

Estudo Técnico Preliminar 46/2020

1. Informações Básicas

Número do processo: 60220.000667/2019-68

2. Introdução

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, de 05 AGO 2020, da SC-1.3 (2548898), bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

Referência: Art. 11 da IN SGD/ME nº 1/2019.

3. Descrição da necessidade

3.1 – ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS - (IN. 01/2019, Art. 14)

A Tabela 2.1 apresenta estimativa do quantitativo de bens e serviços necessários para a composição da solução a ser contratada, bem como para sua sustentação, o qual está dimensionado e justificado em atenção aos equipamentos já adquiridos, aos pontos que precisam da garantia do sigilo da informação (organizações e terminais do SISCOMIS que compõem o SISMC²) e ao tamanho da equipe técnica do MD.

Tabela 3.1. estimativa da demanda

Gp	Item	Bem/Serviço	Descrição	Unid
1	1	Módulo de Segurança Criptográfico (100 Mbps) com garantia, instalação e configuração	Conforme a subseção 1.2.1 deste estudo	Un
	2	Módulo de Segurança Criptográfico (1 Gbps) com garantia, instalação e configuração	Conforme a subseção 1.2.1 deste estudo e visando o acesso aos futuros <i>datacenters</i> do SISMC ² .	Un
2	3	Instalação e configuração do roteador CISCO ASR1001-X /K9	Conforme a subseção 1.2.2 e 1.2.5 deste estudo	Un
	4	Instalação e configuração do roteador CISCO ISR 4451/K9		Un
	5	Instalação e configuração do roteador CISCO ISR 4431 /K9 ou ISR 4331/K9		Un

6	Instalação e configuração do Switch CISCO Catalyst C9200L		Un
7	Serviço de Suporte Técnico para a ROD por 12 meses	Conforme a subseção 1.2.4 deste estudo	Serv
8	Curso 300-501 SPCOR : Implementing and Operating Cisco Service Provider Network Core Technologies	Conforme a subseção 1.2.3 deste estudo	Por pess
9	Curso 300-510 SPRI : Implementing Cisco Service Provider Advanced Routing Solutions		Por pess
10	Curso 300-515 SPVI : Implementing Cisco Service Provider VPN Services (SPVI)		Por pess
11	Curso 350-701 SCOR : Implementing and Operating Cisco Security Core Technologies (SCOR)		Por pess
12	Curso 350-801 CLCOR : Implementing and Operating Cisco Collaboration Core Technologies (CLCOR).		Por pess

Outras justificativas para a presente estimativa encontram-se no APÊNDICE XI deste estudo.

4. Área requisitante

Área Requisitante	Responsável
Subchefia de Comando e Controle (SC-1)	Cel EB CLAUBER GUIMARÃES RÊGO

5. Descrição dos Requisitos da Contratação

5.1 – DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS – (IN. 01/2019, art. 11, Inciso I).
5.1.1 - Identificação das necessidades de negócio (IN. 01/2019, art. 16, inciso I, alínea “a”)
<p>Como introdução, é importante pontuar que existe um imenso arcabouço legal e normativo que definem características específicas e peculiares à Defesa Nacional, dado ainda, dentre outros, a necessidade de um rigor a respeito à segurança da informação, como (e não limitado):</p> <ul style="list-style-type: none"> • a Política Nacional de Defesa (PND) e a Estratégia Nacional de Defesa (END); • a Lei Nº 12.598, de 21 de março de 2012; • o Decreto Nº 9.637, de 26 de dezembro de 2018; e • as normas do GSI, amparadas pelo decreto supra, que norteiam, combinadas com a lei supra, a aquisição do Módulo de Segurança Criptográfico (MSC) pretendido pela SC-1.

É mister expor que o EMCFA está conduzindo um **grande programa de Tecnologia e Segurança da Informação e Comunicações** (TIC e SIC) no qual já foram investidos cerca de R\$ 23 milhões (LOA 2019 e LOA 2020) e cujas etapas previstas nos cronogramas físico-financeiros de execução de alguns contratos dependem, em grande parte, do andamento deste TLE;

O aludido programa é composto por uma miríade de projetos, sendo que um deles, intitulado Cinturão de Defesa Cibernética, possui subprojetos, que foram enumerados sob a metodologia (ou *framework*) de segurança em camadas, cujo planejamento abarca todas essas camadas;

O projeto Cinturão de Defesa Cibernética possui os seguintes objetivos:

- propiciar comunicações seguras, com algoritmo criptográfico de Estado, a todos os elos da Etta Mi D, podendo serem estendidas às operações interagência e ainda interagir com organizações nacionais ou internacionais, militares ou civis (nível 3);
- assegurar a criptografia e a certificação dos dados antes de adentrar na Rede de Passagem (níveis 4 a 7);
- evitar ataques de Brute Force, DDoS, Phishing, Malware ou Man-in-the-Middle (níveis 4 a 7);
- Capacitar o provimento seguro de telefonia, videoconferência e transmissão de dados através da internet, ampliando a capilaridade das comunicações entre os entes integrantes da Etta Mi D no âmbito do SISMC² (níveis 5 a 7);
- autenticação e gestão segura de identidade, inclusive aos usuários móveis (níveis 5 a 7);
- garantir a inviolabilidade da informação na sua gênese (nível 7); e
- garantir a conformidade com as exigências da Lei Nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD - nível 7).

As necessidades de negócio sob análise deste estudo estão definidas nos seguintes documentos:

- a. Termo de Licitação Especial (TLE) (2491066), constante no Apêndice I, que foi deliberado na 31ª Reunião Deliberativa da Comissão Mista da Indústria da Defesa (RD-CMID), realizada em 30 JUL 2020; e
- b. Documento de Oficialização da Demanda (DOD), de 05 AGO 2020, da SC-1.3 (2548898), constante no Apêndice V.

O objeto do TLE e do DOD está enunciado a seguir:

*"Contratação de EED para prover o fornecimento, instalação e configuração de PED Módulo de Segurança Criptográfico (HSM - Hardware Security Module) ASI-HSM e a instalação e configuração de equipamentos (ativos) de interconexão de rede, já adquiridos, em locais a serem determinados, para atualização da Rede Operacional de Defesa (ROD), visando a implantação da Rede de Passagem, contemplando um Sistema Criptográfico de Tráfego de Voz e Dados, e Rede IP Fixa, que obrigatoriamente deve atender aos requisitos de **inserção de Algoritmo Criptográfico de Estado**."*

Diante dessa necessidade, é imperioso que a ROD, principal elemento a ser ajustada por meio da solução desejada e já caracterizada nos documentos supracitados, possua a capacidade de comutar **com segurança** (garantia do sigilo) os dados que contêm as informações sigilosas tramitadas em Operações Conjuntas, em Operações Interagências e em nível estratégico. Entretanto, a aludida capacidade **não está implementada**.

Assim, é preciso, conforme também definido nos aludidos documentos, que a nova arquitetura da ROD execute criptografia **com algoritmo de Estado** por intermédio sobre túneis seguros entre equipamentos de interconexão dispostos nos enlaces de uma rede privada e pública, esta podendo ser a internet ou uma contratada, sobre as quais é assentada a rede de defesa.

Por fim, espera-se, com a conclusão da contratação em questão, alcançar os seguintes resultados e benefícios:

- Propiciar enlaces seguros a todos os elos da Estrutura Militar de Defesa (Etta Mi D), atendendo aos requisitos estabelecidos na legislação vigente;
- Atualizar a topologia da ROD em proveito das atuais demandas operacionais e hipóteses de emprego;
- Atualizar os equipamentos de interconexão da ROD;
- Implementar e manter atualizadas as regras de segurança em função das ameaças cibernéticas e do enquadramento legal;
- Permitir o gerenciamento (monitoramento e configuração) ativo de todos os equipamentos envolvidos;
- Racionalização na distribuição e emprego dos equipamentos de TIC;
- Fornecer à ROD a capacidade de geração de alertas de tentativas de intrusão, utilização de ferramentas de gestão de vulnerabilidades, implementação de ferramentas de criptografias com capacidades para cifrar enlaces completos, enlaces de usuários e dispositivos móveis (*desktops*, *notebooks* e *smartphones*) e capacidade para estabelecer ambientes seguros sem fios, por intermédio do uso de criptografia; e
- Ter a possibilidade de realizar operações de gerenciamento e operação do sistema de comunicações criptográficas de forma eficiente e independente da empresa contratada.

5.2 - Identificação das necessidades funcionais e tecnológicos (IN. 01/2019, art. 16, inciso I, alínea “a”)

Inicialmente, para fins de simplificação, define-se:

- **Nova ROD:** solução de TI a ser obtida que atualizará a atual Rede Operacional de Defesa (ROD), visando a implantação da
- **Solução MSC:** solução de TI a ser obtida por meio do fornecimento, instalação e configuração dos Módulos de Segurança (sobre a Nova ROD, definindo um Sistema Criptográfico de Tráfego de Dados sobre uma rede IP, o qual obrigatoriamente d de Estado; e
- **ROD Segura:** é a composição das soluções **Nova ROD** e **Solução MSC**.

Avaliando o objeto do TLE e DOD com e os respectivos resultados e benefícios esperados, e traduzindo para os **aspectos funcionais** que compõem a lista de aquisição de bens e serviços para atender a demanda do negócio (itens 1 a 6 da tabela 2.1):

I - Fornecedor, instalação e configuração de PED Módulo de Segurança Criptográfico, sendo necessária a transferência de conhe

II - Instalação e configuração de equipamentos (ativos) de interconexão de rede, já adquiridos, em locais a serem determinados, para Passagem, sendo também necessária a transferência de conhecimento.

Conforme também enunciado pelo objeto em epígrafe, cabe ainda destacar que o **item 'II'** supra:

- deve contemplar um "Sistema Criptográfico de Tráfego de Voz e Dados, e Rede IP Fixa, que obrigatoriamente deve atender Esse sistema é consubstanciado pelo **item 'I'** supra, o que será elucidado mais adiante; e
- trata de um serviços sobre equipamentos **já adquiridos**. Tais equipamentos são fabricados pela empresa americana Cisco S

Ademais, há benefícios esperados pelo negócio relacionados a **necessidade de uma rígida continuidade da solução de TI**, mesmo MD, conforme já registrado no TLE e DOD supratranscritos. Diante disso tudo, projeta-se então pelo menos mais dois itens ou grup (itens 7 a 12 da tabela 2.1):

III - capacitação avançada para a equipe técnica do MD responsável pelo planejamento, operação e manutenção da Nova ROD, senci correlacionados (itens 8 a 12 da tabela 2.1);

IV - contratação de empresa para suporte à Nova ROD, a qual apoiará tecnicamente a equipe do MD; e

V - adoção de um Sistema de Monitoramento de Rede para a Nova ROD, com funcionalidades avançadas, visando uma acurada sup

Outrossim, é imperioso, dentro desse contexto, a devida **atualização** do presente e do futuro sistema de monitoramento da ROD Seg adequada atuação da equipe que opera a ROD. Felizmente, dado o contexto tecnológico e os equipamentos adquiridos, essa atualiza

Ademais, alerta-se, além do mais, pela indispensabilidade da celebração do Termo de Compromisso e Manutenção de Sigilo (TCM) vencedoras do certame à respeito deste estudo, no intuito de garantir, na forma da lei, o sigilo das informações que envolvem a pres

Diante do exposto acima, foram exaradas as ESPECIFICAÇÕES TÉCNICAS DA ROD SEGURA, constante no APÊNDICE XI ap tecnológicos, como arquitetura da solução, forma de execução de projeto, regras para implantação, vigência de garantia, processos c profissional e de formação da equipe, formatação da metodologia de trabalho, controles para a segurança da informação e demais re

Adiante, serão enunciados as necessidades tecnológicas para esses quatro itens ora identificados.

5.2.1 - Módulo de Segurança Criptográfico

O Módulo de Segurança Criptográfico (MSC), do inglês *Hardware Security Module* (HSM), é o componente da solução de TI a ser e os terminais do SISCOMIS que compõem o SISMC², de forma transparente para os usuários, adotando a criptografia com **algorit** na subseção 1.1 supra e nos documentos que antecedem este estudo. Assim, o sigilo das informações é garantido quando estas trafe MSC, caracterizam a **Solução MSC**.

Para a construção virtual de um túnel seguro, cabe ressaltar que:

- há dependência ao menos de um par MSC, sendo imprescindível a compatibilidade entre eles dos parâmetros de comunicaç
- um par HSM, que define um ponto A e um ponto B localizados remotamente e em posições distintas, pode implantar vários tráfegar sempre de A para B e vice-versa, não havendo possibilidade de que essa informação criptografada seja entregue a
- é independente da rede sobre o qual é assentado, sendo apenas necessário o conhecimento e a alcançabilidade do endereço I

Dada a característica diferenciada da ROD, e em atenção a legislação vigente, em especial as NC 07 e NC 09/IN01/DSIC/GSI/PR, a comunicações sobre a rede de defesa precisam estar criptografadas, ou seja, é imperioso construir os túneis seguros em todos os tipc

- enlaces satelitais com frequência própria;
- enlaces satelitais com frequência alugada;
- enlaces sobre uma rede pública;
- enlaces em meio confinado sobre uma rede privada;
- enlaces em meio não-confinado sobre uma rede privada; e
- internet.

Ademais, cabe reforçar ainda que, para atender os requisitos estratégicos e a legislação vigente, o MSC deve ainda:

- ser um PED com 100% (cem por cento) de conteúdo nacional para algoritmo criptográfico e com o mínimo de 90% (noventa por cento) de conteúdo nacional para o hardware;
- abarcar o **algoritmo de Estado** conforme definido pela NC 09/IN01/DSIC/GSI/PR, de 15 de julho de 2014.

Cabe ainda reforçar que a solução MSC foca **apenas na camada de nível 3** de segurança, e não as demais, as quais são objetos de c

Concluindo, observa-se que esses módulos, desde que sejam PED contemplados com algoritmo de Estado, são necessários e se comunicam entre si através de um canal de comunicações de uma rede pública.

5.2.2 - Instalação e configuração de equipamentos de interconexão de rede já adquiridos

Parte dos ativos de rede necessários ao estabelecimento da Nova ROD já foram adquiridos em 2019 e estão em processo de recebimento e à sua futura distribuição nas diversas localidades do Território Nacional de frente à carência de mão de obra especializada e disponibilidade especializada para sua instalação, configuração e implementação de dispositivos de segurança (criptografia) de rede, desde que atendidos os seguintes requisitos:

- atualizar a topologia da ROD;
- assegurar a proteção cibernética adequada à ROD após essa atualização;
- permitir o gerenciamento e monitoramento dos equipamentos envolvidos; e
- implantar a Rede de Passagem, definida no RELATÓRIO N° 3/SC-1.3/SC-1/CHOC/EMCFA, de 7 de outubro de 2016 (15:00h), que estabelece a criação de uma rede central ou CORE) entre o MD e as Forças, cuja finalidade é o encaminhamento seguro, flexível e versátil de pacotes IPv4 e IPv6 entre o MD e as Forças e pelas redes internas do MD, uma operacional e a outra administrativa. Essa rede, que está ilustrada na Figura 1.1, será composta por:
 - roteadores de núcleo de rede (roteadores CORE);
 - enlaces entre os roteadores CORE; e
 - enlaces entre os roteadores CORE e os roteadores de borda (roteadores EDGE).

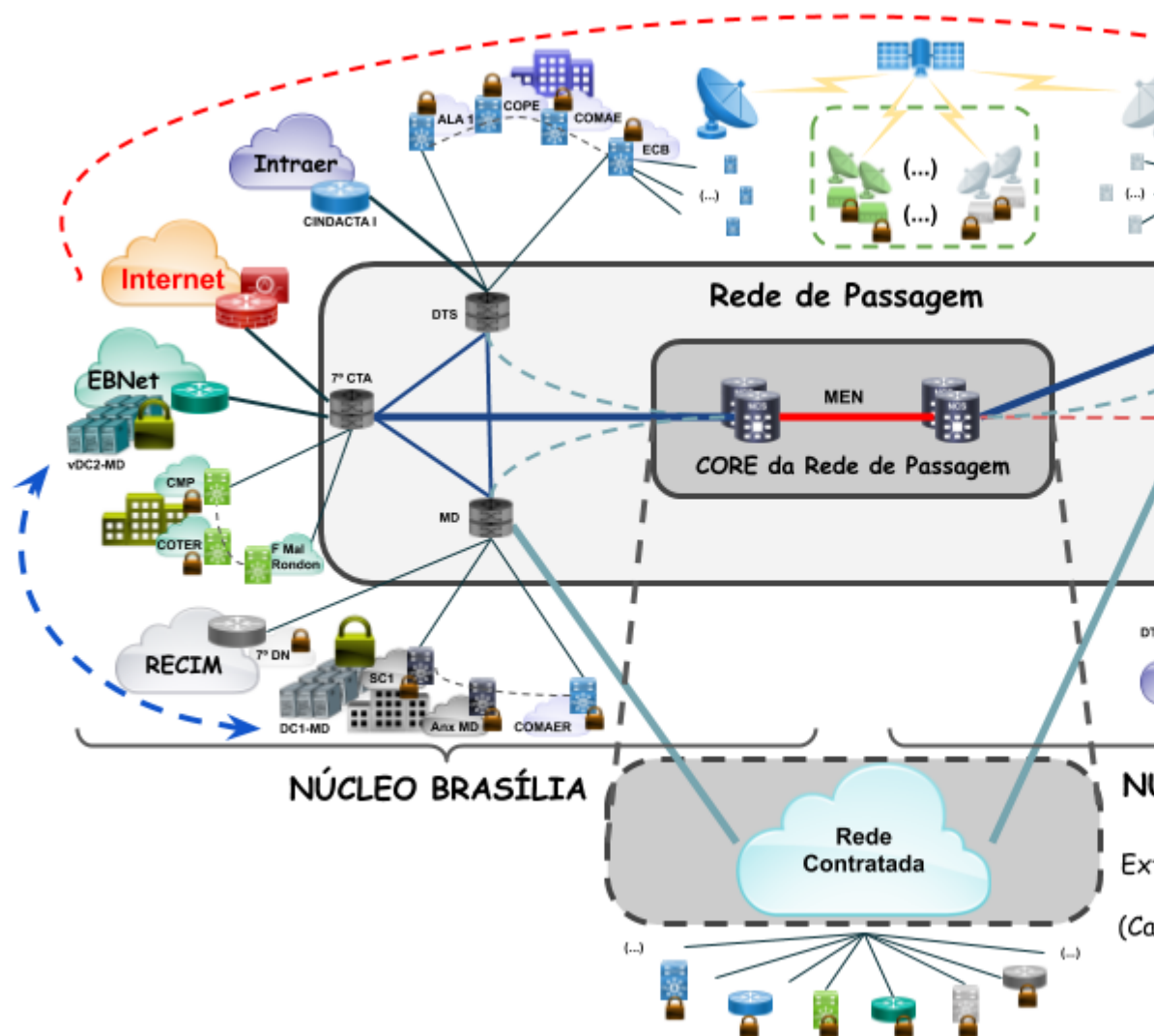


Figura 1.1 - Topologia conceitual da solução

5.2.3 - Capacitação avançada para a equipe técnica do MD

A capacitação avançada para a equipe técnica do MD visa sedimentar conhecimento técnico de alta complexidade, multidomínio, m capacitação deve ser executada antes da implantação, abrangendo dois importantes escopos:

- fundamentos que compõem a solução de TI, com simulação das técnicas, a fim de permitir aos técnicos o conhecimento basilar d
- aplicação desses fundamentos e simulação para cada técnica adotada na presente solução, com o intuito de transferir todo conheci
- compreensão avançada dos fundamentos e técnicas adotadas para a Nova ROD sob a ótica do fabricante do equipamento adquirid tecnologia implementada nesses equipamentos.

Assim, no contexto dos escopos 'a' e 'b', observa-se que:

- devem ser exercidos pelas empresas envolvidas com os itens 1.2.1 e 1.2.2 supra; e
- há a necessidade de estruturar laboratórios para a simulação da Nova ROD.

Na outra mão, no contexto do escopo 'c', observa-se que:

- a empresa envolvida não precisa celebrar o TCMS; e
- há a necessidade de realizar treinamentos oficiais homologados pelo do fabricante do equipamento adquirido.

Outrossim, sempre que possível e vantajoso à Administração, a capacitação deve ser realizada no formato Ensino à Distância (EAD), é mais econômico para administração, uma vez que os custos são reduzidos para as empresas e não há necessidade de passagens e diárias.

Por último, é importante ressaltar ainda a imprescindibilidade da preservação e da evolução do conhecimento, a fim de que este não se torne primordial e necessárias:

- certificar a equipe técnica do MD, pois a preparação para tal processo faz parte da metodologia para a sedimentação do conhecimento para tal certificação, e isso faz com que os especialistas do MD tenham contato com fundamentos da solução ora preterida, da infraestrutura e das técnicas que compõem a ROD; e
- prever capacitações periódicas para assegurar a continuidade e a perpetuação do conhecimento dentro do quadro de pessoal.

5.2.4 - Contratação de empresa para suporte à Nova ROD

Dadas a rigidez dos requisitos de manutenção, que refletem a necessidade de continuidade no fornecimento da Solução de TIC em cibersegurança disponível no MD, é imprescindível a contratação de empresa para suporte à ROD que apoiará tecnicamente a equipe do MD.

Essa empresa deve monitorar os eventos da ROD e, nos casos que possam comprometer a rede, agir prontamente para garantir a resiliência e os procedimentos que serão previstos em contrato.

5.2.5 - Sistema de Monitoramento de Rede para a ROD Segura

A atual ROD não dispõe de um adequado Sistema de Monitoramento de Rede, acarretando na adoção frequente de soluções de contingência. Isso promove respostas equivocadas e custosas, prejudicando a disponibilidade da rede e a experiência do usuário.

Assim, para a ROD Segura, é fundamental a adoção de um Sistema de Monitoramento de Rede com funcionalidades avançadas, correspondentes às que ocorrem na rede e garantindo uma rígida continuidade da ROD e, consequentemente, dos serviços de TI que apoiam o negócio atendido utilizando as funcionalidades de monitoramento dos equipamentos já adquiridos.

5.3 - Requisitos de capacitação (IN. 01/2019, art. 16, inciso I, alínea “b”, combinado com inciso II, alínea “e”) - TREINAMENTOS OFICIAIS DA CISCO

Dos itens 1 a 2 da tabela 2.1

5.3.1. Transferência de Conhecimento

5.3.1.1. Visando o entendimento das tecnologias e conceitos da solução, bem como permitir aos técnicos do CONTRATANTE a adequada operação da Solução MSC, a CONTRATADA deverá ministrar um curso específico para cada técnica/técnica

/software adotados e para cada tipo de equipamento adquirido, expondo, dentre outros, ficha técnica, fundamentos, conceitos, cenários de aplicação.

5.3.1.2. A transferência de conhecimento deverá ser:

5.3.1.2.1. presencial ou à distância preferencialmente;

5.3.1.2.1.1. Se presencial, ocorrerá na sede do MD ou outro local a ser definido em Brasília-DF.

5.3.1.2.1.1.1. A CONTRATADA deverá oferecer coffee break, 1 (uma) vez a cada 4 horas, todos os dias do treinamento, compatível com a quantidade de instruídos e instrutores, contendo, no mínimo: café, água mineral, refrigerante ou suco, biscoito salgado ou doce e sanduíche ou pão de queijo.

5.3.1.2.2. ministrado por técnicos certificados pelos fabricantes ou fornecedores dos equipamentos, técnica/software e outros recursos utilizados nas soluções tecnológicas empregadas pela CONTRATADA;

5.3.1.2.3. difundido para até 15 (quinze) pessoas.

5.3.1.3. Na semana anterior à passagem de conhecimento, a CONTRATADA deve disponibilizar um técnico para realizar a preparação do laboratório para a atividade.

5.3.1.4. O conteúdo programático deverá ser submetido à apreciação do CONTRATANTE para sua aprovação, devendo a CONTRATADA realizar as alterações solicitadas.

5.3.1.5. Deverá ser entregue, impresso e em formato digital:

5.3.1.5.1. o material didático do treinamento e todo material e documentação, preferencialmente em português, necessário a perfeita compreensão da solução instalada (slides, apostila de laboratório, documentação do projeto executado no CONTRATANTE);

5.3.1.5.2. a configuração detalhada e comentada dos equipamentos, inclusive com destaques técnicos acerca da solução.

5.3.1.6. A CONTRATADA assumirá todas as despesas e encargos inerente à transferência de conhecimento, compreendendo as despesas com hospedagem, transporte e alimentação dos instrutores e demais despesas/custos indiretos que incidirem sobre esta contratação.

5.3.1.7. A transferência de conhecimento deverá possuir carga horária mínima de 20 (vinte) horas com no máximo 4 horas diárias. Esse horário poderá ser flexibilizado a critério do CONTRATANTE.

5.3.1.8. Após a sua conclusão da transferência, deverá ser emitido certificado de participação, assinado pelo instrutor, para cada instruído.

5.3.1.9. Caso 50% (cinquenta por cento) ou mais da turma considere o treinamento regular ou insuficiente, a CONTRATADA deverá realizar outro treinamento sem ônus para o CONTRATANTE.

Dos itens 3 a 6 da tabela 2.1

5.3.2. Transferência de Conhecimento

5.3.2.1. O objetivo e as condições da transferência de conhecimento são as mesmas descritas no item 1.3.1. No entanto, deve ser dividido em módulos conforme descrito a seguir:

5.3.2.1.1. Módulo 1: focado na Nova ROD, devendo:

5.3.2.1.1.1. abranger todas as técnicas utilizadas para implantação dessa solução, com ambos os protocolos IPv4 e IPv6, focado também na integração com as redes das Forças, expondo ainda conceitos de IGP (OSPF e EIGRP), BGP, MPLS, CSC, IPSec, GETVPN, DMVPN, QoS e Engenharia de Tráfego;

5.3.2.1.1.2. conter atividades hands-on de todos os conceitos e técnicas supracita, considerando um dos laboratórios definidos no item 3.1.6.7;

- 5.3.2.1.1.3. Deve observar as regras previstas no ANO (vide 3.1.6.5.11); e
- 5.3.2.1.1.4. ter, no mínimo, 40 horas de duração, os quais serão divididos em, no máximo, 20 horas semanais, podendo haver flexibilização com a autorização do CONTRATANTE.
- 5.3.2.1.2. Módulo 2 – focado nos roteadores adquiridos, devendo:
- 5.3.2.1.2.1. incluir, no modelo hands-on, a operação, a configuração e o troubleshooting;
- 5.3.2.1.2.2. ter, no mínimo, 20 horas de duração, podendo haver flexibilização com a autorização do CONTRATANTE.
- 5.3.2.1.3. Módulo 3 – focado no Cisco ONE, devendo:
- 5.3.2.1.3.1. conter, inclusive no modelo hands-on, a implantação do Cisco ONE, Cisco DNA, Network-Based Application Recognition Version 2 (or Next Generation NBAR) e o uso do SWSS, visando principalmente, mas não limitado, o Cisco Application Visibility and Control (AVC), o Flexible NetFlow (FnF) e o Cisco Prime Infrastructure - Lifecycle License, com o intuito de garantir o adequado monitoramento dos equipamentos adquiridos;
- 5.3.2.1.3.2. ter, no mínimo, 20 horas de duração, podendo haver flexibilização com a autorização do CONTRATANTE.
- 5.3.2.1.4. Módulo 4 – focado na implantação do IPv6, devendo:
- 5.3.2.1.4.1. incluir, no modelo hands-on, a operação, a configuração e o troubleshooting;
- 5.3.2.1.4.2. abordar tópicos como MPLS com 6VPE;
- 5.3.2.1.4.3. abordar os estágios para implantação, sendo, dentre outros:
- 5.3.2.1.4.3.1. links com a Internet e nas estações de trabalho do pessoal técnico, com uso de proxies adequados;
- 5.3.2.1.4.3.2. servidores web ou e-mail e DNS;
- 5.3.2.1.4.3.3. equipamentos de segurança;
- 5.3.2.1.4.3.4. servidores corporativos, como de aplicação e de arquivos;
- 5.3.2.1.4.3.5. demais estações de trabalho;
- 5.3.2.1.4.3.6. dispositivos de VoIP e Videoconferência.
- 5.3.2.1.4.5. ter, no mínimo, 20 horas de duração, podendo haver flexibilização com a autorização do CONTRATANTE.

Não se aplica ao item 7 tendo em vista de se tratar de um serviço de suporte.

Dos itens 8 a 12 da tabela 2.1

- 5.3.3. Os treinamentos necessários da Cisco são:
- 5.3.3.1. Curso 300-501 SPCOR: Implementing and Operating Cisco Service Provider Network Core Technologies
- 5.3.3.2. Curso 300-510 SPRI: Implementing Cisco Service Provider Advanced Routing Solutions
- 5.3.3.3. Curso 300-515 SPVI: Implementing Cisco Service Provider VPN Services (SPVI)
- 5.3.3.4. Curso 350-701 SCOR: Implementing and Operating Cisco Security Core Technologies (SCOR)
- 5.3.3.5. Curso 350-801 CLCOR: Implementing and Operating Cisco Collaboration Core Technologies (LCOR).
- 5.3.3.6. Condições Gerais dos para a realização dos treinamentos
- 5.3.3.6.1. Os treinamentos devem ser oficiais do fabricante, podendo ser ministrados por um parceiro de treinamento certificado.
- 5.3.3.6.2. As ementas dos treinamentos devem conter as ementas oficiais do fabricante.
- 5.3.3.6.3. A carga horária dos treinamentos deve ser conforme estabelecida pelo fabricante, devendo o mesmo atestar que é compatível com a ementa definida.
- 5.3.3.6.4. Esses treinamentos devem ser realizados no formato Ensino à Distância (EAD), e as turmas terão a quantidade mínima de 9 alunos.
- 5.3.3.6.5. Os horários para início e término do treinamento serão definidos conforme disponibilidade do CONTRATANTE, incluindo a possibilidade de ser executado fora do horário normal de expediente.

5.3.3.6.6. O ambiente virtual dos treinamentos é de responsabilidade da CONTRATADA.

5.3.3.6.7. Deve haver hands-on, cujos laboratórios poderão ser baseados em equipamentos físicos ou virtuais.

5.3.3.6.8. Os instrutores dos treinamentos devem ser certificados pelo fabricante e qualificados nos treinamentos que vão ministrar, e seus certificados/comprovantes deverão ser entregues ao CONTRATANTE para fins de aprovação dos mesmos.

5.3.3.6.9. Os treinamentos devem ser ministrados em português.

5.3.3.6.10. É de responsabilidade da CONTRATADA fornecer, para cada aluno, todo material didático para a realização dos treinamentos, que deverá ser completo, no sentido de conter todas as informações necessárias ao perfeito entendimento dos tópicos abordados, de modo que os instruendos não necessitem de qualquer outra bibliografia de apoio.

5.3.3.6.11. Deverá ser emitido certificado de participação ao final do curso a cada participante, detalhando programa e carga horária.

5.3.3.6.12. Caso o treinamento não for satisfatório, mediante avaliação tempestiva e fundamentada, em relação à qualidade, a CONTRATADA deverá realizá-la novamente, sem ônus adicional ao CONTRATANTE.

5.3.3.7. Deve ser fornecido o voucher mais atual para certificação, com validade de, no mínimo, 6 (seis) meses, para cada aluno do treinamento contratado.

5.3.3.8. Pode ser fornecido o ambiente de e-learning CISCO, com instrutor em português, sendo que, nesse caso:

5.3.3.8.1. o instrutor deve usar o material do ambiente, inclusive os laboratórios;

5.3.3.8.2. não há a obrigatoriedade, por parte da CONTRATADA, de entregar o material impresso; e

5.3.3.8.3. o ambiente deve ficar disponível, para cada aluno, por no mínimo 6 (seis) meses e trinta dias antes do início do treinamento, podendo esses períodos serem flexibilizados pelo CONTRATANTE apenas.

5.5 - Requisitos legais (IN. 01/2019, art. 16, inciso I, alínea “c”)

5.5.1. Decreto-lei nº 200/1967, art. 10, § 7º - Dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências;

5.5.2. Lei nº 8.666/1993 - Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências;

5.5.3. Lei nº 12.598, de 21 de março de 2012 (somente para 1 e 2 da Tabela 2.1) - que estabelece normas especiais para as compras, as contratações e o desenvolvimento de produtos e de sistemas de defesa; e dispõe sobre regras de incentivo à área estratégica de defesa;

5.5.4. Lei nº 9.854/1999 - Altera dispositivos da Lei no 8.666, de 21 de junho de 1993, que regula o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências;

5.5.5. Decreto nº 9.637/2018 - Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional;

5.5.6. Instrução Normativa nº 5, de 26 de maio de 2017 – Dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional;

5.5.7. Instrução Normativa nº 1, de 4 de abril de 2019 - Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;

5.5.8. Portaria Normativa nº 2.327/MD, de 28 de outubro de 2015 2a Rev. - Política de Segurança da Informação para o Sistema Militar de Comando e Controle - MD31-P-03;

5.5.9. Portaria Normativa nº 18/MD de 2 de março de 2016 – Conceito Operacional para o Sistema Militar de Comando e Controle – MD31-S-02;

5.5.10. Decreto 7.892, de 23 de janeiro de 2013 - Regulamenta o Sistema de Registro de Preços previsto no art. 15 da Lei nº 8.666, de 21 de junho de 1993;

5.5.11. Lei 10.520, de 17 de julho de 2002 - instituiu a modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns; e

5.5.12. Decreto 10.024, de 20 de setembro de 2019 - regulamenta a licitação, na modalidade pregão, na forma eletrônica.

5.6 - Requisitos de garantia e de manutenção (IN. 01/2019, art. 16, inciso I, alínea “d”, combinado com inciso II, alínea “d”)

Dos itens 1 a 2 da tabela 2.1

5.6.1. GARANTIA DOS MÓDULOS CRIPTOGRÁFICOS

5.6.1.1. O presente serviço está relacionado e agregado aos equipamentos e seus componentes previstos nos itens 1 a 2 da tabela 2.1

5.6.1.2. Os equipamentos devem vir com garantia mínima de 48 (quarenta e oito) meses, cuja vigência inicia-se a partir da data de emissão do Termo de Aceite Definitivo correspondente.

5.6.1.3. Deverá haver prestação de assistência técnica por parte da CONTRATADA, durante a vigência da garantia, contemplando, no mínimo, o serviço de atendimento telefônico e suporte remoto via web, ambos em regime de 7 (sete) dias por semana, 24 (vinte e quatro) horas por dia; esse serviço poderá ser usado para abrir solicitações de informações, reportar incidentes ou esclarecer dúvidas quanto à utilização dos produtos e soluções fornecidos.

5.6.1.4. O acesso ao serviço de assistência técnica deve ser feito por telefone, e-mail ou acesso seguro ao site, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

5.6.1.5. Em todas as atividades de assistência técnica, os técnicos da CONTRATADA deverão empregar a língua portuguesa, exceto no uso de termos técnicos e na utilização de textos técnicos, que poderão estar redigidos em outro idioma.

5.6.1.6. A CONTRATADA deverá notificar o CONTRATANTE sobre a liberação de novas versões, correções e descontinuidade dos produtos objeto do contrato. Para correções de técnica/software (patches), é aceitável que os avisos sejam encaminhados através de e-mails, por mecanismo automático de notificação. No caso de liberação de novas versões, ou descontinuidade dos produtos, o CONTRATANTE deverá ser formalmente comunicado, sempre no menor prazo possível a partir do respectivo anúncio.

5.6.1.7. Deve ser informado link (URL) de site na internet do fabricante dos equipamentos com disponibilidade de informações para suporte, tais como: guia de instalação, informações técnicas, atualização e download de drives, firmware, upgrade de BIOS.

5.6.1.8. Deverá ser garantido ao CONTRATANTE o pleno acesso aos sites eletrônicos do fabricante dos produtos ofertados, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, com direito às consultas a quaisquer bases de dados disponíveis para usuários, e também a efetuar downloads de quaisquer atualizações de técnica/software ou documentação.

5.6.1.9. A CONTRATADA deverá fornecer ao CONTRATANTE acesso remoto seguro, via Internet, canais de conhecimento para resolução de problemas (Troubleshooting). Essas ferramentas têm a função de otimizar a resolução de problemas.

5.6.1.10. Qualquer despesa decorrente da manutenção ou suporte realizada durante o período de garantia dos produtos instalados será de responsabilidade da CONTRATADA.

5.6.1.11. As unidades que apresentarem defeitos e necessitarem de recuperação ou substituição deverão ser encaminhadas pela CONTRATADA, sendo que as despesas de transporte deverão ser de responsabilidade da CONTRATADA.

5.6.1.12. A recuperação de equipamento deverá atender os prazos estabelecidos no APÊNDICE XI deste estudo. Nesses casos, deve ser apresentado obrigatoriamente relatório técnico com, pelo menos, as seguintes informações:

5.6.1.12.1. Código da unidade;

5.6.1.12.2. Número de série;

5.6.1.12.3. Falha informada;

5.6.1.12.4. Falha constatada;

5.6.1.12.5. Causa da falha;

5.6.1.12.6. Ação para correção;

5.6.1.12.7. Componentes substituídos/ajustes realizados.

5.6.1.13. Caso haja a necessidade de substituição de equipamentos, a modalidade de garantia deve ser no mínimo 8x5xSDS, ou seja, 8 (oito) horas por dia, 5 (cinco) dias por semana (úteis), com envio do equipamento substituto no mesmo dia (SDS – Same Day Ship).

5.6.1.14. Havendo a substituição, deve ser apresentado pela CONTRATADA, obrigatoriamente, um relatório técnico contendo as informações elencadas para os casos de reparação, e adicionalmente as seguintes informações:

5.6.1.14.1. Número de série da unidade substituta e substituída (no caso de substituição da unidade enviada); e

5.6.1.14.2. Razão da substituição da unidade (quando for caso).

5.6.1.15. Caso não haja atendimento ao prazo de 30 (trinta) dias corridos para a entrega das unidades reparadas e/ou substitutas, o período de garantia para estas unidades será automaticamente estendido pelo mesmo tempo do atraso ocorrido.

5.6.1.16. O CONTRATANTE rejeitará e devolverá à CONTRATADA qualquer unidade reparada ou substituta, sempre que constatar:

5.6.1.16.1. dano em qualquer de suas partes, observadas em inspeção visual;

5.6.1.16.2. funcionamento fora das especificações originais;

5.6.1.16.3. defeito constatado durante a execução de testes para verificação de funcionamento.

5.6.1.17. O tempo em dias corridos, contado entre a comunicação da irregularidade à CONTRATADA e a efetiva reposição da unidade defeituosa, será computado a fim de aferir eventual atraso e respectiva penalização.

5.6.1.18. Caso uma nova falha seja identificada já com o equipamento em operação, deverá ser aberto um novo chamado, obedecendo os tempos de reparação supracitados.

5.6.1.19. Ficará ainda a cargo da CONTRATADA, o apoio no suporte aos equipamentos durante a vigência da garantia, incluindo os seguintes serviços:

5.6.1.19.1. O provimento de informações, assistência e orientação para: instalação, desinstalação, configuração e atualização firmware e técnica/software; aplicação de correções (patches) de firmware e técnica/software; diagnósticos, avaliações e resolução de problemas; características dos produtos; e demais atividades relacionadas à correta operação e funcionamento dos equipamentos;

- 5.6.1.19.2. A atualização e/ou a configuração de toda e qualquer evolução de técnica/software, incluindo correções, patches, fixes, update, service packs, novas releases, versions, builds, upgrades, entre outros;
- 5.6.1.19.3. O atendimento às solicitações relacionadas a todo e qualquer incidente de hardware ou técnica/software, erros apresentados, formas de utilização do hardware ou técnica/software e correções necessárias para o restabelecimento de suas funcionalidades, incluindo troca de peças defeituosas, sem ônus adicionais para o CONTRATANTE;
- 5.6.1.19.4. As correções de firmware e ainda a desinstalação, reconfiguração ou reinstalação e correção de falhas de técnica/software, ajustes e reparos necessários, de acordo com os manuais, normas técnicas específicas e recomendações do fabricante;
- 5.6.1.19.5. Cada configuração (ou reconfiguração) deve garantir o acesso remoto ao CONTRATANTE; e
- 5.6.1.19.6. O fornecimento de informações e orientações necessárias das implementações e atualizações lançadas pelo fabricante para o perfeito funcionamento dos equipamentos, prestado via telefone e e-mail.

Dos itens 3 a 6 da tabela 2.1 serão atendidos pelo item 7 da tabela 2.1.

Não se aplica aos itens 7 a 12 da tabela 2.1.

5.7 - Requisitos temporais (IN. 01/2019, art. 16, inciso I, alínea “e”)

Dos itens 1 a 6 da tabela 2.1

A tabela 1.1 apresenta o cronograma de execução física e financeira, cujo detalhamento do fornecimento e das etapas ou fases da solução a ser contratada será definido no Plano de Implantação, observando todo o planejamento previsto no APÊNDICE XI deste estudo.

Tabela 1.1. Cronograma de Execução Físico-Financeiro

Evento	Atividade	Percentual Pago	Prazo	Responsável
1	Assinatura do Contrato	-	-	CONTRATANTE / CONTRATADA
2	Emissão do empenho relativo aos itens da Ata de Registro de Preços	-	1du	CONTRATANTE
3	Envio da designação do PREPOSTO da CONTRATADA	-	3du	CONTRATADA
4	Reunião inicial	-	5du	CONTRATANTE / CONTRATADA
5	Realização de <i>site survey</i> , Design da Solução e prontificação da elaboração do Plano de Implantação da execução do objeto contratado	10%	20du	CONTRATADA

6	Análise e, se necessário, exigência de correção do Design da Solução e do Plano de Implantação	-	2du	Equipe de Fiscalização do Contrato e Gestor
7	Entrega do Design da Solução e do Plano de Implantação corrigido	-	3du	CONTRATADA
8	Aprovação do Design da Solução e do Plano de Implantação	10%	0d	Equipe de Fiscalização do Contrato, Gestor
9	Emissão das OFBS por fase/etapa	-	2du	Gestor
10	Entrega dos bens e serviços, com testes de aceitação, ajustes de implementação e configuração no ambiente	20%	45du	Equipe de Fiscalização do Contrato e CONTRATADA
11	Solução de eventuais pendências devido a não conformidade com os termos da ARP dos itens fornecidos.	-	5du	CONTRATADA
12	Aceitação e emissão do Termo de Recebimento Provisório	-	5du	Equipe de Fiscalização do Contrato, Gestor
13	(Se necessário) Novos testes de aceitação e ajustes de implementação e configuração no ambiente	-	5du	Equipe de Fiscalização do Contrato e CONTRATADA
14	Entrega do <i>as-built</i>	10%	20d	CONTRATADA
15	Recebimento definitivo e emissão do Termo de Recebimento Definitivo	50%	10d	Equipe de Fiscalização do Contrato, Gestor

Dos itens 7 a 12 da tabela 2.1

A tabela 1.2 apresenta o cronograma de execução física e financeira, cujo detalhamento do fornecimento e das etapas ou fases da solução a ser contratada será definido no Plano de Implantação, observando todo o planejamento previsto no APÊNDICE XI deste estudo.

Tabela 1.2. Cronograma de Execução Físico-Financeiro

Evento	Atividade	Prazo (em dias corridos)	Responsável
1	Assinatura do Contrato	-	CONTRATANTE / CONTRATADA
2	Envio da designação do PREPOSTO da CONTRATADA	3	CONTRATADA

3	Reunião inicial (serviço de suporte)	5	CONTRATANTE / CONTRATADA
4	Apresentação do Plano de Liberação e anexos para a execução do objeto contratado (serviço de suporte)	20	CONTRATADA
5	Análise e, se necessário, exigência de correção do Plano de Liberação e anexos (serviço de suporte)	2	Equipe de Fiscalização do Contrato e Gestor
6	Entrega do Plano de Liberação e anexos corrigidos (serviço de suporte)	3	CONTRATADA
7	Aprovação do Plano de Liberação e anexos (serviço de suporte)	0	Equipe de Fiscalização do Contrato, Gestor
8	Emissão das OFBS	2	Gestor
9	Entrega dos serviços, com testes de aceitação, ajustes de implementação e configuração no ambiente (serviço de suporte)	60	Equipe de Fiscalização do Contrato e CONTRATADA
10	Solução de eventuais pendências devido a não conformidade dos itens fornecidos (serviço de suporte)	5	CONTRATADA
11	Aceitação e emissão do Termo de Recebimento Provisório	5	Equipe de Fiscalização do Contrato, Gestor
12	(Se necessário, para o serviço de suporte) Novos testes de aceitação e ajustes de implementação e configuração no ambiente	5	Equipe de Fiscalização do Contrato e CONTRATADA
13	Recebimento definitivo e emissão do Termo de Recebimento Definitivo	10	Equipe de Fiscalização do Contrato, Gestor

5.8 - Requisitos de segurança (IN. 01/2019, art. 16, inciso I, alínea “f”, combinado com inciso II, alínea “i”)

Para todos os itens da tabela 2.1

5.8.1. A CONTRATADA deve estar plenamente aderente as políticas e normas do CONTRATANTE quanto à segurança de informações, zelando pelo seu cumprimento, responsabilizando-se, inclusive, pelas ações de seus agentes.

5.8.2. A CONTRATADA deve garantir o sigilo e a inviolabilidade das informações a que eventualmente possa ter acesso, durante os procedimentos de suporte da solução instalada.

5.8.3. Todas as informações do projeto são consideradas confidenciais não sendo permitida sua divulgação por meio da CONTRATADA ou seus agentes sem autorização prévia e expressa do CONTRATANTE.

5.8.4. Responsabilização por falhas de segurança: no caso de não cumprimento das dessas disposições, a CONTRATADA estará sujeita às sanções administrativas previstas na legislação pertinente.

5.8.5. Da autenticação, autorização e accounting

5.8.5.1. Todo o acesso ao equipamento deverá ser realizado mediante autenticação.

5.8.1.8. Esse mecanismo deverá ter o cadastro de perfis individuais ou associação de grupos pré-definidos para os usuários, com as permissões necessárias a suas atividades.

5.8.5.3. Ter autenticação em base local de usuários, e permitir o uso simultâneo de autenticação em base local e base remota.

5.8.5.4. Todo equipamento deve armazenar as senhas locais de forma criptografada.

5.8.5.5. Não devem existir usuários com senha padrão. Cada senha deverá ser explicitamente criada antes de poder ser utilizada, caso isso não seja possível, deverá a CONTRATADA alterar todas as senhas padrão durante a instalação, o que será definido pelo CONTRATANTE.

5.8.5.6. Os sistemas devem utilizar senhas de qualidade conforme definição da ISO/IEC 27002.

5.8.5.7. No caso de usuários locais, em caso de erros sucessivos de senha, a conta deverá ser bloqueada por um período de tempo pré-determinado.

5.8.5.8. Ter a definição de níveis de privilégios para os administradores e operadores.

5.8.5.9. As consoles de administração deverão forçar o logout do usuário após um tempo pré-determinado sem atividade (idle timeout).

5.8.5.10. O nível padrão de privilégio deverá ser o menor possível para cada tipo de usuário, de acordo com suas atribuições (Ex. None, read-only, etc).

5.8.5.11. Ter a recuperação de acesso privilegiado por parte do administrador caso este perca o acesso por qualquer motivo. Deve requerer acesso físico ao equipamento para realização de tal procedimento.

5.8.6. Da Configuração e Backup

5.8.6.1. Deve restaurar as configurações do equipamento à sua condição inicial (ou default) de forma automatizada. Para isso, não deve ser necessário que o operador saiba os valores de cada item de configuração.

5.8.6.2. A console CLI deve suportar utilização de scripts de configuração, de forma a possibilitar automatização de ações.

5.8.6.3. A solução deverá permitir a instalação remota de atualizações e novas versões de seu sistema operacional. Deverá prover meios de garantir a integridade do arquivo recebido antes de executar sua instalação, e deve ter procedimento de retorno à versão original no caso de falhas no processo de atualização.

5.8.6.4. A solução deverá armazenar as configurações do sistema (backup) em um servidor remoto. A informação armazenada deve ser suficiente para restauração do equipamento para seu estado operacional no momento em que a configuração foi salva.

5.8.6.5. O sistema deverá permitir a restauração da configuração citada no item anterior de forma remota.

5.8.6.6. Os sistemas deverão salvar e exibir a sua configuração em um formato textual bem definido, de forma a permitir futura integração com sistemas de gerência de configuração.

5.8.7. Logs e Auditoria

- 5.8.7.1. Os registros (logs) da solução deverão conter informações suficientes para rastrear a origem de transações gerenciais, tais como nome do usuário que realizou a ação, endereço IP de origem, horário e ação realizada.
- 5.8.7.2. Os equipamentos devem ter o armazenamento local de logs, com informação completa de horário (timestamp).
- 5.8.7.3. Enviar esses logs para um servidor centralizado através do protocolo Syslog.
- 5.8.7.4. Possuir registro de eventos de segurança (logon, logoff, troca de senhas, escalação de privilégios, troca de senhas, criação, alteração, deleção de usuários, tentativas de logon invalidas, sucesso na autenticação, alterações de configuração, atualização de técnica/software, etc) e enviá-los tanto via Syslog (preferencialmente em conexão TCP – syslog-ng --) quanto via SNMP.
- 5.8.7.5. Os logs não deverão possuir senhas de usuários ou serviços.
- 5.8.8. Outros requisitos
- 5.8.8.1. A CONTRATADA deverá fornecer uma listagem de serviços que poderão estar ativos nos equipamentos. Tal lista deverá conter os protocolos e as portas utilizadas em cada caso.
- 5.8.8.2. A solução deve prover um meio de desabilitar os serviços não utilizados e todos os serviços desnecessários à operação devem ser desativados.
- 5.8.8.3. A CONTRATADA deve sugerir um modelo de configuração segura do equipamento, a qual deverá ser homologada pela equipe do CONTRATANTE.
- 5.8.8.4. Deve ser configurado todos os mecanismos de segurança nele presentes que visem à prestação segura do serviço, livre de falhas que possam comprometer sua segurança e integridade.
- 5.8.8.5. Deve sincronizar de horário através dos protocolos NTP ou SNTP do CONTRATANTE
- 5.8.8.6. Os equipamentos devem ser fornecidos livres de mecanismos escusos que permitam acesso remoto (como por exemplo, backdoors) a seus dados, configurações ou informações neles armazenadas ou transmitidos.

5.9 - Requisitos sociais, ambientais e culturais (IN. 01/2019, art. 16, inciso I, alínea “g”)

Não se aplica ao presente processo.

5.10 - Requisitos tecnológicos (IN. 01/2019, art. 16, inciso II, alínea "a", "b" e "c")

Constante no APÊNDICE XI deste estudo.

5.11 - Requisitos experiência profissional, formação e metodologia de trabalho da equipe da solução de TI (IN. 01/2019, art. 16, inciso II, alínea "f", "g" e "h")**5.11.1. Dos itens 1 a 2 da tabela 2.1**

5.11.11. O presente serviço de instalação está relacionado e agregado aos equipamentos e seus componentes previstos nos itens 2.1 e 2.2, a fim de se obter a Solução MSC, definida em 1.2.1.2.

5.11.12. A equipe técnica que se incumbirá da execução dos serviços de instalação será aquela apresentada pela CONTRATADA, cabendo a esta informar os dados dos técnicos envolvidos para a previa liberação dos mesmos junto às Organizações.

5.11.13. Os serviços de instalação e configuração para os equipamentos fornecidos serão executados nas Organizações envolvidas nesta especificação.

5.11.13.1. As configurações mais avançadas poderão ser feitas remotamente.

5.11.14. Cabe à CONTRATADA a responsabilidade pelas despesas da logística dos equipamentos até a instalação, com o respectivo seguro, sendo este obrigatório, e do deslocamento e da hospedagem dos especialistas da CONTRATADA.

5.11.15. Cabe também à CONTRATADA fornecer aos seus profissionais todos os recursos e condições necessárias ao desenvolvimento de suas funções e exigidos por legislação ou norma do trabalho específica.

5.11.16. Os serviços deverão ser planejados conforme cronograma previsto em Plano de Implantação (instalação e configuração), cujos requisitos estão enumerados no item 1.11.110.

5.11.17. A CONTRATADA deverá elaborar os seguintes documentos que caracterizarão cada fase da instalação e configuração dos equipamentos:

5.11.17.1. Site Survey, definida no item 1.11.111;

5.11.17.2. Design da Solução MSC, definido no item 1.11.112, o qual apresenta o modelo conceitual de toda a solução;

5.11.17.3. Plano de Implantação, definido no item 1.11.113; e

5.11.17.4. As-built das implantações, definida no item 1.11.114.

5.11.18. Essa documentação deve atentar para as diretrizes técnicas relacionadas à Solução MSC enumeradas no 5.11.110

5.11.19. A fase final da implantação da solução é caracterizada pelo Período de Funcionamento Experimental (PFE), conforme esclarecido em 1.11.115.

5.11.110. Diretrizes técnicas para a implantação dos módulos criptográficos e da solução

5.11.110.1. O modelo conceitual da solução dos túneis seguros com o algoritmo de Estado está diagramado na Figura 5 do ADENDO A, cujos MSC estão representados pelos cadeados.

5.11.110.2. Visando permitir um mínimo de escalabilidade, o arranjo desses túneis deve ser no mínimo ponto-multiponto, podendo ser, e preferencialmente, dinâmico e spoke-and-spoke.

5.11.110.2.1. Caso haja a possibilidade de um arranjo dinâmico e spoke-and-spoke, o CONTRATANTE poderá exigir à CONTRATADA essa técnica.

5.11.110.3. A Tabela 8 e Tabela 9 do ADENDO B apresenta a localização e quantitativos para instalação dos MSC, visando atender as Organizações – Pontos de Presença (PP) e Hubs satelitais do SISCOMIS – e os terminais do SISCOMIS.

- 5.11.110.3.1. A instalação nos TS estará condicionada a coordenação futura com o CONTRATANTE, respeitando a Tabela 8; e
- 5.11.110.3.2. Já a instalação dos MSC nas Organizações deve ocorrer nos endereços indicados na Tabela 9 do ADENDO B.
- 5.11.111. Site Survey
- 5.11.111.1. O Site Survey inicia-se com um diagnóstico da situação atual da ROD, o qual deve contemplar no mínimo:
- 5.11.111.1.1. a localização onde o equipamento será instalado (atualizar o endereço se for o caso, apontar a posição interna, como bloco, sala e a seção/divisão/departamento da Organização);
- 5.11.111.1.2. a revisão da arquitetura atual da rede sob a ótica da solução de TI ora contratada; e
- 5.11.111.1.3. o levantamento de eventuais óbices e pontos de falhas que possam prejudicar a implantação da Solução MSC.
- 5.11.111.2. A CONTRATADA deverá realizar a coleta de dados necessários à elaboração do Site Survey através de vistorias in loco ou de levantamento de informações prestadas por integrantes do MD e das Organizações.
- 5.11.111.2.1. Os dados calcados no levantamento informações por meio dos aludidos integrantes, bem como através de vistorias, é de responsabilidade apenas da CONTRATADA, não acarretando em ônus ao CONTRATANTE em consequência de imprecisão desses dados.
- 5.11.111.2.2. A não implantação dos equipamentos por consequência da falta ou imprecisão desses dados não acarretará em ônus ao CONTRATANTE.
- 5.11.111.3. Após diagnóstico, a CONTRATADA deverá informar, por meio de relatório, eventuais pendências ou inconsistências no ambiente das Organizações que possam impossibilitar a implantação dos equipamentos, devendo registrar, no mínimo, informações referentes à(s):
- 5.11.111.3.1. verificação de espaço necessário para a instalação dos equipamentos;
- 5.11.111.3.2. condições da infraestrutura elétrica, de aterramento e de proteção contra descargas elétricas e surtos, bem como verificação de pontos de alimentação nos racks para instalação dos equipamentos; e
- 5.11.111.3.3. disponibilidade de pontos de dados, elétrico/óptico nos patch pannels/DIO existentes.
- 5.11.111.4. Fica a cargo do CONTRATANTE solucionar eventuais pendências ou inconsistências apontadas pela CONTRATADA, desde que não seja uma ação prevista nesta especificação. Porém, a não adequação do ambiente não é limitante para a instalação dos equipamentos. Caso o CONTRATANTE não providencie soluções de contorno para a instalação dos mesmos, fica a CONTRATADA isenta de penalidades em virtude de falhas exclusivamente provocadas por essa não adequação.
- 5.11.112. Design da Solução MSC
- 5.11.112.1. O design da solução é um documento que expõe o conceito, em alto nível, da arquitetura, do modelo e da topologia da tecnologia a ser implementada na ROD. Logo, esse design deve considerar o:
- 5.11.112.1.1. site survey realizado na etapa anterior;
- 5.11.112.1.2. design lógico (camada 3), apresentando as características superficiais da solução fornecida;
- 5.11.112.1.3. registro dos possíveis riscos do conceito adotado e a forma de mitigação; e
- 5.11.112.1.4. registro dos requisitos de segurança e robustez, incluindo políticas de segurança para os elementos de rede.
- 5.11.112.2. Esse design precisa ser aprovado para que a etapa seguinte seja autorizada pelo CONTRATANTE.
- 5.11.113. Plano de Implantação (ou Plano de Inserção)

5.11.113.1. A definição das configurações a serem aplicadas devem estar em consonância com o previsto nos seguintes documentos:

5.11.113.1.1. Plano de Implantação da Solução ou HLD (High Level Design): documento, flexível e mutável, contendo as descrições em alto nível da implantação da solução em questão, com:

5.11.113.1.1.1. a estratégia de implantação da rede, observando:

5.11.113.1.1.1.1. os aspectos de resiliência (redundância e contingência);

5.11.113.1.1.1.2. a forma de minimizar eventuais impactos durante a implantação da solução; e

5.11.113.1.1.1.3. o modo de implantação, com as respectivas etapas.

5.11.113.1.1.2. o detalhamento do design lógico definido na etapa anterior, compreendendo agora:

5.11.113.1.1.2.1. a topologia detalhada;

5.11.113.1.1.2.2. ao boas práticas definidas nas RFC 7696 e 8221;

5.11.113.1.1.2.3. As configurações necessárias, em forma de template, para o monitoramento dos ativos (módulos e modems dos hubs e dos terminais do SISCOMIS) pelas ferramentas de visibilidade e monitoramento já em produção no ambiente do CONTRATANTE (necessariamente Cisco ONE e Cisco DNA, podendo ser ainda CA Spectrum, Zabbix ou Nagios), podendo haver a necessidade de implantar alertas com envios em aplicativos de mensageiria e o snmpv3 ou model drive telemetry (streaming telemetry). Deve-se atentar para o ADENDO D e ADENDO E;

5.11.113.1.1.1.1.1. a elaboração ou atualização do Plano de Endereçamento IPv4 e IPv6.

5.11.113.1.1.3. O cronograma de execução, que será acordado por representantes das PARTES;

5.11.113.1.1.4. o Caderno de Testes, que após a aprovação dos requisitos apresentados no caderno pelo CONTRATANTE, deverá ser realizado, em conjunto com a empresa fornecedora dos equipamentos, os testes no ambiente. Os testes deverão ser acompanhados por representante do CONTRATANTE que possuirá autonomia para a aprovação quando do seu término bem-sucedido. O Caderno deverá ser composto de, no mínimo:

5.11.113.1.1.4.1. Plano de Testes;

5.11.113.1.1.4.2. Equipes;

5.11.113.1.1.4.3. Ambiente;

5.11.113.1.1.4.4. Caso de Testes;

5.11.113.1.1.4.5. Testes; e

5.11.113.1.1.4.6. Critérios de Aceitação.

5.11.113.1.1.5. a lista e detalhes técnicos de todos os elementos a serem utilizados, bem como, as interfaces e seus protocolos adotados para a integração sistêmica da solução;

5.11.113.1.1.6. o Plano de Contingenciamento e Resposta da solução em caso de falhas (Troubleshooting Plan), observando inclusive o item 5.2.6.

5.11.113.1.2. Plano de Implantação da localidade ou LLD (Low Level Design): documento contendo o refinamento e o detalhamento das implantações configurações necessárias (vide item 1.11.113.1.2.2) que serão aplicadas em cada equipamento e técnica/software, tudo com base nas definições contidas no HLD (vide item 1.11.113.1.1).

5.11.113.1.2.1. Caso o escopo de instalação abranja várias localidades, poderá ser elaborado somente um documento de LLD com todas as configurações das localidades.

5.11.113.1.2.2. Plano de Liberação

5.11.113.1.2.2.1. Define mudanças pontuais que ocorrerão na ROD que serão planejadas, testadas e implantadas. A liberação pode principalmente incluir mudanças processos de gerenciamento, operação e documentação, mas também no hardware, software e outros;

5.11.113.1.2.2.2. Deve ter a preocupação em realizar as implantações exigidas enquanto protege a integridade dos serviços do negócio;

5.11.113.1.2.2.3. Deve conter pacotes de liberação (ou pacotes de trabalho), um conjunto de itens de configuração que será construído, testado e implantado ao mesmo tempo, como uma única liberação;

5.11.113.1.2.1.11.1 Cada pacote de liberação poderá incluir uma ou mais unidades de liberação.

5.11.114. As-built

5.11.114.1. O As-built registra em detalhes, para a toda a solução e para cada equipamento, o que foi instalado e configurado, em conformidade com o previsto no Plano de Implantação.

5.11.114.2. O documento de as-built deve incluir as atualizações decorrentes de quaisquer modificações realizadas durante a execução das atividades de instalação, contendo, no mínimo, as seguintes informações, como se fosse uma atualização do Site Survey:

5.11.114.2.1. Bay-face das instalações, contendo desenho e plotagem, utilizando técnica/software apropriado, da disposição dos equipamentos nos racks, identificando sua localização física, os equipamentos e as portas conectadas (Front / Rear);

5.11.114.2.2. Diagrama unifilar do cabeamento;

5.11.114.2.3. Tabela de conexões origem e destino; e

5.11.114.1.11.1 Levantamento Fotográfico.

5.11.114.2.5. Atualização, sempre que couber, da documentação listada no item 1.11.17.

5.11.115. Período de Funcionamento Experimental

5.11.115.1. Define-se o Período de Funcionamento Experimental (PFE) como:

5.11.115.1.1. o suporte fornecido para o presente Serviço de TI por um período de tempo após ele ter sido liberado.

5.11.115.1.2. o período correspondente entre:

5.11.115.1.2.1. a configuração do primeiro túnel seguro; e

5.11.115.1.2.2. 30 dias após a implantação do último túnel previsto no Plano de Implantação

5.11.115.2. O PFE tem por objetivo a verificação do correto funcionamento da solução durante o tempo necessário para acompanhar um ciclo do Padrão de Atividade do Negócio (PAN) do CONTRATANTE.

5.11.115.3. Assim, a solução deverá demonstrar que não degradará mais de 10% o desempenho da rede.

5.11.115.4. Durante o PFE, a CONTRATADA pode rever alguns requisitos acerca da solução e também fornecer recursos e ajustes adicionais para o Gerenciamento de Incidentes e Problemas, desde que previamente remetido ao CONTRATANTE para análise e autorização.

5.11.115.5. Apenas após a finalização dos testes de cada implantação, o PFE dos equipamentos.

5.11.115.6. Durante o PFE, devem ser sanados eventuais problemas de implantação e operação que venham surgir.

5.11.115.7. O PFE é considerado finalizado se, após 30 (trinta) dias corridos, não for identificado pelo CONTRATANTE quaisquer problemas na solução ou no equipamento implantado.

5.11.115.8. Caso, durante o PFE, o CONTRATANTE identifique a ocorrência de problemas relacionados ao correto funcionamento da solução ou do equipamento implantado que não sejam solucionados pela CONTRATADA, a contagem de tempo do PFE poderá, a critério do CONTRATANTE, ser reiniciada.

5.11.115.9. Em caso de cumprimento satisfatório dos níveis de serviços estabelecidos durante o PFE, o CONTRATANTE tem um prazo de 15 (quinze) dias corridos a contar do término do PFE para emitir o Termo de Recebimento Provisório.

5.11.115.10. O Termo de Recebimento Provisório, que é emitido para cada equipamento, deve incluir a data em que o PFE foi finalizada, a fim de aferir o seu encerramento.

5.11.115.11. Após a emissão do Termo de Recebimento Provisório, o CONTRATANTE é responsável por realizar as medidas técnicas e administrativas necessárias para a validação da entrega do PP e emitir o Termo de Recebimento Definitivo correspondente no prazo máximo de 60 (sessenta).

5.11.115.12. Caso a CONTRATADA não cumpra com os requisitos estabelecidos durante o PFE, o CONTRATANTE pode iniciar o processo administrativo necessário para notificar a CONTRATADA e, se for o caso, em cumprimento ao previsto na Lei 8.666/93, realizar a rescisão unilateral do contrato, configurada pela incúria, desorganização, incapacidade e/ou resistência da CONTRATADA em prestar o serviço correspondente. Além disso, o CONTRATANTE deve aplicar as demais sanções e penalidades previstas neste Termo de Referência.

5.11.115.13. Ao final do PFE, a CONTRATADA deverá elaborar relatório detalhado contendo informações sobre o funcionamento da solução.

5.11.115.14. Com o PFE, deve haver o serviço de Operação Assistida, a qual pode ser remota.

5.11.115.15. Durante a Operação Assistida, os seguintes serviços podem ser executados:

5.11.115.15.1. Desinstalação/reinstalação dos equipamentos; e

5.11.115.15.2. Configuração/alteração de quaisquer funcionalidades dos equipamentos.

5.11.115.16. A Operação Assistida deve realizar a Monitoração da Solução, que consiste na supervisão necessária para o bom funcionamento da solução contratada.

5.11.115.17. A Operação Assistida será exercida por uma Central de Serviços (CS) concebida pela CONTRATADA, observando o item 1.11.116.

5.11.116. Central de Serviços (CS)

5.11.116.1. A CONTRATADA então deverá oferecer uma Central de Serviços (CS), com um Gerente de Serviços, funcionando 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, durante toda a vigência em questão.

5.11.116.2. A CS deverá incluir atendimento remoto (chamado), em língua portuguesa (PT-BR), por telefone obrigatoriamente e por sistema de ticket ou por e-mail, a fim de permitir a abertura das Ordens de Serviço (OS).

5.11.116.3. Todas as OS abertas deverão ser registradas em sistema informatizado para o devido acompanhamento e controle da execução dos serviços.

5.11.116.4. Não deverá haver qualquer limitação para o número de:

5.11.116.4.1. solicitações de suporte técnico; e

5.11.116.4.2. servidores do CONTRATANTE autorizados a abrir chamados de suporte técnico. No entanto, o CONTRATANTE apresentará uma lista de servidores autorizados.

5.11.116.5. Os serviços de suporte serão preferencialmente tratados remotamente pela equipe de suporte da CONTRATADA.

5.11.116.6. Caso a CONTRATADA não consiga atuar através de assistência remota, a presença local de técnico, poderá ser solicitada, cabendo à CONTRATADA a responsabilidade pelas despesas de deslocamento do especialista e não haverá nenhuma cobrança adicional no valor a ser pago.

5.11.116.6.1. A equipe deverá ser capaz de atender cada uma das localidades de instalação dos equipamentos em até 24 (vinte e quatro) horas.

5.11.117. Chamados

5.11.117.1. O atendimento aos chamados serão classificados conforme sua severidade, a critério do CONTRATANTE, e devem ser executados de acordo com o no APÊNDICE XI deste estudo.

5.11.117.2. A abertura do chamado indicará o início para contagem do tempo de solução das ocorrências, do qual deverão ser descontadas as horas que dependam exclusivamente de ação do CONTRATANTE.

5.11.117.3. Caso seja demandado, por parte do CONTRATANTE, a presença do técnico nas severidades 1 e 2 indicados na Tabela 5, este deverá comparecer, nos prazos correlacionados, em um dos endereços descritos na Tabela 8 e Tabela 9 do ADENDO B, até a resolução definitiva ou contorno.

5.11.117.4. Diante da necessidade de serviço, do não atendimento da CONTRATADA ou, ainda, da evolução do problema, o CONTRATANTE poderá escalar os chamados para níveis superiores de severidade e/ou seus respectivos prazos.

5.11.117.5. Antes do fechamento de cada chamado, a CONTRATADA consultará o CONTRATANTE para validar o fechamento do chamado.

5.11.117.6. Um chamado fechado sem anuência do CONTRATANTE ou sem que o problema tenha sido de fato resolvido, será reaberto e os prazos serão contados a partir do instante de abertura do chamado original, inclusive para efeito de aplicação das sanções previstas.

5.11.117.7. Durante todo o período de suporte técnico, a CONTRATADA deverá informar e manter um número de telefone celular para fins de ligação direta entre o fiscal de contrato (CONTRATANTE) e o preposto.

5.11.117.8. A CONTRATADA disponibilizará ao CONTRATANTE, via aplicativo ou mídia digital, Relatório de Ocorrências mensais, constando as características gerais, período de atendimento, status atual da ocorrência, nome do funcionário do CONTRATANTE que abriu o chamado e a descrição do problema.

5.11.117.9. A CONTRATADA deverá garantir também os níveis mínimos de serviços, no que couber e sempre que possível, definidos no ADENDO E.

5.11.117.10. Os serviços de suporte técnico serão prestados nos equipamentos adquiridos, e abarácará também qualquer módulo que venha a ser adicionado nesses ativos, e compreendem os tipos de manutenção indicados no APÊNDICE XI deste estudo.

Dos itens 3 a 6 da tabela 2.1

5.11.2.1. O presente serviço de instalação está relacionado e agregado apenas aos ativos de rede e seus componentes já adquiridos e listados nos itens 3 a 6 da Tabela 2.1.

5.11.2.2. A CONTRATADA deve obedecer todos os requisitos previstos no APÊNDICE XI deste estudo.

5.11.2.3. A CONTRATADA apresentará pessoa ou equipe para a implantação com perfil técnico adequado e especialização necessária à execução do(a):

5.11.2.1.11.2. instalação e configuração dos equipamentos adquiridos nas Organizações;

5.11.2.3.2. acompanhamento dos serviços de instalação e configuração;

5.11.2.3.3. gerenciamento remoto dos os equipamentos adquiridos (Tabela 1);

5.11.2.3.4. acompanhamento dos processos de gerenciamento dos serviços.

5.11.2.4. Essa pessoa ou equipe deve ter pelo menos 1 (um) especialista certificado em, no mínimo, CCNP Service Provider.

5.11.2.5. Os serviços deverão ser planejados conforme cronograma previsto em Plano de Implantação, cujos requisitos adicionais estão enumerados no item 1.11.2.6.

5.11.2.6. Diretrizes técnicas para a implantação dos ativos de rede e da Nova ROD

5.11.2.6.1. A implantação dos ativos de rede definidos na Tabela 1 deve ocorrer de tal forma a obter os modelos conceituais apresentados nas Figuras 1 e 3 do ADENDO A.

5.11.2.6.2. A implantação da Nova ROD, definida em 1.2.1.1, deve estar integralmente alinhada com o item 1.3, e ser transparente à Solução MSC, definida em 1.2.1.2.

5.11.2.6.3. Esses ativos serão implantados nos endereços indicados na Tabela 10 do ADENDO C.

5.11.2.6.1.1.2. Com a evolução do processo de implantação, pode haver a necessidade de alteração nos endereços, o que deve ser de comum acordo entre as partes e devidamente registrada no Plano de Implantação.

5.11.2.6.3.2. Observa-se que atualmente a maioria desses ativos encontram-se no Rio de Janeiro, no Parque de Material de Eletrônica da Aeronáutica do Rio de Janeiro (PAME-RJ), situado na Rua General Gurjão, Nr 4, Bairro Caju, CEP 20931-040. Logo, é de responsabilidade da CONTRATADA toda a logística e seu respectivo seguro para o transporte dessa localidade até o ponto final de implantação.

5.11.2.6.4. A Nova ROD deve operar com ambos os protocolos IPv4 e IPv6, bem como realizar a respectiva tradução entre eles, de modo a permitir acesso a serviços que usam apenas IPv4, apenas IPv6 ou ambos.

5.11.2.6.5. A CONTRATADA deve elaborar a seguinte documentação adicional para a Nova ROD, para ambos os protocolos IPv4 e IPv6 (sempre que couber), os quais poderão ser implantados na rede, a critério do CONTRATANTE:

5.11.2.6.5.1. Plano de Roteamento: que expõe o respectivo plano de custos dos caminhos de rede, de forma a permitir o balanceamento o tráfego;

5.11.2.6.5.2. Plano de VPN: que deve adotar o MPLS e o Carrier Supporting Carrier (CSC), identificando as Organizações participantes, definindo o modo de implantação do QoS e da Engenharia de Tráfego etc;

5.11.2.6.5.3. Plano Multipoint VPN: visa estabelecer túneis multipontos sobre a internet, a ROD e as intranets das Forças por meio de tecnologias como Multipoint GRE, GETVPN e/ou DMVPN, podendo adotar o IPSec e todas as possibilidades de implementações Hub-and-spoke, Spoke-to-Spoke e/ou Hierárquico. Pode haver a necessidade de utilizar mais de uma tecnologia;

5.11.2.6.5.4. Plano de QoS: que inclui, dentre outros, as configurações necessárias para tratamento do tráfego de voz sobre IP (VoIP), traffic shapping etc;

5.11.2.6.5.5. Plano de NAT: que deve apresentar proposta para implementação de tradução de endereços, atualizando o atualmente praticado para a Nova ROD, considerando, sobretudo, uma forma de rastreamento desses endereços;

5.11.2.6.5.6. Plano de Ajustes de MTU, podendo considerar no lugar o de MSS, para as interfaces dos equipamentos em cada camada da rede, considerando a diversidade de serviços existentes sobre a rede;

5.11.2.6.5.7. Plano de Segurança:

5.11.2.6.5.7.1. possibilidade de ativação de firewalls e IPS dos ativos já adquiridos, principalmente, mas não limitado, nos pontos indicados em vermelho na Figura 8 do ADENDO A;

5.11.2.6.5.7.2. políticas e posicionamento dos firewalls em produção – quatro ASAs, um Checkpoint e um Palo Alto –, cujos eventuais remanejamentos e configurações ficarão a cargo do CONTRATANTE;

5.11.2.6.5.7.3. deve-se definir fluxos e respectivos controles, podendo haver a necessidade de se definir VLANS;

5.11.2.6.5.7.4. atentar para autenticação, autorização e accounting previsto no item 5.2.5.

5.11.2.6.5.8. Plano de Reação Contra Ataques Cibernéticos: considerando inclusive, mas não limitado, o Controller/Trigger Router através da técnica Remotely Triggered Black Hole (RTBH) filtering;

5.11.2.6.5.9. Plano de Monitoramento, que de prever:

5.11.2.6.5.9.1. a implantação do Cisco ONE, Cisco DNA, Network-Based Application Recognition Version 2 (or Next Generation NBAR) e o uso do SWSS, visando principalmente, mas não limitado, o Cisco Application Visibility and Control (AVC), o Flexible NetFlow (FnF) e o Cisco Prime Infrastructure - Lifecycle License, com o intuito de garantir o adequado monitoramento dos equipamentos adquiridos;

5.11.2.6.5.9.2. as configurações necessárias, em forma de template, para o monitoramento dos ativos, equipamentos de rede (vide Tabela 1) e modems dos hubs e dos terminais do SISCOMIS (139 modems) pelas ferramentas de visibilidade e monitoramento (ferramentas da Cisco ONE, podendo ser ainda CA Spectrum, Zabbix ou Nagios) em implantação ou já em produção no ambiente do CONTRATANTE, podendo existir no ambiente ferramenta de alertas com envios para aplicativos de mensageiria e o SNMPv3 ou Model Drive Telemetry (Streaming Telemetry);

5.11.2.6.5.9.3. a configuração da ferramenta para gerar indicadores (perda de pacote, latência, jitter etc) dos equipamentos, a ser acordado com o CONTRATANTE, podendo ser adotado técnicas de RMON (Remote Network Monitoring), como IP SLA (Internet Protocol Service Level Agreement), NQA (Network Quality Analyzer) ou similar;

5.11.2.6.5.9.4. a confecção de relatórios, a serem gerados, de fiscalização dos contratos externos do CONTRATANTE de enlaces WAN, os quais a CONTRATADA confeccionará e analisará, em apoio ao CONTRATANTE, indicadores como, dentre outros, Disponibilidade, Perda de Pacote da Rede, Latência da Rede, Jitter, indicadores como, dentre outros e sempre que possível, Disponibilidade, Perda de Pacote da Rede, Latência da Rede, Jitter, Eb/N0, BER, Lock de portadoras e Potência RF;

5.11.2.6.5.9.5. a adoção de modelos de telas de monitoramento, com a respectiva implantação, similar ao exposto no ADENDO D.

5.11.2.6.5.10. Plano de Remanejamento: deve considerar os ativos de rede que já estão instalados e os que serão substituídos, observado, sempre que for caso, as configurações necessárias motivadas pelas mudanças. Os ativos remanescentes devem ser transportados para o MD e essa logística é a cargo da CONTRATADA, nos moldes do item 2.4.4;

5.11.2.6.5.11. Minuta de Acordo de Nível Operacional (ANO) da Nova ROD:

5.11.2.6.5.11.1. estabelece procedimentos para gestão, controle e operação; e

5.11.2.6.5.11.2. contempla ainda uma Acordo de Troca de Tráfego (ATT), o qual delinea filtros e políticas de tráfego.

5.11.2.6.5.12. Plano de Transição, conforme descrito no item 1.11.2.7.

5.11.2.6.6. A fase para cada documentação adicional definida com o CONTRATANTE.

5.11.2.6.7. A CONTRATADA deverá ainda estruturar ao menos dois laboratórios, na infraestrutura do CONTRATANTE, para a simulação da Nova ROD, os quais permitirão realizar experimentos e simulações de rede que tangenciam as soluções e técnicas contidas na Nova ROD. Para tanto, deve-se preparar:

5.11.2.6.7.1. Laboratório físico, reaproveitando os equipamentos que serão substituídos ou remanejados, conforme item 1.11.2.6.5.10; e

5.11.2.6.7.2. Laboratório virtual, usando o EVE gratuito, com as customizações necessárias para facilitar a construção de vários ambientes de treinamento e de simulação.

5.11.2.7. Plano de Transição

5.11.2.7.1. A CONTRATADA deverá elaborar o Plano de Transição, que contém procedimentos da passagem, de uma empresa para outra, da operação e manutenção da ROD, bem como gerenciamento dos serviços relacionados a essa rede, sem que haja queda na qualidade dos serviços de TI prestados pelo CONTRATANTE.

5.11.2.7.2. Esse plano deve incluir, dentre outros:

5.11.2.7.2.1. entrega de versões finais da documentação;

5.11.2.7.2.2. transferência das responsabilidades entre as empresas;

5.11.2.7.2.3. cronograma de atividades a serem realizadas pelo CONTRATANTE e pela CONTRATADA.

5.11.2.7.2.4. transferência final de conhecimentos remanescente sobre a operação e a manutenção da Solução;

5.11.2.7.2.5. transferência de perfis de acesso;

5.11.2.7.2.6. as configurações necessárias para operação, manutenção e monitoramento dos ativos em questão;

5.11.2.7.2.7. transferência de caixas postais, quando for o caso; e

5.11.2.7.2.8. devolução de recursos, se for o caso.

5.11.2.8. Transferência de Conhecimento

5.11.2.8.1. O objetivo e as condições da transferência de conhecimento são as mesmas descritas no item 2.4.18. No entanto, deve ser dividido em módulos conforme descrito a seguir:

5.11.2.8.1.1. Módulo 1: focado na Nova ROD, devendo:

5.11.2.8.1.1.1. abranger todas as técnicas utilizadas para implantação dessa solução, com ambos os protocolos IPv4 e IPv6, focado também na integração com as redes das Forças, expondo ainda conceitos de IGP (OSPF e EIGRP), BGP, MPLS, CSC, IPSec, GETVPN, DMVPN, QoS e Engenharia de Tráfego;

5.11.2.8.1.1.2. Conter atividades hands-on de todos os conceitos e técnicas supracita, considerando um dos laboratórios definidos no item 5.11.2.6.7;

5.11.2.8.1.1.3. Deve observar as regras previstas no ANO (vide 1.11.2.6.5.11); e

5.11.2.8.1.1.4. ter, no mínimo, 40 horas de duração, os quais serão divididos em, no máximo, 20 horas semanais, podendo haver flexibilização com a autorização do CONTRATANTE.

5.11.2.8.1.2. Módulo 2 – focado nos roteadores adquiridos (Tabela 1), devendo:

5.11.2.8.1.2.1. incluir, no modelo hands-on, a operação, a configuração e o troubleshooting;

5.11.2.8.1.2.2. ter, no mínimo, 20 horas de duração, podendo haver flexibilização com a autorização do CONTRATANTE.

5.11.2.8.1.3. Módulo 3 – focado no Cisco ONE, devendo:

5.11.2.8.1.1.11.2. conter, inclusive no modelo hands-on, a implantação do Cisco ONE, Cisco DNA, Network-Based Application Recognition Version 2 (or Next Generation NBAR) e o uso do SWSS, visando principalmente, mas não limitado, o Cisco Application Visibility and Control (AVC), o Flexible NetFlow (FnF) e o Cisco Prime Infrastructure - Lifecycle License, com o intuito de garantir o adequado monitoramento dos equipamentos adquiridos;

5.11.2.8.1.3.2. ter, no mínimo, 20 horas de duração, podendo haver flexibilização com a autorização do CONTRATANTE.

5.11.2.8.1.4. Módulo 4 – focado na implantação do IPv6, devendo:

5.11.2.8.1.4.1. incluir, no modelo hands-on, a operação, a configuração e o troubleshooting;

5.11.2.8.1.4.2. abordar tópicos como MPLS com 6VPE;

5.11.2.8.1.4.3. abordar os estágios para implantação, sendo, dentre outros:

5.11.2.8.1.4.1.11.2. links com a Internet e nas estações de trabalho do pessoal técnico, com uso de proxies adequados;

5.11.2.8.1.4.3.2. servidores web ou e-mail e DNS;

5.11.2.8.1.4.3.3. equipamentos de segurança;

5.11.2.8.1.4.3.4. servidores corporativos, como de aplicação e de arquivos;

5.11.2.8.1.4.3.5. demais estações de trabalho;

5.11.2.8.1.4.3.6. dispositivos de VoIP e Videoconferência.

5.11.2.8.1.4.4. Deve observar as regras previstas no ANO (vide 1.11.2.6.5.11); e

5.11.2.8.1.4.5. ter, no mínimo, 20 horas de duração, podendo haver flexibilização com a autorização do CONTRATANTE.

Do item 7 da tabela 2.1

5.11.3.1. O presente serviço de suporte remoto visa apoiar tecnicamente a equipe do MD na configuração, operação e manutenção da Nova ROD, já caracterizada no item 1 desta especificação, por meio de um gerenciamento de processos de operação de serviços de TI, nos moldes preconizados pelas boas práticas do ITIL v3 ou v4.

5.11.3.2. Esses processos:

5.11.3.2.1. devem ser tutorados, sempre que possível, por um sistema de software, usando as ferramentas do CONTRATANTE, podendo ser quaisquer do item 3.1.6.5.9.2, ou ainda ser proposto pela CONTRATADA, sendo que a adoção de qual ferramenta será decidida pelo CONTRATANTE.

5.11.3.2.2. estão definidos ao longo desse apêndice, mas o detalhamento será delineado no Plano de Liberação (vide item 1.11.3.23).

5.11.3.2.2.1. A confecção desse detalhamento será de responsabilidade da CONTRATADA, mas o CONTRATANTE fornecerá os modelos.

5.11.3.3. Para o item 7 da Tabela 4, por ser classificado como serviço de natureza continuada, a vigência do contrato será de até 12 (doze) meses e poderá ser prorrogada conforme Art. 57 da Lei 8.666, inciso II e IV.

5.11.3.3.1. O serviço continuado não se forma com base em termos genéricos ou abstratos, mas apenas quando, diante de um caso concreto, a Administração verificar a essencialidade da prestação contratual para a manutenção de suas atividades e a necessidade de sua contratação por mais de um exercício financeiro continuamente.

5.11.3.1.11.3. Na realidade, o que caracteriza o caráter contínuo de um determinado serviço é sua essencialidade para assegurar a integridade do patrimônio público de forma rotineira e permanente ou para manter o funcionamento das atividades finalísticas do ente administrativo, de modo que sua interrupção possa comprometer a prestação de um serviço público ou o cumprimento da missão institucional. (TCU, Acórdão nº 132/2008, Rel. Min. Aroldo Cedraz, j. Em 12.02.2008).

5.11.3.4. O suporte deve ser 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, durante toda a vigência do contrato.

5.11.3.5. Os serviços deverão ser planejados conforme cronograma previsto em Plano de Liberação (vide item 5.11.3.23), que será elaborado pela CONTRATADA, nos moldes preconizados pelas boas práticas do ITIL v3 ou v4.

5.11.3.6. A fim de facilitar esse o Plano de Liberação, o CONTRATANTE disponibilizará os seguintes documentos:

5.11.3.6.1. Design atual da ROD;

5.11.3.6.2. As-built da ROD; e

5.11.3.6.3. Plano de Transição atual: documento que contém procedimentos da passagem do gerenciamento dos serviços da ROD consolidados em um compêndio e este advém do item 3.1.

5.11.3.7. A equipe técnica que realizará o suporte, composta por uma pessoa ou mais, será aquela apresentada pela CONTRATADA, cabendo a esta informar os dados dos técnicos envolvidos para a prévia liberação dos mesmos junto ao CONTRATANTE.

5.11.3.8. A CONTRATADA apresentará pessoa ou equipe para esse suporte com perfil técnico adequado e especialização necessária à execução do:

5.11.3.8.1. atendimento dos chamados;

5.11.3.8.2. gerenciamento e operação remota dos equipamentos adquiridos (Tabela 1);

5.11.3.8.3. monitoramento (apenas) dos ativos a compõem a ROD (os MSC, Tabela 1 e Tabela 3), com exceção dos ativos de segurança listados na Tabela 2;

5.11.3.8.4. assessoria de configuração e resolução de eventuais problemas e incidentes dos ativos de segurança listados na Tabela 2;

- 5.11.3.8.5. acompanhamento dos processos de gerenciamento dos serviços de TI suportados pela ROD.
- 5.11.3.9. Essa pessoa ou equipe deve ter pelo menos 1 (um) especialista certificado em, no mínimo, CCNP Service Provider.
- 5.11.3.10. Não haverá relação de subordinação e dependência entre os empregados integrantes da equipe da CONTRATADA e o CONTRATANTE.
- 5.11.3.11. Qualquer substituição na equipe técnica, após a sua definição, deverá ser efetuada, por escrito, com prévia anuência pelo CONTRATANTE, ficando desde já estabelecido que, nesta eventualidade, o substituto deverá possuir, no mínimo, as mesmas qualificações técnicas do substituído.
- 5.11.3.12. A CONTRATADA deverá garantir os níveis mínimos de serviços, no que couber e sempre que possível, definidos no ADENDO E.
- 5.11.3.13. A CONTRATADA deverá oferecer uma Central de Serviços (CS) que executará as tarefas previstas no item 2.4.16.
- 5.11.3.14. O serviço de suporte técnico deverá contemplar ainda, dentre outras, atividades tais como:
- 5.11.3.14.1. Orientações sobre uso e configuração dos hardware e técnica/software adotados, bem como sanar eventuais dúvidas e/ou dificuldades na utilização desses produtos para a Nova ROD;
- 5.11.3.14.2. Ações pró-ativas para aumentar a confiabilidade da Nova ROD, evitar e identificar a ocorrência de falhas ou suas consequências de técnica/software ou hardware, bem como orientações para prolongar sua vida útil, realizando diagnóstico, análise, avaliação, investigação e correção desses problemas de funcionamento; e
- 5.11.3.14.3. Apoio técnico na recuperação de ambientes em caso de pane ou perda de dados, sendo que o backup das configurações é de responsabilidade da CONTRATADA, devendo, para tanto, usar os equipamentos do CONTRATANTE.
- 5.11.3.15. Gerenciamento de configuração
- 5.11.3.15.1. A CONTRATADA deverá fazer o gerenciamento de configuração da ROD, relacionado à manutenção, adição e atualização de relacionamentos entre os componentes e da situação dos componentes durante a operação da rede.
- 5.11.3.15.1.1. Engloba, ainda, a configuração dos parâmetros como os limites para que um alarme seja ativado e uma notificação seja enviada.
- 5.11.3.15.2. Deve ser capaz de identificar os componentes da rede e definir a conectividade entre eles, bem como modificar a configuração, sob a anuência do CONTRATANTE, em resposta às avaliações de desempenho, recuperação de falhas, problemas de segurança, atualização da rede ou para atender às necessidades dos usuários.
- 5.11.3.15.3. Suas principais funções são:
- 5.11.3.15.3.1. coleta de informações;
- 5.11.3.15.1.11.3. controle de inventário;
- 5.11.3.15.3.3. início e encerramento das operações dos elementos gerenciados;
- 5.11.3.15.3.4. alteração da configuração dos elementos; e
- 5.11.3.15.3.5. geração de relatórios.
- 5.11.3.15.4. Indicadores a serem elaborados semestralmente:
- 5.11.3.15.4.1. Índice de Evolução de Itens de Configuração: Histórico semestral do número de IC registrados.
- 5.11.3.15.4.2. Índice de não-conformidades de IC: Número de IC não-conformes com o Plano de Configuração/Número de IC Auditados no período
- 5.11.3.16. Gerenciamento de incidentes e problemas

5.11.3.16.1. O objetivo deste gerenciamento é detectar e isolar possíveis incidentes e problemas que possam causar falhas significativas à ROD.

5.11.3.16.2. Quando ocorrer um incidente ou problema, a CONTRATADA deve:

5.11.3.16.2.1. registrar o incidente ou problema;

5.11.3.16.2.2. determinar o local da falha;

5.11.3.16.2.3. isolar, para que o componente possa continuar a funcionar sem interferências;

5.11.3.16.2.4. reconfigurar a rede a fim de minimizar o impacto da operação sem o componente que falhou;

5.11.3.16.2.5. reparar o componente com problemas para restaurar a rede ao seu estado anterior;

5.11.3.16.2.6. gerar Base de Dados de Erros Conhecidos (BDEC).

5.11.3.16.3. Indicadores a serem elaborados bimestralmente:

5.11.3.16.3.1. Índice de Eficiência de Resolução de Incidentes: Número de Incidentes Fechados no período sem o acionamento do Processo Gerenciamento de Problemas/Número de Incidentes Fechados no período

5.11.3.16.1.11.3. Índice de Resolução de Incidentes: Número de Incidentes Fechados no período (IF)/Número de Incidentes (I)

5.11.3.16.1.11.3.1. $I = \text{Aberto} + \text{Em andamento} + \text{Resolvido} + \text{IF}$

5.11.3.16.3.3. Índice de Problemas Solucionados: Números de Problemas Fechados no período (PF)/Número de Problemas (P)

5.11.3.16.3.3.1. $P = \text{Aberto} + \text{Em andamento} + \text{PF}$

5.11.3.17. Gerenciamento de Mudança

5.11.3.17.1. É processo responsável pelo controle do ciclo de vida de todas as mudanças, permitindo que as benéficas sejam feitas com o mínimo de interrupção à ROD.

5.11.3.17.2. O objetivo deste gerenciamento é garantir que os métodos e procedimentos padronizados mais adequados serão usados para o manuseio eficiente e imediato de todas as alterações.

5.11.3.17.3. Suas principais funções são:

5.11.3.17.3.1. Registrar Mudança;

5.11.3.17.1.11.3. Avaliar Mudanças;

5.11.3.17.3.3. Planejar e propor a mudança;

5.11.3.17.3.4. Gerenciar e realizar a liberação;

5.11.3.17.3.5. Revisar Mudança se for o caso; e

5.11.3.17.3.6. Encerrar Mudança.

5.11.3.17.4. Indicadores a serem elaborados semestralmente:

5.11.3.17.4.1. Índice de Evolução de Mudanças: Histórico do número de Mudanças Registradas nos últimos seis meses

5.11.3.17.4.2. Índice de Mudanças Emergenciais Aprovadas: Número de Mudanças Emergenciais registradas/Número de Mudanças Registrados

5.11.3.17.4.3. Índice de Mudanças Aprovadas: Número de Mudanças Aprovadas no período (MA)/Número de Mudanças (M)

5.11.3.18. Gerenciamento de desempenho

5.11.3.18.1. O objetivo deste gerenciamento é garantir a qualidade de exigida para a ROD.

5.11.3.18.2. Suas principais atividades são:

5.11.3.18.2.1. monitorar o desempenho;

5.11.3.18.2.2. caracterizar recarga de trabalho;

5.11.3.18.2.3. ajustar parâmetros;

5.11.3.18.2.4. identificar gargalos e corrigi-los;

5.11.3.18.2.5. comparar desempenho entre sistemas alternativos;

5.11.3.18.2.6. dimensionar os componentes do sistema;

5.11.3.18.2.7. gerar previsão de crescimento e tendências.

5.11.3.18.3. Esse gerenciamento auxilia no planejamento, administração e manutenção de grandes redes, sendo úteis para reconhecer situações de gargalo e aplicar ações corretivas antes que elas possam causar problemas ao usuário.

5.11.3.18.4. Indicadores a serem elaborados trimestralmente:

5.11.3.18.4.1. Índice de Capacidade de Serviços: Conjunto de medições feitas sobre a capacidade e desempenho dos equipamentos e enlaces, definidas no Plano de Capacidade (armazenamento, processamento, utilização de banda etc.)

5.11.3.19. Central de Serviços (CS)

5.11.3.19.1.1. A CONTRATADA então deverá oferecer uma Central de Serviços (CS) funcionando 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, durante toda a vigência em questão.

5.11.3.19.1.2. A CS pode ser composta pela mesma equipe já caracterizada no item 1.11.3.8.

5.11.3.19.1.3. A CS deverá incluir atendimento remoto (chamado), em língua portuguesa (PT-BR), por telefone obrigatoriamente e por sistema de ticket ou por e-mail, a fim de permitir a abertura das Ordens de Serviço (OS).

5.11.3.19.1.3.1. O Modelo das Ordens de Serviço (OS) para chamados será definido durante a elaboração do Plano de Liberação.

5.11.3.19.1.4. Não deverá haver qualquer limitação para o número de:

5.11.3.19.1.4.1. solicitações de suporte técnico; e

5.11.3.19.1.4.2. servidores do CONTRATANTE autorizados a abrir chamados de suporte técnico. No entanto, o CONTRATANTE apresentará uma lista de servidores autorizados.

5.11.3.19.1.5. Os serviços de suporte serão preferencialmente tratados remotamente pela equipe de suporte da CONTRATADA.

5.11.3.20. Monitoramento

5.11.3.20.1. O monitoramento da ROD deve abarcar os MSC e os ativos listados nas Tabelas 1 e 3, bem como os enlaces WAN, LAN, internet e das redes metropolitanas que conectam esses ativos, obedecendo o previsto no item 5.1.6.5.9.

5.11.3.20.1.1. Não há necessidade de configuração ou intervenção nos MSC e nos ativos listados na Tabela 3.

5.11.3.20.2. Todas as views de monitoramento devem estar disponibilizadas ao CONTRATANTE.

5.11.3.20.3. Deve monitorar a disponibilidade dos enlaces e dos ativos, gerando relatórios mensais.

- 5.11.3.20.4. Deve haver monitoramento ainda, sempre que possível, dos fluxos do tráfego da rede, apresentando, dentre outros, o volume, a distribuição do tráfego por aplicação (ssl, http, etc),
- 5.11.3.20.5. Deve contabilizar indicadores dos enlaces WAN, como perda de pacote, latência e jitter, gerando relatórios mensais.
- 5.11.3.20.6. O monitoramento de falhas deve ser proativo, ou seja, quando se registra um incidente ou problema até o vigésimo minuto após a sua ocorrência, bem como o início do procedimento de resolução, devendo observar o ADENDO E.
- 5.11.3.20.7. Deve monitorar a “saúde” de todos equipamentos e enlaces que compõem a Nova ROD.
- 5.11.3.20.8. Todos os relatórios supracitados devem ser encaminhados por e-mail e disponibilizados em sítio eletrônico hospedado na infraestrutura do CONTRATANTE, de forma similar ao exposto no seguinte sítio <<https://www.rnp.br/sistema-rnp/ferramentas/documentos>>.
- 5.11.3.20.9. Esse sítio eletrônico deve ser elaborado pela CONTRATADA, e deve conter ainda:
- 5.11.3.20.9.1. informações sobre eventuais mudanças que possam causar degradação ou indisponibilidade da ROD, incluindo o cronograma das preventivas;
- 5.11.3.20.9.2. a situação dos enlaces e ativos em tempo real, mostrando em cores distintas a estado desses itens, como disponibilidade, indisponibilidade, inativo, etc;
- 5.11.3.20.9.3. os diagramas on-line apresentados no ADENDO D.
- 5.11.3.20.10. Os detalhes e ajustes desses relatórios serão definidos no Plano de Liberação.
- 5.11.3.20.11. A CONTRATADA poderá ser ainda demandada pelo CONTRATANTE a configurar indicadores adicionais por meio das ferramentas aqui citadas e confeccionar relatórios correspondentes, sejam periódicos ou não.
- 5.11.3.21. Chamados
- 5.11.3.21.1. O atendimento aos chamados, que é remoto, serão classificados conforme o seu nível severidade, a critério do CONTRATANTE, e devem ser executados de acordo com o APÊNDICE XI deste estudo.
- 5.11.3.21.2. A abertura do chamado indicará o início para contagem do tempo de solução das ocorrências do qual deverão ser descontadas as horas que dependam exclusivamente de ação do CONTRATANTE.
- 5.11.3.21.3. Diante da necessidade de serviço, e do não atendimento da CONTRATADA ou, ainda, da evolução do incidente ou problema, o CONTRATANTE poderá escalar os chamados para níveis superiores de severidade e/ou seus respectivos prazos.
- 5.11.3.21.4. Antes do fechamento de cada chamado, a CONTRATADA consultará o CONTRATANTE para validar o fechamento do chamado.
- 5.11.3.21.5. Um chamado fechado sem anuência do CONTRATANTE ou sem que o problema tenha sido de fato resolvido, será reaberto e os prazos serão contados a partir do instante de abertura do chamado original, inclusive para efeito de aplicação das sanções previstas.
- 5.11.3.21.6. Durante todo o período de suporte técnico, a CONTRATADA deverá informar e manter um número de telefone celular para fins de ligação direta entre o fiscal de contrato (CONTRATANTE) e o preposto.
- 5.11.3.22. Dos Relatórios Técnicos e documentos

5.11.3.22.1. Após toda ação pró-ativa ou recuperação de ambientes, deve haver registro pela CONTRATADA, em relatórios técnicos, para acompanhamento e controle da execução, bem como a devida atualização do As-built caso haja alteração de configuração.

5.11.3.22.2. Os relatórios técnicos deverão conter: data e hora do chamado, do início e término do atendimento, problema relatado, sintomas identificados, questionamento formulado, solução apresentada, número de horas para resolver, responsável pelo atendimento.

5.11.3.22.3. Os relatórios técnicos deverão ser assinado pelo técnico do CONTRATANTE ou pelo fiscal do contrato na condição de responsável pelo acompanhamento dos serviços.

5.11.3.22.4. O relatório técnico deverá ser encaminhado ao CONTRATANTE até o terceiro dia útil do mês subsequente ao mês analisado, junto com a fatura referente ao mesmo, sendo contados o prazo a partir da assinatura do contrato.

5.11.3.22.5. A CONTRATADA também disponibilizará ao CONTRATANTE, via aplicativo ou mídia digital, Relatório de Ocorrências mensais, constando as características gerais, período de atendimento, status atual da ocorrência, nome do funcionário do CONTRATANTE que abriu o chamado e a descrição do problema.

5.11.3.22.6. A CONTRATADA deverá atualizar o Plano de Transição (item 1.11.3.6.3) e seus anexos até três meses antes do encerramento do contrato.

5.11.3.23. Plano de Liberação (ou Plano de Inserção)

5.11.3.23.1. Define mudanças que ocorrerão na ROD que serão planejadas, testadas e implantadas. A liberação pode principalmente incluir mudanças processos de gerenciamento, operação e documentação, mas também no hardware, software e outros;

5.11.3.21.11.3. Deve ter a preocupação em entregar o suporte exigido pelo negócio enquanto protege a integridade dos serviços;

5.11.3.23.3. Deve conter pacotes de liberação (ou pacotes de trabalho), um conjunto de itens de configuração que será construído, testado e implantado ao mesmo tempo, como uma única liberação;

5.11.3.23.4. Cada pacote de liberação poderá incluir uma ou mais unidades de liberação.

5.11.3.24. Período de Funcionamento Experimental

5.11.3.24.1. A CONTRATADA passará por um Período de Funcionamento Experimental (PFE), que tem por objetivo a verificação do correto funcionamento da solução durante o tempo necessário para acompanhar um ciclo do Padrão de Atividade do Negócio (PAN) do CONTRATANTE.

5.11.3.24.2. Define-se o PFE como o suporte fornecido para o presente Serviço de TI por um período de 15 (quinze) dias corridos após a conclusão do Plano de Liberação.

5.11.3.24.3. Durante o PFE, a CONTRATADA pode rever alguns requisitos acerca da solução e também fornecer recursos e ajustes adicionais para o Gerenciamento de Incidentes e Problemas, desde que previamente remetido ao CONTRATANTE para análise e autorização.

5.11.3.24.4. Durante o PFE, devem ser sanados eventuais problemas de implantação e operação que venham surgir.

5.11.3.24.5. O PFE é considerado finalizado se, após 15 (quinze) dias corridos, não for identificado pelo CONTRATANTE quaisquer problemas no serviço prestado.

5.11.3.24.6. Caso, durante o PFE, o CONTRATANTE identifique a ocorrência de problemas relacionados ao correto funcionamento da solução ou do equipamento implantado que não sejam solucionados pela CONTRATADA, a contagem de tempo do PFE poderá, a critério do CONTRATANTE, ser reiniciada, e o tempo anterior não será computado para fins de pagamento.

5.11.3.24.7. Em caso de cumprimento satisfatório dos níveis de serviços estabelecidos durante o PFE, o CONTRATANTE tem um prazo de 15 (quinze) dias corridos a contar do término do PFE para emitir o Termo de Recebimento Provisório.

5.11.3.24.8. O Termo de Recebimento Provisório deve incluir a data em que o PFE foi finalizada, a fim de aferir o seu encerramento.

5.11.3.24.9. Após a emissão do Termo de Recebimento Provisório, o CONTRATANTE é responsável por realizar as medidas técnicas e administrativas necessárias para a validação da liberação e emitir o Termo de Recebimento Definitivo correspondente no prazo máximo de 15 (quinze) dias corridos.

5.12 - Demais requisitos necessários e suficientes à escolha da solução de TIC

Conforme as subseções anteriores.

6. Levantamento de Mercado

6.1- ANÁLISE DE SOLUÇÕES

6.1.1 - Identificação das Soluções – (IN. 01/2019, art 11, inciso II, alínea “a” ao “i”)

As soluções para atender a presente demanda sob análise deste estudo estão listados na subseção 1.2 e na seção 5 - REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS deste estudo, totalizando quatro soluções de TI.

Considerando as opções técnicas, a seção 5 e as abordagens de como atender a demanda, há apenas uma opção de solução técnica identificada, de lato sensu, que está descrita no APÊNDICE XI deste estudo, a fim de atender os requisitos estratégicos definidos no DOD e no TLE já qualificados neste estudo.

6.1- Disponibilidade de solução similar na APF – (IN. 01/2019, art 11, inciso II, alínea “a”)

Conforme registro da Tabela 3.1.

6.3 – Soluções alternativas do mercado - (IN. 01/2019, art 11, inciso II, alínea “b”)

Conforme a seção 5 - REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS deste estudo.

6.4 - Os diferentes modelos de prestação do serviço – (IN. 01/2019, art 11, inciso II, alínea “f”)

Conforme APÊNDICE XI deste estudo.

6.5 - A possibilidade de aquisição na forma de bens ou contratação como serviço - (IN. 01/2019, art 11, inciso II, alínea “h”)

A aquisição será realizada por meio de processo licitatório.

6.6 - A ampliação ou substituição da solução implantada - (IN. 01/2019, art 11, inciso II, alínea “h”)

Conforme APÊNDICE XI deste estudo.

6.7 – Análise Comparativo de Soluções - (IN. 01/2019, art 11, inciso III, caput)

Tabela 6.1. Análise Comparativo de Soluções

Requisito	Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X	X (para o MSC apenas)	
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
---	-----------	--	--	---

6.8 - REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS - (IN. 01/2019, art 11, § 1º)

Para a solução **Nova ROD**, foram observadas, conforme Tabela 5.1, as seguintes Linhas de Ação consideradas inviáveis.

Tabela 5.1. soluções para a Nova ROD consideradas inviáveis

Nr	L Aç	Descrição	Justificativa da inviabilidade
1	Obter consultoria e apoio do EB	Utilizar das capacitações e experiências adquiridas pelos profissionais do EB nas tecnologias que envolvem a implementação da Rede de Passagem, conforme proposto em Relatório 1855687.	Conforme despacho 2681148
2	Usar a equipe do MD	Usar equipe do MD para implantar a solução.	Conforme descrito no TLE, a solução de esforço hercúlio e a equipe do MD não p disponibilidade de tempo para a implanta

Por outro lado, para a **Solução MSC**, foi observada, conforme Tabela 5.2, a seguinte Linha de Ação considerada inviável.

Tabela 5.2. soluções para a Solução MSC consideradas inviáveis

Nr	L Aç	Descrição	Justificativa d
1	Adotar criptografia IPSec	Adotar a criptografia IPSec já disponível nos ativos de rede adquiridos	Não é um algoi

6.9 – ANÁLISE COMPARATIVA DE CUSTOS

6.10 – PESQUISA DE PREÇOS - (IN. 01/2019, art. 20)

A fim de construir a estimativa adequada de custo total da contratação, consolidada na seção 8 deste estudo, e dados que o mercado de EED é restrito e limitado e que a solução MSC é tecnicamente muito específica, realizou-se uma extensa pesquisa de preços para a solução pretendida, que se **iniciou no segundo semestre de 2019** e prosseguiu no decorrer deste ano.

Nesse contexto, e inicialmente, cabe ressaltar que, em uma primeira aproximação de valores, de 10 SET 2020, já se registrou as seguintes propostas prévias:

- Proposta Comercial Prévia da Kryptus (2680452);
- Proposta Comercial Prévia da YSSY (2683444); e
- Proposta Comercial Prévia da ATelecom (2683460).

No entanto, diante das recomendações da Administração, em OUT 2020, fez-se uma nova pesquisa de mercado, onde foram encaminhados **dez e-mails** a EED na área de TIC e SIC.

Mais uma vez, diante de novas recomendações de 09 NOV 2020, propondo que o futuro certame considere a Lei Nº 12.598, de 21 de março de 2012, **apenas** para os MSC, o que foi acatado pela Equipe de Planejamento. Assim, iniciou-se, no mesmo dia, mais uma nova pesquisa de mercado, por meio de *e-mails* às EED, obtendo os resultados constantes nas tabelas a seguir, as quais se basearam nas propostas comerciais apensadas neste processo (2933150).

A **tabela 6.1** apresenta um comparativo de custos de aquisição dos MSC baseado em propostas comerciais de EED, as quais informam atender os requisitos deste estudo. Nesse comparativo, que apresenta os valores médios e mínimos, pode-se observar que a variação da Solução MSC é de **20,12%**.

Tabela 6.1. comparativo entre os custos de aquisição dos MSC

		PIQL		Z Tecnologia
SOLUÇÃO MSC	Qtd	Preço Unit (R\$)	Preço Total (R\$)	Preço Unitário (R\$)
Módulo de Segurança Criptográfico (100 Mbps) com garantia, instalação e configuração	151	25.792,00	3.894.592,00	36.000,00
Módulo de Segurança Criptográfico (1 Gbps) com garantia, instalação e configuração	4	125.437,00	501.748,00	119.000,00
TOTAL		R\$ 4.396.340,00		R\$ 5.912.000,00

A **tabela 6.2** apresenta um comparativo de custos de instalação dos ativos de rede já adquiridos baseado em propostas comerciais de empresas.

Tabela 6.2. comparativo entre os custos de instalação dos ativos de rede já adquiridos

				PIQL		A Telecom		Wise It		Kryptos	
Gp	Nr	INSTALAÇÃO DOS EQUIPAMENTOS EXISTENTES	Qtd	Preço Unit (R\$)	Preço Total (R\$)	Preço Unit (R\$)	Preço Total (R\$)	Preço Unitário (R\$)	Preço Total (R\$)	Preço Unitário (R\$)	Preço Total (R\$)

2	3	Instalação e configuração do roteador CISCO ASR 1001-X/K9	15	161.160,27	2.417.404,05	22.500,00	337.500,00	30.000,54	450.008,10	5.113,90	76.708,
	4	Instalação e configuração do roteador CISCO ISR 4451/K9	19	145.448,24	2.763.516,56	8.250,00	156.750,00	20.950,90	398.067,10	5.113,90	97.164,
	5	Instalação e configuração do roteador CISCO ISR 4431/K9 ou ISR 4331/K9	71	83.612,82	5.936.510,22	8.250,00	585.750,00	14.400,34	1.022.424,14	5.113,90	363.086
	6	Instalação e configuração do Switch CISCO Catalyst C9200L	34	22.315,44	758.724,96	7.940,00	269.960,00	4.275,80	145.377,20	5.113,90	173.872
TOTAL				R\$ 11.876.155,79		R\$ 1.349.960,00		R\$ 2.015.876,54		R\$ 710.832,10	

Observa-se, ainda com base na tabela 6.2, uma variação entre os valores médio e mínimo de **82,18%**, a qual é excessiva. Essa distorção é causada inicialmente pelos altos valores constantes na proposta da empresa PIQL, e, nesse caso, convém descartá-la.

Assim, e diante de tal deturpação, a **tabela 6.3** apresenta um comparativo **ajustado** de custos dessa instalação, agora sem a proposta da empresa PIQL, onde se tem uma nova variação entre os valores médio e mínimo, reduzindo para **47,69%**. Sem uma avaliação de contexto, essa diferença ainda se apresenta alta, dado que a proposta da Kryptus para a instalação em questão é bem menor quando comparada com as demais. Isso se deve ao fato de que as instalações dos ativos adquiridos ocorrerão nas mesmas localidades onde os módulos MSC serão implantados, reduzindo o custo de logística da empresa.

Tabela 6.3. comparativo ajustado entre os custos de instalação dos ativos de rede já adquiridos

Gp	Nr	INSTALAÇÃO DOS EQUIPAMENTOS EXISTENTES	Qtd	A Telecom		Wise It		Kryptos		MÉDIAS	
				Preço Unit (R\$)	Preço Total (R\$)	Preço Unitário (R\$)	Preço Total (R\$)	Preço Unitário (R\$)	Preço Total (R\$)	Preço Unitário (R\$)	Preço Total (R\$)
	3	Instalação e configuração do roteador CISCO ASR 1001-X/K9	15	22.500,00	337.500,00	30.000,54	450.008,10	5.113,90	76.708,50	19.204,81	288.072,20

2	4	Instalação e configuração do roteador CISCO ISR 4451/K9	19	8.250,00	156.750,00	20.950,90	398.067,10	5.113,90	97.164,10	11.438,27	217.327,07
	5	Instalação e configuração do roteador CISCO ISR 4431/K9 ou ISR 4331/K9	71	8.250,00	585.750,00	14.400,34	1.022.424,14	5.113,90	363.086,90	9.254,75	657.087,01
	6	Instalação e configuração do Switch CISCO Catalyst C9200L	34	7.940,00	269.960,00	4.275,80	145.377,20	5.113,90	173.872,60	5.776,57	196.403,27
TOTAL				R\$ 1.349.960,00		R\$ 2.015.876,54		R\$ 710.832,10		R\$ 1.358.889,55	

Cabe ainda destacar que, embora o valor da linha 6 da proposta da empresa Wise IT é a menor, o que se deve considerar para a coluna MÍNIMOS é o menor valor do grupo. Logo, levou-se em conta, para esse item, a proposta da Kryptus.

A **tabela 6.4** apresenta um comparativo de custos para o suporte à Nova ROD baseado em propostas comerciais de empresas, as quais informam atender os requisitos deste estudo. Nesse comparativo, que apresenta os valores médios e mínimos, pode-se observar que a variação desse suporte é de **14,5%**.

Tabela 6.4. comparativo entre os custos para o suporte à Nova ROD

Nr	SUPORTE NOVA ROD	Qtd	A Telecom	Wise It	Kryptos	MÉDIAS	MÍNIMOS	Variação
7	Serviço de Suporte Técnico para a ROD por 12 meses	1	646.800,00	562.540,95	764.400,00	657.913,65	562.540,95	14,50%

A **tabela 6.5** apresenta um comparativo de custos para os cursos avançados do fabricante dos equipamentos já adquiridos. Nesse comparativo, que apresenta os valores médios e mínimos, pode-se observar que a variação para esses cursos é de **25,17%**.

Tabela 6.5. comparativo entre os custos para os cursos

			ITLS		A Telecom		Wise It		Kryptos		MÉDIAS
Nr	CURSOS AVANÇADOS DO FABRICANTE	Qtd	Preço Unit (R\$)	Preço Total (R\$)	Preço Unit (R\$)	Preço Total (R\$)	Preço Unitário (R\$)	Preço Total (R\$)	Preço Unitário (R\$)	Preço Total (R\$)	Preço Unitário (R\$)
	Curso 300-501 SPCOR:										

8	Implementing and Operating Cisco Service Provider Network Core Technologies	11	12.550,00	138.050,00	22.200,00	244.200,00	21.335,00	234.685,00	15.687,50	172.562,50	16.864,50
9	Curso 300-510 SPRI: Implementing Cisco Service Provider Advanced Routing Solutions	7	13.830,00	96.810,00	23.800,00	166.600,00	23.511,00	164.577,00	17.287,50	121.012,50	18.451,70
10	300-515 SPVI: Implementing Cisco Service Provider VPN Services (SPVI)	7	13.830,00	96.810,00	23.800,00	166.600,00	23.511,00	164.577,00	17.287,50	121.012,50	18.451,70
11	350-701 SCOR: Implementing and Operating Cisco Security Core Technologies (SCOR)	7	7.800,00	54.600,00	13.700,00	95.900,00	13.260,00	92.820,00	9.750,00	68.250,00	10.462,00
12	350-801 CLCOR: Implementing and Operating Cisco Collaboration Core Technologies (CLCOR).	7	8.900,00	62.300,00	14.800,00	103.600,00	15.130,00	105.910,00	11.125,00	77.875,00	11.771,00
VALOR TOTAL			R\$ 448.570,00		R\$ 776.900,00		R\$ 762.569,00		R\$ 560.712,50		R\$ 599.4

Cabe assinalar ainda que, durante toda essa pesquisa, ocorreram inúmeras comunicações entre o Integrante Técnico e as representantes das EED, a fim de refinar requisitos tecnológicos em direção da simplificação, desde que sejam garantidos os elementos necessários e suficientes a atender aos interesses do negócio. Diante de toda essa interação, foi possível ajustar alguns requisitos tecnológicos e também foi preciso negar algumas solicitações de EED, pois estas feriam as necessidades do negócio e /ou o escopo do subprojeto supracitado.

Assim, diante do ostentado até aqui, é de entendimento que a pesquisa de preços com as EED, cujo mercado é restrito e limitado, dada a natureza dos serviços / produtos de segurança, foi metódica e adequada.

Concluindo a presente pesquisa, a **tabela 6.6** apresenta um comparativo de custos totais da contratação, cuja variação entre os valores médios e mínimos é de **25,04%**. Cabe destacar aqui, uma vez desconsiderado custos de instalação de ativos constantes na proposta da empresa PIQL, pode-se desprezar o cálculo da mediana para a esta pesquisa.

Tabela 6.6. comparativo de custos totais da contratação

Gp	Nr	Bem/Serviço	Qtd	PIQL/ITLS		Z Tecnologia / A Tele	
				Preço Unit (R\$)	Preço Total (R\$)	Preço Unitário (R\$)	Preço Total (R\$)
1	1	Módulo de Segurança Criptográfico (100 Mbps) com garantia, instalação e configuração	151	25.792,00	3.894.592,00	36.000,00	5.436.000,00
	2	Módulo de Segurança Criptográfico (1 Gbps) com garantia, instalação e configuração	4	125.437,00	501.748,00	119.000,00	476.000,00
2	3	Instalação e configuração do roteador CISCO ASR 1001-X/K9	15			22.500,00	337.500,00
	4	Instalação e configuração do roteador CISCO ISR 4451/K9	19			8.250,00	156.750,00
	5	Instalação e configuração do roteador CISCO ISR 4431/K9 ou ISR 4331/K9	71			8.250,00	585.750,00
	6	Instalação e configuração do Switch CISCO Catalyst C9200L	34			7.940,00	269.960,00
	7	Serviço de Suporte Técnico para a ROD por 12 meses	1			646.800,00	646.800,00
	8	Curso 300-501 SPCOR: Implementing and Operating Cisco Service Provider Network Core Technologies	11	12.550,00	138.050,00	22.200,00	244.200,00
	9	Curso 300-510 SPRI: Implementing Cisco Service Provider Advanced Routing Solutions	7	13.830,00	96.810,00	23.800,00	166.600,00
	10	300-515 SPVI: Implementing Cisco Service Provider VPN Services (SPVI)	7	13.830,00	96.810,00	23.800,00	166.600,00
	11	350-701 SCOR: Implementing and Operating Cisco Security Core Technologies (SCOR)	7	7.800,00	54.600,00	13.700,00	95.900,00
	12	350-801 CLCOR: Implementing and Operating Cisco Collaboration Core Technologies (CLCOR).	7	8.900,00	62.300,00	14.800,00	103.600,00

VALOR TOTAL

R\$ 4.844.910,00

R\$ 8.685.660,00

--	--	--

Por fim, considerando o contexto das empresas consultadas e visando uma maior economicidade para a Administração por meio do futuro certame, é de entendimento que se **deve considerar os valores mínimos na estimativa do custo total da contratação** da presente solução de TI ora pretendida.

– (IN. 01/2019, art. inciso III, alínea “a”)

6.11 – CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE (TCO) - (IN. 01/2019, art. 11, inciso III, letra “b”)

O TCO da ROD Segura está estimada na Tabela 6.7, com a previsão inicial de R\$ 6.058.260,93 (seis milhões e cinquenta e oito mil e duzentos e sessenta reais e noventa e três centavos).

Tabela 6.7. TCO da solução

Solução viável 1				
Categoria de Custos		Ano (R\$)		
		Ano 1	Ano 2	Ano 3
Custo Hardware (+)	Hardware 1	3.894.592,00	0,00	0,00
	Hardware 2	441.725,88	0,00	0,00
Custos de Software (+)	Licenças de Sistemas	0,00	43.705,26	0,00
	Licenças de Clientes	0,00	0,00	0,00

Custos de Implementação (+)	Implementação 1	710.832,10	0,00	0,00
Custos de Integração (+)	Integração 1	0,00	0,00	0,00
Custos de Treinamento(+)	Treinamento 1	448.570,00	0,00	0,00
Custos de Manutenção (+)	Manutenção 1	562.540,95	590.668,00	620.201,40
Custos de Materiais	Material 1	0,00	0,00	0,00
Custos de Operação (+)	Operação 1	0,00	0,00	0,00
Subtotal Custos / Ano		6.058.260,93	634.373,25	620.201,40
Custo de Descarte (+)		-	-	-
Valor de Descarte (-)		-	-	-
Custo Total		6.058.260,93	634.373,25	620.201,40

Aqui cabe ressaltar, para o TCO em questão, que o Custo de Descarte e o Valor de Descarte **não se aplicam** ao presente estudo, tendo em vista que os MSC são equipamentos de segurança e por isso:

- em caso de necessidade de descarte, serão destruídos em conformidade com as normas vigentes, a fim de que os requisitos de Segurança da Informação e das Comunicações (SIC) não sejam comprometidos; e
- estima-se que haverá reaproveitamento desses ativos para simulações e testes em laboratório.

6.12 – MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO) – (IN. 01/2019, art. 11, inciso III, alínea “a”)

Não se aplica neste estudo com base ao já exposto no item 3.1.

7. Descrição da solução como um todo

7.1 – DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA – (IN. 01/2019, art. 14)

7.1.1 – Bens e Serviços que compõem a solução

Conforme Tabela 2.1 deste estudo.

7.2 – Parcelamento da Solução de TIC Escolhida (IN. 01/2019, art. 12, §2º, inciso I)

O parcelamento da solução de TIC escolhida, exposto também no APÊNDICE XI deste estudo, está esclarecido na subseção 1.2 deste Estudo, a saber:

1. Módulo de Segurança Criptográfico;
2. Instalação e configuração de equipamentos de interconexão de rede já adquiridos;
3. Capacitação avançada para a equipe técnica do MD;
4. Contratação de empresa para suporte à Nova ROD.

8. Estimativa das Quantidades a serem Contratadas

8.1 – Parcelamento da Solução de TIC Escolhida (IN. 01/2019, art. 12, §2º, inciso I)

O parcelamento da solução de TIC escolhida, exposto também no APÊNDICE XI deste estudo, está esclarecido na subseção 1.2 deste Estudo, a saber:

1. Módulo de Segurança Criptográfico;
2. Instalação e configuração de equipamentos de interconexão de rede já adquiridos;
3. Capacitação avançada para a equipe técnica do MD;
4. Contratação de empresa para suporte à Nova ROD.

9. Estimativa do Valor da Contratação

9.1 – ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO - (IN. 01/2019, art. 20)

Com base na pesquisa de preços apresentado na seção 6 deste estudo, chegou-se na estimativa de Custo Total da Contratação listado na Tabela 8.1.

Tabela 8.1. estimativa de Custo Total da Contratação

Gp	Nr	Bem/Serviço	Qtd	Preço Unitário (R\$)	Preço Total (R\$)
1	1	Módulo de Segurança Criptográfico (100 Mbps) com garantia, instalação e configuração	151	25.792,00	3.894.592,00
	2	Módulo de Segurança Criptográfico (1 Gbps) com garantia, instalação e configuração	4	110.431,47	441.725,88
	3	Instalação e configuração do roteador CISCO ASR 1001-X/K9	15	5.113,90	76.708,50

2	4	Instalação e configuração do roteador CISCO ISR 4451/K9	19	5.113,90	97.16
	5	Instalação e configuração do roteador CISCO ISR 4431/K9 ou ISR 4331/K9	71	5.113,90	363.0
	6	Instalação e configuração do Switch CISCO Catalyst C9200L	34	5.113,90	173.8
	7	Serviço de Suporte Técnico para a ROD por 12 meses	1	562.540,95	562.5
	8	Curso 300-501 SPCOR: Implementing and Operating Cisco Service Provider Network Core Technologies	11	12.550,00	138.0
	9	Curso 300-510 SPRI: Implementing Cisco Service Provider Advanced Routing Solutions	7	13.830,00	96.81
	10	300-515 SPVI: Implementing Cisco Service Provider VPN Services (SPVI)	7	13.830,00	96.81
	11	350-701 SCOR: Implementing and Operating Cisco Security Core Technologies (SCOR)	7	7.800,00	54.60
	12	350-801 CLCOR: Implementing and Operating Cisco Collaboration Core Technologies (CLCOR).	7	8.900,00	62.30
VALOR TOTAL				R\$ 6.058.260,93	

10. Justificativa para o Parcelamento ou não da Solução

7.1 – Bens e Serviços que compõem a solução

Conforme Tabela 2.1 deste estudo.

11. Contratações Correlatas e/ou Interdependentes

Não se Aplica

12. Alinhamento entre a Contratação e o Planejamento

12.1 - ALINHAMENTO AOS PLANOS ESTRATÉGICOS DA ÁREA(IN01/2019 Art. 10, Inciso I)	
ID	Objetivos Estratégicos

OE 4	Prestar o suporte tecnológico aos assuntos estratégicos e internacionais, às operações conjuntas e à logística.
IE 4.2	Prover, aprimorar e manter em funcionamento seguro e ininterrupto os centros de comando e controle componentes e a infraestrutura do SISMC ² .
IE 4.3	Ampliar a interoperabilidade do Ministério da Defesa com as Forças Singulares

As referências ao alinhamento ao Planos Estratégicos da Secretaria Geral - SG podem ser encontradas nos links <http://intranet.defesa/index.php/informacoes-institucionais-superior/planejamento-estrategico-da-sg> e <https://www.governodigital.gov.br/EGD>.

12.2 - ALINHAMENTO AO PDTIC VIGENTE (IN01/2019 Art. 10, Inciso I)			
ID	Ação do PDTIC	ID	Meta do PDTIC associada
A 4.3.1	Ampliar a estrutura de enlaces terrestres e satelitais da ROD/SISCOMIS	M. 4.3.14	Ampliar a estrutura de enlaces terrestres e satelitais da ROD/SISCOMIS até o final de 2019. Buscando atingir o IADTIC em 75%

O PDTIC pode ser acessado por meio dos links <https://www.defesa.gov.br/legislacao> e <http://intranet.defesa/index.php/informacoes/34-programas-e-projetos/241-plano-diretor-de-tecnologia-da-informacao>.

13. Resultados Pretendidos

13.1 – Benefícios a serem alcançados com a aquisição (IN. 01/2019, art. 11, inciso v)

Conforme descrito na subseção 1.1 deste estudo.

14. Providências a serem Adotadas

14.1 - AS NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE PARA EXECUÇÃO CONTRATUAL - (IN. 01/2019, art 11, inciso II, alínea “e”)

Em estudo preliminar realizado nos compartimentos e na infraestrutura do Ministério da Defesa que hospedarão a solução em tela, não foram identificadas necessidades de readequação do espaço físico, climatização, rede elétrica e segurança orgânica.

14.2 – Infraestrutura Tecnológica

Esta solução não implicará em alterações no ambiente de rede atual da ROD e do SISCOMIS.

14.3 – Infraestrutura Elétrica

Esta solução não implicará em alterações no ambiente atual da ROD e do SISCOMIS de provimento de energia elétrica nos pontos onde será empregada.

14.4 – Logística

Esta solução implicará em geração de logísticas para a sua implementação, já especificada no APÊNDICE XI deste estudo.

14.5– Espaço Físico

Os espaços físicos dos locais de instalação da solução já estão adequados para a sua implementação.

14.6– Mobiliário

Não haverá necessidade de adequação de mobiliário, uma vez que será empregado *racks* já existentes nas Organizações que abrigarão os equipamentos da solução pretendida.

4.6 – Outras que se apliquem

Não foram verificadas outras necessidades, que não as já especificadas nesse estudo.

15. Possíveis Impactos Ambientais

Não se aplica

16. Declaração de Viabilidade

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

16.1. Justificativa da Viabilidade

16.1 – Justificativa Solução Escolhida - (IN. 01/2019, art. 11, inciso v)

Conforme a seção 3 – ANÁLISE DE SOLUÇÕES e na seção 5 - REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS deste estudo.

17. Responsáveis

JOSÉ EDUARDO FRANÇA - MAJ (EB)
INTEGRANTE TÉCNICO

CLAUBER GUIMARÃES RÊGO - CEL (EB)
INTEGRANTE REQUISITANTE

ANTÔNIO CARLOS DA COSTA PEREIRA - CAPITÃO DE MAR E GUERRA (EN)
AUTORIDADE MÁXIMA DA ÁREA DE TIC

Lista de Anexos

Atenção: alguns arquivos digitais enumerados abaixo podem ter sido anexados mesmo sem poderem ser impressos.

- Anexo I - Apendice_I____Especificacoes_Tecnicas_TR_v5.pdf (1.82 MB)