análise de tráfego de roteamento BGP, com garantia para 60 (sessenta) meses, para ser disponibilizado/instalado na infraestrutura local, como um produto com licenciamento perpétuo - Modalidade *On Premise* . |

| Id | Descrição da solução - Grupo2 |
|---|---|
| 2 | **Locação** de software/ferramenta de análise de tráfego de roteamento BGP, com garantis para 60 (sessenta) meses, com um serviço em nuvem (Modalidade *Software as a Service - Cloud*) - A **Solução 2** não é tecnicamente viável, pois, a modalidade não preconiza as melhores práticas que orientam e recomendam que soluções que se utilizam tecnologias de amostragem de fluxos de pacotes (*flows*), SNMP, e demais informações geradas pelo protocolo BGP, sejam disponibilizadas na origem onde estas informações estão sendo coletadas, a fim de manter a integridade dos dados, mitigar atrasos entre o tempo de propagação do conteúdo até o seu destino (*delay*) e questões relacionadas à segurança da informação, uma vez que os dados coletados para análise não devem ser transportados em meios públicos, mesmo sendo previamente criptografados.<br><br>Destaca-se ainda, em relação a **Solução 2**, que o tráfego dos dados e informações sensíveis serão direcionadas para a nuvem (*Cloud*) do fabricante que é, por definição, Nuvem Pública.<br><br>Nesse contexto, a alternativa em pauta deve ser analisada também em consonância com as restrições estabelecidas no contexto dos normativos que determinam a sua adoção, visto que envolvem a segurança nacional na forma de potencial exposição de dados confidenciais. |

Entre esses normativos, o documento “Boas práticas, orientações e vedações para contratação de Serviços de Computação em Nuvem” – elaborado pela SLTI/MPOG e vinculado à Portaria MP/STI nº 20, de 14 de junho de 2016 – apresenta como pré-requisito, no parágrafo 2, que:

Compete à autoridade máxima do órgão, com apoio do Comitê de Governança Digital, do Comitê de Segurança da Informação e Comunicações e do Comitê Estratégico de Tecnologia da Informação, a definição dos serviços de Tecnologia da Informação e Comunicação (TIC), no todo ou em parte, que possam comprometer a segurança nacional.

Desse modo, para adotar a arquitetura de nuvem, conforme determinação do referido documento, seria necessário identificar previamente os sistemas que não comprometeriam a segurança nacional.

Até a presente data, trata-se de um trabalho ainda em definição e, portanto, não seria possível adotar esta alternativa até a publicação formal dos serviços de TIC que se enquadram no referido normativo.

## ANÁLISE COMPARATIVA DAS SOLUÇÕES

Em análise comparativa, a **Solução 3** é a opção **viável** para Presidência da República, pois nesta modalidade poderemos garantir a efetivação dos mesmos níveis de segurança e sigilo de dados, atualmente implementados nos ativos e serviços ofertados pela Presidência da República, visto que os componentes serão instalados e disponibilizados localmente, isto é, totalmente nas dependências físicas da contratante. Além de que, toda a responsabilidade de gestão, monitoramento, o controle e a supervisão sob os cuidados diretos da equipe técnica da Presidência da República.

A escolha por essa solução viabilizará o atendimento as determinações e recomendações da administração pública, com relação aos requisitos de segurança da informação, especificamente aos assuntos constantes na Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, e suas Normas Complementares. Cabe ainda ressalta, que com aquisição da referida solução, buscaremos a mitigação dos riscos de descumprimentos de questões relacionadas a desconformidade com as leis e normas locais, uma vez que os nossos dados classificados não estarão hospedados locais remotos e até em outros países, onde as leis existentes podem entrar em conflito com os interesses públicos do governo brasileiro, como o “*Patriot Act*”, vigente nos Estados Unidos, ou o “ *Data Protection Directive*” da UE, que restringe o fluxo de dados além das fronteiras da comunidade.

Além de tudo até aqui exposto, preconiza-se como melhor prática que, soluções ou ferramentas que se utilizam tecnologias de amostragem de fluxos de pacotes (*flows*), SNMP, e demais informações geradas pelo protocolo BGP, sejam disponibilizadas localmente no ambiente, isto é, na origem onde estas informações estão sendo coletadas, a fim de manter a integridade dos dados, mitigar atrasos entre o tempo de propagação do conteúdo até o seu destino (*delay*) e questões relacionadas à segurança da informação, uma vez que os dados coletados para análise não devem ser transportados em meios públicos, mesmo sendo previamente criptografados.

A **Solução 1 é financeiramente inviável**, pois, ao final do contrato de uso o acesso à solução será imediatamente interrompido, bem como os benefícios de segurança e controle que motivaram a sua contratação. Ao findar o contrato, as funcionalidades e demais serviços serão totalmente descontinuados, não podendo ser utilizados nem de modo parcial/limitado, pois a infraestrutura (servidores e software), serão completamente removidos do ambiente do CONTRATANTE pela CONTRATADA. Como resultado, todas as funcionalidades, até mesmo as mais básicas serão descontinuadas/canceladas, sendo que o mesmo não ocorreria com a aquisição de um produto com licenciamento perpétuo - Modalidade *On Premise.* Como já exemplificado, nesta modalidade, ao final do contrato, apenas os serviços de atualizações, suporte e garantia, seriam interrompidos, mas manteríamos as funcionalidades básicas da solução, bem como seus benefícios mais significativos.

A **Solução 2 é tecnicamente inviável**, pois não preconiza as melhores práticas que orientam e recomendam que soluções que se utilizam tecnologias de amostragem de fluxos de pacotes (*flows*), SNMP, e demais informações geradas pelo protocolo BGP, sejam disponibilizadas na origem onde estas informações estão sendo coletadas, a fim de manter a integridade dos dados, mitigar atrasos entre o tempo de propagação do conteúdo até o seu destino (*delay*) e questões relacionadas à segurança da informação, uma vez que os dados coletados para análise não devem ser transportados em meios públicos, mesmo sendo previamente criptografados.

Destaca-se ainda, em relação a **Solução 2**, que o tráfego dos dados e informações sensíveis serão direcionadas para a nuvem ( *Cloud*) do fabricante que é, por definição, Nuvem Publica.

Nesse contexto, a alternativa em pauta deve ser analisada também em consonância com as restrições estabelecidas no contexto dos normativos que determinam a sua adoção, visto que envolvem a segurança nacional na forma de potencial exposição de dados confidenciais.

Entre esses normativos, o documento “Boas práticas, orientações e vedações para contratação de Serviços de Computação em Nuvem” – elaborado pela SLTI/MPOG e vinculado à Portaria MP/STI nº 20, de 14 de junho de 2016 – apresenta como pré-requisito, no parágrafo 2, que:

Compete à autoridade máxima do órgão, com apoio do Comitê de Governança Digital, do Comitê de Segurança da Informação e Comunicações e do Comitê Estratégico de Tecnologia da Informação, a definição dos serviços de Tecnologia da Informação e Comunicação (TIC), no todo ou em parte, que possam comprometer a segurança nacional.

Desse modo, para adotar a arquitetura de nuvem, conforme determinação do referido documento, seria necessário identificar previamente os sistemas que não comprometeriam a segurança nacional.

Até a presente data, trata-se de um trabalho ainda em definição e, portanto, não seria possível adotar esta alternativa até a publicação formal dos serviços de TIC que se enquadram no referido normativo.

| Requisito - 3.2.2 | Solução | Sim | Não | Não se aplica |
|---|---|---|---|---|
| A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública? | Solução 1 | | | |
| | Solução 2 | | | |
| | Solução 3 | | | |
| A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software) | Solução 1 | | | X |
| | Solução 2 | | | X |
| | Solução 3 | | | X |
| A Solução é composta por software livre ou software público? (quando se tratar de software) | Solução 1 | | | X |
| | Solução 2 | | | X |
| | Solução 3 | | | X |

| | | | | |
|---|---|---|---|---|
| A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG? | Solução 1 | | | X |
| | Solução 2 | | | X |
| | Solução 3 | | | X |
| A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital) | Solução 1 | | | X |
| | Solução 2 | | | X |
| | Solução 3 | | | X |
| 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 | | | X |
| | Solução 3 | | | X |

## 9. Descrição da solução como um todo

| DESCRIÇÃO DA SOLUÇÃO |
|---|

| | |
|---|---|
| 1 | **Aquisição** de roteadores BGP (*Border Gateway Protocol*) com garantia de 60 (sessenta) meses. |

Em análise comparativa referente ao **Lote 1, a Solução 1** é a opção viável para Presidência da República, pois viabiliza a adoção da Topologia de Rede proposta no **Item 7. Necessidades de Negócios da Solução** deste E.T.P., com a dupla abordagem de equipamentos de redes, bem como viabiliza a manutenção, operação e gerenciamento direto dos técnicos especializados da Presidência da República nos equipamentos adquiridos, possibilitando a pronta tomada de decisão e ação em eventos de riscos ou falhas.

| Requisito | Solução | Sim | Não | Não se aplica |
|---|---|---|---|---|
| A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública? | Solução 1 | X | | |
| A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software) | Solução 1 | | | X |
| A Solução é composta por software livre ou software público? (quando se tratar de software) | Solução 1 | | | X |
| A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG? | Solução 1 | | | X |
| A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital) | Solução 1 | | | X |
| 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 |

## 10. Estimativa das Quantidades a serem Contratadas

| ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS |
|---|

Aquisição de 02 (dois) roteadores BGP (Border Gateway Protocol) com garantia de 60 (sessenta) meses, incluindo licenças perpétuas, suporte técnico por 12 (doze) meses, instalação e configuração dos equipamentos de modo que a Presidência da República do Brasil opere como Sistema Autônomo (AS), bem como a aquisição de solução/ferramenta de análise de tráfego e roteamento BGP para os objetos citados, com garantia de 60 (sessenta) meses, licenças perpétuas, suporte técnico por 12 (doze) meses, instalação, configuração, além de treinamentos especializados para ambas as soluções.

| GRUPO | ITEM | DESCRIÇÃO /ESPECIFICAÇÃO | UNIDADE DE MEDIDA | QUANTIDADE |
|---|---|---|---|---|
| 1 | 1 | ROTEADOR DE BORDA BGP COM GARANTIA, LICENÇAS E ATUALIZAÇÕES | Unidade | 02 |
| | **2** | SUPORTE TÉCNICO ON-SITE | Meses | 12 |

| | | | | |
|---|---|---|---|---|
| | **3** | TREINAMENTO ESPECIALIZADO | Treinamento | 01 |
| **2** | 1 | FERRAMENTA DE ANÁLISE DE TRÁFEGO E ROTEAMENTO BGP COM GARANTIA, LICENÇAS E ATUALIZAÇÕES | Unidade | 01 |
| | **2** | SUPORTE TÉCNICO ON-SITE | Meses | 12 |
| | **3** | TREINAMENTO ESPECIALIZADO | Treinamento | 01 |

*Os preços estimados na tabela acima serão os considerados como máximos para aceitação da proposta pela Presidência da República.

## 11. Estimativa do Valor da Contratação

**ANÁLISE COMPARATIVA DE CUSTOS (TCO)**

**DO PREÇO ESTIMADO E DA DOTAÇÃO ORÇAMENTÁRIA (observado o disposto nos arts. 20 e 21 da IN. SGD /ME nº 1/2019)**

O valor total da contratação está estimado em **R$ 923.423,00 (novecentos e vinte e três mil e quatrocentos e setenta e seis reais).**

No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento da União, para o exercício de 2021, na Unidade Gestora 110001, na classificação abaixo

| Conta | Sub | Título |
|---|---|---|
| 44.90.52 | 37 | Equipamentos de TIC - ativos de rede |
| 33.90.40 | 21 | Serviços Técnicos Profissionais de TIC |

**Descrição:**

Aquisição de 02 (dois) roteadores BGP (Border Gateway Protocol) com garantia de 60 (sessenta) meses, incluindo licenças perpétuas, suporte técnico por 12 (doze) meses, instalação e configuração dos equipamentos, bem como a aquisição de solução /ferramenta de análise de tráfego e roteamento BGP para os objetos citados, com garantia de 60 (sessenta) meses, licenças perpétuas, suporte técnico por 12 (doze) meses, instalação, configuração, além de treinamentos especializados para ambas as soluções.

**Custo Total – Memória de Cálculo**

**Pesquisa de Preço:**

01) **Painel de Preço** - Foi realizada pesquisa de preço no Painel de Preço utilizando o CATMAT 104620, em que foram identificados diversos registros de aquisições, contudo, após análise foram identificado apenas 1 edital de aquisição de roteadores, sendo este a Contratação Similar identificada (Pregão eletrônico nº 22/2020/TRT 8ª Região) que não atende as especificações técnicas mínimas requeridas por essa Presidência da República. Os demais valores identificados no Painel de Preço não atendem as especificações da aquisição da Presidência da República.

**Fornecedores** - Foram consultados diversos fornecedores de diferentes fabricantes. As propostas enviadas compõem o Mapa Comparativo de Pesquisa de Preço.

Diante do exposto, **considerando o critério de preço médio para fornecedor,** estima-se o **custo único total** da solução de **R$ 923.476,00 (novecentos e vinte e três mil e quatrocentos e setenta e seis reais),** obtido das diversas propostas comerciais coletadas pela Presidência da República, conforme o disposto na Planilha de Pesquisa de Preço.

**MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)**

| DESCRIÇÃO DA SOLUÇÃO | ESTIMATIVA DE TCO AO LONGO DOS ANOS | | | | | TOTAL |
|---|---|---|---|---|---|---|
| | ANO 2022 | ANO 2023 | ANO 2024 | ANO 2025 | ANO 2026 | |
| GRUPO 1 | R$ 782.726,00 | R$ 54.000,00 | R$ 54.000,00 | R$ 54.000,00 | R$ 54.000,00 | R$ 998.726,00 |
| GRUPO 2 | R$ 140.750,00 | R$ 30.000,00 | R$ 30.000,00 | R$ 30.000,00 | R$ 30.000,00 | R$ 260.750,00 |

**FONTE DE RECURSOS**

Tesouro Nacional - Fonte 100

## 12. Justificativa para o Parcelamento ou não da Solução

**INDIVISIBILIDADE DA SOLUÇÃO ESCOLHIDA**

Quanto a separação dos itens em dois grupos distintos, verifica-se que o objeto é composto por elementos independentes, que unidos formam um sistema cooperativo que, por suas características, deve funcionar de forma sincronizada, sob pena de comprometer o resultado esperado. Em outras palavras, a falta dos equipamentos ou da ferramenta de análise de tráfego, e ainda a instalação inadequada destes prejudicará todo o conjunto.

A separação em grupos distintos também se faz necessária com objetivo de atender a ampla concorrência entre os diversos fabricantes das soluções dos grupos, que deverão manter a interoperabilidade e a integração dos itens.

## 13. Contratações Correlatas e/ou Interdependentes

**CONTRATAÇÕES SIMILIMARES, CORRELATAS E/OU INTERDEPENDENTES**

Não foram encontradas soluções similares ou correlatas.

## 14. Alinhamento entre a Contratação e o Planejamento

**ALINHAMENTO ENTRE A CONTRATAÇÃO E O PLANEJAMENTO**

Destaca-se, na tabela abaixo, o alinhamento da contratação pretendida em relação aos instrumento de programação estratégica da Presidência da República*:*

| ALINHAMENTO AOS PLANOS ESTRATÉGICOS | |
|---|---|
| **ID** | **Objetivos Estratégicos** |
| 0E01 | Entregar soluções de TIC que agreguem valor estratégico |
| 0E02 | Viabilizar a entrega de serviços digitais para a sociedade |
| 0E04 | Buscar continuamente a satisfação do usuário dos serviços de TIC |

| | |
|---|---|
| 0E05 | Promover a inovação de soluções de TIC |
| 0E11 | Promover o processo contínuo de modernização da infraestrutura e serviços de TIC |
| 0E14 | Ampliar a capacidade de entrega dos serviços de TIC |

| ALINHAMENTO AO PDTIC (2020-2021) | | | |
|---|---|---|---|
| **ID** | **Ação do PDTIC** | **ID** | **Meta do PDTIC associada** |
| A23 | Ampliar a capacidade da rede de dados, voz e vídeo da PR | A23 | Capacidade da Rede ampliada e atualizada |
| A24 | Implantar serviço de comunicação unificada | A24 | Serviço implantado |
| A28 | Implantar infraestrutura própria de fibras ópticas, integrando o Palácio do Planalto, Anexos e complexo N2 ao Espaço Israel Pinheiro, IN, Pavilhão de Metas e as Residências Oficiais | A28 | Infraestrutura de fibras contratada e implantada |
| A33 | Atualizar infraestrutura tecnológica dos Palácios e Residências Oficiais, e dos Escritórios Regionais | A33 | Aquisições e contratações realizadas |
| A56 | Atualizar o parque de instrumentos de segurança eletrônica e de comunicações de aplicação nos ambientes de uso do PR | A56 | Equipamentos adquiridos |

| ALINHAMENTO AO PAC 2021 | |
|---|---|
| **Item** | **Descrição** |
| **1983** | ROTEADOR, TIPO USO ESCRITÓRIO, PROTOCOLO LAN TCP/IP, NAT, DHCP, DNS, PAP, CHAP, PROTOCOLO WAN TCP/IP, NAT, DHCP, DNS, PAP, CHAP, TENSÃO ALIMENTAÇÃO 110, CONECTORES RJ-45 E FIBRA ÓTICA, RECURSO SEGURANÇA FIREWALL INTEGRADO, PAP/CHAP, FILTRAGEM END E, RECURSO GERENCIAMENTO TELNET, CONSOLE, WEB, RECURSO ADICIONAL PADRÃO 19 POL, 1U E SUPORTE VPN, CARACTERÍSTICAS ADICIONAIS 4 PORTAS 10/100 BASE TX FAST ETHERNET E 1 PORTA, VELOCIDADE ROTEAMENTO 100 |

# 15. Resultados Pretendidos

**RESULTADOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO**

- **A contratação em comento pretende atingir os seguintes objetivos:**
  - Entregar soluções de TIC que agreguem valor estratégico.
  - Viabilizar a entrega de serviços digitais para a sociedade.
  - Buscar continuamente a satisfação do usuário dos serviços de TIC.
  - Promover a inovação de soluções de TIC.
  - Promover o processo contínuo de modernização da infraestrutura e serviços de TIC.
  - Ampliar a capacidade de entrega dos serviços de TIC.

O cumprimento dos supramencionados objetivos deve observar a discriminação técnica abaixo (em observância ao disposto no art. 14 da IN. SGD/ME nº 1/2019):

Aquisição de 02 (dois) roteadores BGP (*Border Gateway Protocol*), conjuntamente com uma solução/ferramenta de análise de tráfego e roteamento BGP, de modo que a Presidência da República do Brasil desempenhe com excelência e segurança as funções requeridas por um Sistema Autônomo (AS), nos termos do Documento de Oficialização da Demanda (DOD).

A especificação das necessidades e requisitos técnicos necessários - a serem contemplados pela aquisição em referência - encontra-se descrita, em sua integralidade, nos termos dos itens 2 e 4 do Termo de Referência.

# 16. Providências a serem Adotadas

**PROVIDÊNCIAS A SEREM ADOTADAS**

- Ainda no que tange à manutenção corretiva e evolutiva da solução: não há necessidade de ser prever recursos materiais, nem de se contratar qualquer serviço de mão-de-obra continuada, e, em relação às necessidades de recursos humanos.

# 17. Possíveis Impactos Ambientais

| IMPACTOS AMBIENTAIS |
|---|
| • Não se verifica, **no momento**, a necessidade de adequação do ambiente do contratante para a execução do objeto do contrato, bem como de alteração no que tange à sua respectiva infraestrutura tecnológica, elétrica, logística, espaço físico, mobiliário e demais necessidades previstas para a aquisição em comento. |

# 18. Soluções Inviáveis

| SOLUÇÕES INVIÁVEIS | |
|---|---|
| 2 | **Utilização** do Firewall como roteadores BGP (*Border Gateway Protocol*) - A **Solução 2** não é tecnicamente viável, pois a solução de Firewall não suportaria a necessidade da Presidência da República, pois não foi projetado para executar todas as funcionalidades específicas requerida por um roteador BGP, mas que eventualmente poderia ser utilizados como um *backup* em caso de falhas, o que será superado com a adoção da Topologia de Rede proposta no Item 1.1 deste E.T.P.<br><br>**Aluguel** de roteadores BGP (*Border Gateway Protocol*) das empresas contratadas - A **Solução 3** não viabiliza a adoção da Topologia de Rede proposta no Item 1.1 deste E.T.P., com a dupla abordagem de equipamentos de redes e não viabiliza a manutenção, operação e gerenciamento direto dos técnicos especializados da Presidência da República no equipamento, o que restringe a decisão e tomada de ação em eventos de riscos ou falhas. |
| 3 | **Aluguel** de roteadores BGP (*Border Gateway Protocol*) das empresas contratadas - A **Solução 3** não viabiliza a adoção da Topologia de Rede proposta no Item 1.1 deste E.T.P., com a dupla abordagem de equipamentos de redes e não viabiliza a manutenção, operação e gerenciamento direto dos técnicos especializados da Presidência da República no equipamento, o que restringe a decisão e tomada de ação em eventos de riscos ou falhas. |

| Id | 4.2 - Descrição da solução - Grupo 2 |
|---|---|
| | **Locação** de *software*/ferramenta de análise de tráfego de roteamento BGP, com suporte e licença para 60 (sessenta) meses, como um serviço com período de uso pré-definido (Modalidade *Software as a Service - Subscription*) - A **Solução 1 é financeiramente inviável**, pois, ao final do contrato de uso o acesso à solução será imediatamente |

| | |
|---|---|
| 1 | interrompido, bem como os benefícios de segurança e controle que motivaram a sua contratação. Ao findar o contrato, as funcionalidades e demais serviços serão totalmente descontinuados, não podendo ser utilizados nem de modo parcial /limitado, pois a infraestrutura (servidores e software), serão completamente removidos do ambiente do CONTRATANTE pela CONTRATADA. Como resultado, todas as funcionalidades, até mesmo as mais básicas serão descontinuadas/canceladas, sendo que o mesmo não ocorreria com a aquisição de um produto com licenciamento perpétuo - Modalidade *On Premise.* Como já exemplificado, nesta modalidade, ao final do contrato, apenas os serviços de atualizações, suporte e garantia, seriam interrompidos, mas manteríamos as funcionalidades básicas da solução, bem como seus benefícios mais significativos. |
| 2 | **Locação** de software/ferramenta de análise de tráfego de roteamento BGP, com suporte e licença para 60 (sessenta) meses, com um serviço em nuvem (Modalidade *Software as a Service - Cloud*) - A **Solução 2 não é tecnicamente viável**, pois, a modalidade não preconiza as melhores práticas que orientam e recomendam que soluções que se utilizam tecnologias de amostragem de fluxos de pacotes (*flows*), SNMP, e demais informações geradas pelo protocolo BGP, sejam disponibilizadas na origem onde estas informações estão sendo coletadas, a fim de manter a integridade dos dados, mitigar atrasos entre o tempo de propagação do conteúdo até o seu destino (*delay*) e questões relacionadas à segurança da informação, uma vez que os dados coletados para análise não devem ser transportados em meios públicos, mesmo sendo previamente criptografados.<br><br>Destaca-se ainda, em relação a **Solução 2**, que o tráfego dos dados e informações sensíveis serão direcionadas para a nuvem (*Cloud*) do fabricante que é, por definição, Nuvem Publica.<br><br>Nesse contexto, a alternativa em pauta deve ser analisada também em consonância com as restrições estabelecidas no contexto dos normativos que determinam a sua adoção, visto que envolvem a segurança nacional na forma de potencial exposição de dados confidenciais.<br><br>Entre esses normativos, o documento “Boas práticas, orientações e vedações para contratação de Serviços de Computação em Nuvem” – elaborado pela SLTI/MPOG e vinculado à Portaria MP/STI nº 20, de 14 de junho de 2016 – apresenta como pré-requisito, no parágrafo 2, que:<br><br>Compete à autoridade máxima do órgão, com apoio do Comitê de Governança Digital, do Comitê de Segurança da Informação e Comunicações e do Comitê Estratégico de Tecnologia da Informação, a definição dos serviços de Tecnologia da Informação e Comunicação (TIC), no todo ou em parte, que possam comprometer a segurança nacional.<br><br>Desse modo, para adotar a arquitetura de nuvem, conforme determinação do referido documento, seria necessário identificar previamente os sistemas que não comprometeriam a segurança nacional.<br><br>Até a presente data, trata-se de um trabalho ainda em definição e, portanto, não seria possível adotar esta alternativa até a publicação formal dos serviços de TIC que se enquadram no referido normativo. |

## 19. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

### 19.1. Justificativa da Viabilidade

O presente estudo técnico preliminar evidenciou que a contratação garantirá o atendimento às necessidades, sendo viável do ponto de vista técnico e de negócio.

## 20. Responsáveis

A Equipe de Planejamento da Contratação foi instituída pela Portaria nº 311, de 09 de novembro de 2021 - SEI 2997688. Conforme o § 2º do Art. 11 da IN

ADRIANO FRANCO BEZERRA
INTEGRANTE REQUISITANTE

A Equipe de Planejamento da Contratação foi instituída pela Portaria nº 311, de 09 de novembro de 2021 - SEI 2997688. Conforme o § 2º do Art. 11 da IN

MARCELO FERREIRA PINHEIRO
INTEGRANTE TÉCNICO

Portaria nº 270 de 13 de outubro de 2021.

CARLOS AUGUSTO PISSUTTI
DIRETOR DE TECNOLOGIA SUBSTITUTO