

APÊNDICE XI AO TERMO DE REFERÊNCIA DA CONTRATAÇÃO DO MD
ESPECIFICAÇÕES TÉCNICAS DA ROD SEGURA

Sumário

1. DESCRIÇÃO DA SOLUÇÃO DE TI.....	1
1.1. Objeto.....	1
1.2. Definições.....	2
1.3. Escopo da solução de TI.....	2
2. MÓDULOS CRIPTOGRÁFICOS.....	5
2.1. MÓDULO DE SEGURANÇA CRIPTOGRÁFICO (100 Mbps).....	5
2.2. MÓDULO DE SEGURANÇA CRIPTOGRÁFICO (1 Gbps).....	6
2.3. GARANTIA DOS MÓDULOS CRIPTOGRÁFICOS.....	7
2.4. INSTALAÇÃO E CONFIGURAÇÃO DOS MÓDULOS CRIPTOGRÁFICOS.....	9
3. SERVIÇOS.....	17
3.1. INSTALAÇÃO E CONFIGURAÇÃO DOS ATIVOS DE REDE.....	17
3.2. SERVIÇO DE SUPORTE TÉCNICO PARA A NOVA ROD.....	21
3.3. TREINAMENTOS OFICIAIS DA CISCO.....	28
4. DAS CONDIÇÕES DE RECEBIMENTO E HABILITAÇÕES.....	29
4.1. CONDIÇÕES DE RECEBIMENTO DOS EQUIPAMENTOS E DOS SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO....	29
4.2. SEGURANÇA DA INFORMAÇÃO.....	31
5. CONSIDERAÇÕES FINAIS.....	33
ADENDO A – PROPOSTA DE SOLUÇÃO PARA A NOVA ROD.....	35
ADENDO B – LOCALIZAÇÃO DAS ORGANIZAÇÕES E DOS TERMINAIS SATELITAIS.....	43
ADENDO C – LOCALIZAÇÃO DA INSTALAÇÃO DOS ATIVOS DE REDE.....	47
ADENDO D – MODELOS DE TELAS DE MONITORAMENTO.....	49
ADENDO E – NÍVEIS MÍNIMOS DE SERVIÇOS (NMS).....	55

1. DESCRIÇÃO DA SOLUÇÃO DE TI

1.1. Objeto

1.1.1. Contratação de EED para prover o fornecimento, instalação e configuração de PED Módulo de Segurança Criptográfico (MSC), caracterizando um Sistema Criptográfico de dados corporativos trafegados através de uma rede de comunicações, que obrigatoriamente deve atender aos requisitos de inserção de algoritmo criptográfico de Estado, e ainda a contratação de empresas para a instalação, configuração e suporte remoto de equipamentos (ativos) de interconexão de rede, já adquiridos, bem como para capacitação avançada à equipe técnica do MD, a fim de atualizar a Rede Operacional de Defesa (ROD), visando também a implantação da Rede de Passagem.

1.2. Definições

1.2.1. Para fins de simplificação, define-se:

1.2.1.1. **Nova ROD:** solução de TI a ser obtida que atualizará a atual Rede Operacional de Defesa (ROD), visando a implantação da Rede de Passagem (RP);

1.2.1.2. **Solução MSC:** solução de TI a ser obtida por meio do fornecimento, instalação e configuração dos Módulos de Segurança Criptográfico (MSC), os quais estabelecerão os túneis seguros sobre a Nova ROD, definindo um Sistema Criptográfico de Tráfego de Dados sobre uma rede IP, o qual obrigatoriamente deve atender aos requisitos de inserção de Algoritmo Criptográfico de Estado; e

1.2.1.3. **ROD Segura:** é a composição das soluções Nova ROD e Solução MSC.

1.3. Escopo da solução de TI

1.3.1. A solução de TI de que se trata a presente especificação tem como objetivo permitir a atualização da Rede Operacional de Defesa (ROD) visando implantar uma Rede de Passagem (RP) adequada, com o intuito de assegurar, às atividades operacionais de defesa, soluções cibernéticas seguras, flexíveis e versáteis.

1.3.2. No campo da segurança da informação, a solução MSC garantirá o sigilo das informações trafegadas pela ROD.

1.3.3. Para atender essas demandas do negócio, a atual topologia da ROD, diagramada nas Figuras 1 e 2 do ADENDO A – PROPOSTA DE SOLUÇÃO PARA A NOVA ROD desta especificação, será atualizada para a da **ROD Segura**, conforme Figuras 3 e 5 também do ADENDO A.

1.3.4. Na atual topologia da ROD, deve-se observar, conforme exposto da Figura 2, que:

1.3.4.1. há dois núcleos, que são redes metropolitanas:

1.3.4.1.1. Núcleo Brasília, composto pelos seguintes nós:

1.3.4.1.1.1. MD (SC1);

1.3.4.1.1.2. DTS; e

1.3.4.1.1.3. 7º CTA

1.3.4.1.2. Núcleo Rio de Janeiro, composto apenas pelo nó ERM RJ.

1.3.4.2. Esses dois núcleos tem dependência de uma única empresa, a qual também conecta outros pontos da ROD espalhados pelo país.

1.3.5. Para a **Solução MSC**, deve-se interpretar que:

1.3.5.1. os MSC são representados pelos cadeados presentes nas Figuras 3 e 5.

1.3.5.2. já os túneis seguros estão representados pelas setas tracejadas da Figura 5.

1.3.6. Já a arquitetura para a **Nova ROD** está caracterizada na Figura 4 do ADENDO A, possuindo diversos módulos interconectados, dos quais se destacam:

1.3.6.1. **Rede de Passagem (RP)**, que possui ainda um sub-módulo **CORE**;

1.3.6.2. **MD** (Ministério da Defesa) ou **FS** (Força Singular), que agrega os seguintes sub-módulos:

1.3.6.2.1. **Edge**, que é a interface com o backbone de integração e concentra principalmente ativos responsáveis pelos serviços de rede e pela segurança da informação da região;

1.3.6.2.2. **DC CORE**, onde ocorre a comutação de dados entre os DC e os servidores da Defesa; e

1.3.6.2.3. **DC** (ou **vDC**), que é o ambiente de hospedagem dos servidores da Defesa.

1.3.7. Para atender a Nova ROD, observa-se a necessidade de se constituir quatro instâncias de roteadores (Figura 4 do ADENDO A):

1.3.7.1. roteadores centrais da RP, caracterizados pela sigla **P**, responsáveis pela rápida comutação de pacotes da Nova ROD;

1.3.7.2. roteadores de borda da RP, caracterizados pela sigla **PE**, que interfaceiam com as demais organizações (Presidência da República – PR –, MD ou FS) e permitem o tráfego, segregado ou não, dos dados de Defesa; e

1.3.7.3. ativos de borda da organização, caracterizados pela sigla **CE**, que definem o limite entre a RP e as organizações. Esses ativos podem ser os roteadores enumerados na Tabela 1 ou da própria organização (*firewall*, roteador ou *switch* L3); e

1.3.8. A Nova ROD possuirá enlaces de comunicações em uma trama redundante e versátil, independentemente dos tipos canais sobre os quais esses enlaces estarão assentados. Essa versatilidade será garantida pelos equipamentos já adquiridos, os quais serão instalados conforme Tabela 1 e cuja distribuição conceitual está ilustrada na Figura 6.

Tabela 1: quantidade de equipamentos que serão instalados

	Mínima	Provável	Máxima
CISCO ASR 1001-X	5	11	15
CISCO ISR 4451-X	8	19	19
CISCO ISR 4431	24	56	71
CISCO Catalyst C9200L	19	29	34
TOTAL	56	115	132

1.3.9. Conforme proposta diagramada na Figura 3, a aludida trama deve:

1.3.9.1. viabilizar a criação de diversas VPN, segregadas ou não, de modo a proporcionar um trânsito, flexível ou não, dos dados operacionais entre o MD e as Forças, adotando o Multi-Protocol Label Switching (**MPLS**), definido pelas RFC 3031, 6178 e 6790;

1.3.9.2. estender a ROD sobre a Internet por meio de túneis seguros e dinâmicos;

1.3.9.3. permitir o uso, como cliente, do Carrier Supporting Carrier (CSC), definido pelas RFC 4364, 4577, 4684 e 5462; e

1.3.9.4. proporcionar tráfego IPv4 e IPv6.

1.3.10. Cabe ressaltar que o protocolo de roteamento IGP da RP poderá ser, a critério do CONTRATANTE, o OSPF ou EIGRP.

1.3.11. Ainda conforme proposta da Figura 3, essa rede MPLS irá rearranjar, pelo menos, os dois núcleos:

1.3.11.1. O Núcleo Brasília, com a seguinte disposição:

1.3.11.1.1. 7º CTA, com ativos P e PE;

1.3.11.1.2. MD (SC1), com ativos PE; e

1.3.11.1.3. DTS, com ativos PE.

1.3.11.2. O Núcleo Rio de Janeiro, com a seguinte disposição:

1.3.11.2.1. ERM RJ, com ativos P e PE; e

1.3.11.2.2. 2º CTA, com ativos PE.

1.3.12. Já conforme proposta da Figura 7, poderá ser ativado o Núcleo Manaus, o qual será agregado à rede MPLS¹, com a seguinte disposição:

1.3.12.1. 4º CTA, com ativos P e PE; e

1.3.12.2. DTCEA, com ativos PE.

1.3.13. A ROD também possui os ativos de segurança listados na Tabela 2, os quais também fazem parte do escopo do 3.1 deste apêndice, mas apenas para assessorar a configuração desses ativos e a resolução de eventuais problemas e incidentes, **não havendo a necessidade de ações para monitoramento, geração de alertas e relatórios (também não sendo necessário suporte do fabricante).**

Tabela 2: lista de ativos de segurança da Nova ROD

Equipamento	Quantidade
ASA 5510	4
Checkpoint 12000	2
Palo Alto PA-3020	1

1.3.14. A ROD ainda possui os ativos do segmento espacial listados na Tabela 3, os quais também fazem parte do escopo do 3.1 deste apêndice, mas apenas para o monitoramento, geração de alertas (identificar e alarmar) e relatórios, **não havendo a necessidade de ações para configuração e resolução de problemas e incidentes (também não sendo necessário suporte do fabricante).**

Tabela 3: lista de ativos do segmento espacial da Nova ROD

Equipamento	Quantidade
CDM-625A	36
CDM-625	103

1.3.15. A Tabela 4 apresenta a lista de bens e serviços previstos na presente contratação.

Tabela 4: lista de bens e serviços da solução de TI

Gp	Item	Bem/Serviço	Unid	Qtd
1	1	Módulo de Segurança Criptográfico (100 Mbps) com garantia, instalação e configuração	Un	151

1. Isso não exclui a rede contratada ilustrada na Figura 3.

Gp	Item	Bem/Serviço	Unid	Qtd
	2	Módulo de Segurança Criptográfico (1 Gbps) com garantia, instalação e configuração	Un	4
2	3	Instalação e configuração do roteador CISCO ASR1001-X/K9	Un	15
	4	Instalação e configuração do roteador CISCO ISR 4451/K9	Un	19
	5	Instalação e configuração do roteador CISCO ISR 4431/K9 ou ISR 4331/K9	Un	71
	6	Instalação e configuração do Switch CISCO Catalyst C9200L	Un	34
	7	Serviço de Suporte Técnico para a ROD por 12 meses	Serviço	1
	8	Curso 300-501 SPCOR : Implementing and Operating Cisco Service Provider Network Core Technologies	Por pessoa	11
	9	Curso 300-510 SPRI : Implementing Cisco Service Provider Advanced Routing Solutions	Por pessoa	7
	10	Curso 300-515 SPVI : Implementing Cisco Service Provider VPN Services (SPVI)	Por pessoa	7
	11	Curso 350-701 SCOR : Implementing and Operating Cisco Security Core Technologies (SCOR)	Por pessoa	7
	12	Curso 350-801 CLCOR : Implementing and Operating Cisco Collaboration Core Technologies (CLCOR)	Por pessoa	7

2. MÓDULOS CRIPTOGRÁFICOS

2.1. MÓDULO DE SEGURANÇA CRIPTOGRÁFICO (100 Mbps)

2.1.1. HARDWARE

- 2.1.1.1. Deve possuir pelo menos 3 (três) interfaces RJ45 com 100 Mbps;
- 2.1.1.2. Deve possuir no mínimo 3 (três) adaptadores de rede;
- 2.1.1.3. Deverá permitir ser acomodado em *rack* padrão 19”, devendo ser fornecido com todos os acessórios para tal;
- 2.1.1.4. Deve possuir no máximo 2 (duas) unidades de *rack* (*RU – Rack Units*);
- 2.1.1.5. Deve possuir cabos de alimentação padrão NBR14136;
- 2.1.1.6. Deve possuir interface de console para configuração;
- 2.1.1.7. Deve ser fornecido com cabo de console;
- 2.1.1.8. Deve ser fornecido com, pelo menos, uma interface USB externa em funcionamento, para armazenamento de configurações ou sistema operacional;
- 2.1.1.9. Deve possuir suporte de pelo menos 220 túneis seguros ativos, adotando o algoritmo de Estado;
- 2.1.1.10. Deve possuir alimentação elétrica tensão de 100V a 240V, frequência de 60Hz;
- 2.1.1.11. Deve ser posteriormente registrado, na forma da lei, como um Produto Estratégico de Defesa;
- 2.1.1.12. Deve possuir 100% (cem por cento) de conteúdo nacional para algoritmo criptográfico e com o mínimo de 60% (sessenta por cento) para o equipamento;

- 2.1.1.13. Deve possuir, preferencialmente em português, manuais para instalação, configuração e manutenção de todos seus equipamentos, bem como manuais de uso das API's e bibliotecas de programação.

2.1.2. COMPATIBILIDADE

- 2.1.2.1. Deve ser compatível com:

- 2.1.2.1.1. IPv4 e IPv6, inclusive para o uso do algoritmo de Estado e para a preservação dos respectivos campos reservados para o QoS;
- 2.1.2.1.2. Padrão IEEE 802.3 (Ethernet);
- 2.1.2.1.3. SNMPv3;
- 2.1.2.1.4. NTP ou SNTP.

2.1.3. PERFORMANCE

- 2.1.3.1. Deve possuir desempenho de pelo menos 100 Mbps full-duplex com algoritmo de Estado;
- 2.1.3.2. Deve suportar topologias e características como:
 - 2.1.3.2.1. estabelecer túneis seguros ponto-a-ponto e ponto-a-multiponto;
 - 2.1.3.2.2. autoajustável diante de uma falha do servidor central (hub), permitindo com que qualquer nó se torne um novo servidor.
- 2.1.3.3. Deve possuir os seguintes modos de operação:
 - 2.1.3.3.1. Modo Bridge e Gateway;
 - 2.1.3.3.2. Operação de forma transparente.

2.1.4. LICENCIAMENTO

- 2.1.4.1. Deve embarcar o algoritmo de Estado atendendo as especificações previstas nas normas do Departamento de Segurança da Informação do GSI, conforme definido pela NC 09/IN01/DSIC/GSI/PR, de 15 de julho de 2014;
- 2.1.4.2. O algoritmo de Estado deve estar posteriormente **homologado pelo GSI**, conforme definido pela NC 09/IN01/DSIC/GSI/PR, de 15 de julho de 2014;
- 2.1.4.3. Deve ser fornecido todo o licenciamento e *feature set* necessários para a implementação das funcionalidades requeridas;
- 2.1.4.4. As licenças são de caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de *técnica/software* com o fabricante ou seu representante.

2.2. MÓDULO DE SEGURANÇA CRIPTOGRÁFICO (1 Gbps)

- 2.2.1. Deve atender todas as especificações contidas no item 2.1.
- 2.2.2. Deve ainda possuir:
 - 2.2.2.1. pelo menos 2 (duas) interfaces SFP e 1 (uma) interface RJ45 com 1000 Mbps;
 - 2.2.2.2. possuir fonte redundante com mecanismo de chaveamento automático.

2.3. GARANTIA DOS MÓDULOS CRIPTOGRÁFICOS

- 2.3.1. O presente serviço está relacionado e agregado aos equipamentos e seus componentes previstos nos itens 2.1 e 2.2.
- 2.3.2. 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.
- 2.3.3. 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.
- 2.3.4. 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, devendo observar os itens 2.4.16 e 2.4.17.
- 2.3.5. 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.
- 2.3.6. 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.
- 2.3.7. 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.
- 2.3.8. 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.
- 2.3.9. 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.
- 2.3.10. Qualquer despesa decorrente da manutenção ou suporte realizados durante o período de garantia dos produtos instalados será de responsabilidade da CONTRATADA.
- 2.3.11. 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.
- 2.3.12. A recuperação de equipamento deverá atender os prazos estabelecidos na Tabela 12 deste apêndice. Nesses casos, deve ser apresentado obrigatoriamente relatório técnico com, pelo menos, as seguintes informações:
 - 2.3.12.1. Código da unidade;
 - 2.3.12.2. Número de série;

- 2.3.12.3. Falha informada;
 - 2.3.12.4. Falha constatada;
 - 2.3.12.5. Causa da falha;
 - 2.3.12.6. Ação para correção;
 - 2.3.12.7. Componentes substituídos/ajustes realizados.
- 2.3.13. 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).
- 2.3.14. 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:
- 2.3.14.1. Número de série da unidade substituta e substituída (no caso de substituição da unidade enviada); e
 - 2.3.14.2. Razão da substituição da unidade (quando for caso).
- 2.3.15. 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.
- 2.3.16. O CONTRATANTE rejeitará e devolverá à CONTRATADA qualquer unidade reparada ou substituta, sempre que constatar:
- 2.3.16.1. dano em qualquer de suas partes, observadas em inspeção visual;
 - 2.3.16.2. funcionamento fora das especificações originais;
 - 2.3.16.3. defeito constatado durante a execução de testes para verificação de funcionamento.
- 2.3.17. 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.
- 2.3.18. Caso uma nova falha seja identificada já com o equipamento em operação, deverá ser aberto um novo chamado, obedecendo os tempos de reparação supracitados.
- 2.3.19. Ficará ainda a cargo da CONTRATADA, o apoio no suporte aos equipamentos durante a vigência da garantia, incluindo os seguintes serviços:
- 2.3.19.1. 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;
 - 2.3.19.2. 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;
 - 2.3.19.3. 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;

- 2.3.19.4. 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;
- 2.3.19.5. Cada configuração (ou reconfiguração) deve garantir o acesso remoto ao CONTRATANTE; e
- 2.3.19.6. 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*.
- 2.3.20. Considerando o disposto no art. 9º do Decreto nº 7.970, de 28 de março de 2013, a CONTRATADA deve apresentar garantias para que, no caso de descontinuidade da produção do MSC ou na ocorrência do encerramento da pessoa jurídica relativa à área estratégica de defesa, sem sucessor equivalente que garanta a sua perenidade, seja assegurada a continuidade das capacitações tecnológica e produtiva no País, tais como:
 - 2.3.20.1. transferência à União, quando requisitado, da tecnologia relacionada aos PED;
 - 2.3.20.2. disponibilização da capacidade tecnológica e produtiva para outras EED;
 - 2.3.20.3. autorização da produção, sob licença, por outras EED;
 - 2.3.20.4. transferência da propriedade intelectual;
 - 2.3.20.5. ressarcimento dos investimentos realizados pela União; ou
 - 2.3.20.6. apresentação de garantias reais.
- 2.3.21. A fim de resguardar o segredo industrial, e para cumprimento de composição dos dados estatísticos do setor, a CONTRATADA deverá encaminhar ao Ministério da Defesa e ao Ministério da Economia, relatórios anuais dos resultados sobre a produção, o comércio e o mercado de trabalho, e dos impactos sobre a cadeia da base industrial de defesa, conforme ato conjunto dos Ministros de Estado da Defesa e da Economia (art. 10 do Decreto nº 7.970/2013).

2.4. INSTALAÇÃO E CONFIGURAÇÃO DOS MÓDULOS CRIPTOGRÁFICOS

- 2.4.1. 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.
- 2.4.2. 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.
- 2.4.3. Os serviços de instalação e configuração para os equipamentos fornecidos serão executados nas Organizações envolvidas nesta especificação.
 - 2.4.3.1. As configurações mais avançadas poderão ser feitas remotamente.
- 2.4.4. 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.
- 2.4.5. 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.
- 2.4.6. Os serviços deverão ser planejados conforme cronograma previsto em Plano de Implantação (instalação e configuração), cujos requisitos estão enumerados no item 2.4.10.
- 2.4.7. A CONTRATADA deverá elaborar os seguintes documentos que caracterizarão cada fase da instalação e configuração dos equipamentos:

- 2.4.7.1. **Site Survey**, definida no item 2.4.11;
- 2.4.7.2. **Design da Solução MSC**, definido no item 2.4.12, o qual apresenta o modelo conceitual de toda a solução;
- 2.4.7.3. **Plano de Implantação**, definido no item 2.4.13; e
- 2.4.7.4. **As-built** das implantações, definida no item 2.4.14.
- 2.4.8. Essa documentação deve atentar para as diretrizes técnicas relacionadas à Solução MSC enumeradas no 2.4.10
- 2.4.9. A fase final da implantação da solução é caracterizada pelo Período de Funcionamento Experimental (PFE), conforme esclarecido em 2.4.15.
- 2.4.10. Diretrizes técnicas para a implantação dos módulos criptográficos e da solução
 - 2.4.10.1. 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.
 - 2.4.10.2. 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.
 - 2.4.10.2.1. Caso haja a possibilidade de um arranjo dinâmico e spoke-and-spoke, o CONTRATANTE poderá exigir à CONTRATADA essa técnica.
 - 2.4.10.3. 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.
 - 2.4.10.3.1. A instalação nos TS estará condicionada a coordenação futura com o CONTRATANTE, respeitando a Tabela 8; e
 - 2.4.10.3.2. Já a instalação dos MSC nas Organizações deve ocorrer nos endereços indicados na Tabela 9 do ADENDO B.
- 2.4.11. Site Survey
 - 2.4.11.1. O *Site Survey* inicia-se com um diagnóstico da situação atual da ROD, o qual deve contemplar no mínimo:
 - 2.4.11.1.1. 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);
 - 2.4.11.1.2. a revisão da arquitetura atual da rede sob a ótica da solução de TI ora contratada; e
 - 2.4.11.1.3. o levantamento de eventuais óbices e pontos de falhas que possam prejudicar a implantação da Solução MSC.
 - 2.4.11.2. 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.
 - 2.4.11.2.1. 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.
 - 2.4.11.2.2. A não implantação dos equipamentos por consequência da falta ou imprecisão desses dados não acarretará em ônus ao CONTRATANTE.
 - 2.4.11.3. 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):
 - 2.4.11.3.1. verificação de espaço necessário para a instalação dos equipamentos;

2.4.11.3.2. 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

2.4.11.3.3. disponibilidade de pontos de dados, elétrico/óptico nos *patch pannels*/DIO existentes.

2.4.11.4. 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.

2.4.12. Design da Solução

2.4.12.1. 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:

2.4.12.1.1. *site survey* realizado na etapa anterior;

2.4.12.1.2. *design* lógico (camada 3), apresentando as características superficiais da solução fornecida;

2.4.12.1.3. registro dos possíveis riscos do conceito adotado e a forma de mitigação; e

2.4.12.1.4. registro dos requisitos de segurança e robustez, incluindo políticas de segurança para os elementos de rede.

2.4.12.2. Esse *design* precisa ser aprovado para que a etapa seguinte seja autorizada pelo CONTRATANTE.

2.4.13. Plano de Implantação (ou Plano de Inserção)

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

2.4.13.1.1. **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:

2.4.13.1.1.1. a estratégia de implantação da rede, observando:

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

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

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

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

2.4.13.1.1.2.1. a topologia detalhada;

2.4.13.1.1.2.2. as boas práticas definidas nas RFC 7696 e 8221;

2.4.13.1.1.2.3. 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;

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

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

2.4.13.1.1.4. 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:

2.4.13.1.1.4.1. Plano de Testes;

2.4.13.1.1.4.2. Equipes;

2.4.13.1.1.4.3. Ambiente;

2.4.13.1.1.4.4. Caso de Testes;

2.4.13.1.1.4.5. Testes; e

2.4.13.1.1.4.6. Critérios de Aceitação.

2.4.13.1.1.5. 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;

2.4.13.1.1.6. o Plano de Contingenciamento e Resposta da solução em caso de falhas (*Troubleshooting Plan*), observando inclusive o item 4.2.6.

2.4.13.1.2. **Plano de Implantação da localidade ou LLD (*Low Level Design*)**: documento contendo o refinamento e o detalhamento das implantações configurações necessárias (vide item 2.4.13.1.2.2) que serão aplicadas em cada equipamento e técnica/*software*, tudo com base nas definições contidas no HLD (vide item 2.4.13.1.1).

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

2.4.13.1.2.2. Plano de Liberação

2.4.13.1.2.2.1. 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;

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

2.4.13.1.2.2.3. 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;

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

2.4.14. As-built

2.4.14.1. 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.

2.4.14.2. 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*:

2.4.14.2.1. *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*);

- 2.4.14.2.2. Diagrama unifilar do cabeamento;
- 2.4.14.2.3. Tabela de conexões origem e destino;
- 2.4.14.2.4. Levantamento Fotográfico; e
- 2.4.14.2.5. Atualização, sempre que couber, da documentação listada no item 2.4.7.

2.4.15. Período de Funcionamento Experimental

- 2.4.15.1. Define-se o Período de Funcionamento Experimental (PFE) como:
 - 2.4.15.1.1. o suporte fornecido para o presente Serviço de TI por um período de tempo após ele ter sido liberado.
 - 2.4.15.1.2. o período correspondente entre:
 - 2.4.15.1.2.1. a configuração do primeiro túnel seguro; e
 - 2.4.15.1.2.2. 30 dias após a implantação do último túnel previsto no Plano de Implantação
- 2.4.15.2. 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.
- 2.4.15.3. Assim, a solução deverá demonstrar que não degradará mais de 10% o desempenho da rede.
- 2.4.15.4. 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.
- 2.4.15.5. Apenas após a finalização dos testes de cada implantação, o PFE dos equipamentos.
- 2.4.15.6. Durante o PFE, devem ser sanados eventuais problemas de implantação e operação que venham surgir.
- 2.4.15.7. O PFE é considerado finalizado se, após 30 (trinta) dias corridos, não for identificado pelo CONTRATANTE quaisquer problemas na solução ou no equipamento implantado.
- 2.4.15.8. 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.
- 2.4.15.9. 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.
- 2.4.15.10. O Termo de Recebimento Provisório, que é emitido para cada equipamento, deve incluir a data em que o PFE foi finalizado, a fim de aferir o seu encerramento.
- 2.4.15.11. 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) dias corridos.
- 2.4.15.12. 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.

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

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

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

2.4.15.15.1. Desinstalação/reinstalação dos equipamentos; e

2.4.15.15.2. Configuração/alteração de quaisquer funcionalidades dos equipamentos.

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

2.4.15.17. A Operação Assistida será exercida por uma Central de Serviços (CS) concebida pela CONTRATADA, observando o item 2.4.16.

2.4.16. Central de Serviços (CS)

2.4.16.1. 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.

2.4.16.2. 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).

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

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

2.4.16.4.1. solicitações de suporte técnico; e

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

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

2.4.16.6. 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.

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

2.4.17. Chamados

2.4.17.1. Os atendimentos aos chamados serão classificados conforme sua severidade, a critério do CONTRATANTE, e devem ser executados de acordo com a Tabela 5.

Tabela 5. Descrição do nível de severidade

Severidade	Descrição	Tipo de Atendimento	Tempo de Atendimento	Tempo de Solução	Tempo para Solução Definitiva
1 Alta	Chamados associados às situações de alto impacto, incluindo os casos de degradação severa de	On-site ou Remoto*	No máximo 2 (duas) horas após a abertura do chamado	Até 10 (dez) horas contadas após início do atendimento	Até 5 (cinco) dias contadas após início do atendimento

Severidade	Descrição	Tipo de Atendimento	Tempo de Atendimento	Tempo de Solução	Tempo para Solução Definitiva
	desempenho				
2 Média	Chamados referentes às situações de baixo impacto ou para aqueles problemas que se apresentam de forma intermitente, incluindo os casos em que haja a necessidade de substituição de componente(s) que possua(m) redundância	On-site ou Remoto*	No máximo 4 (quatro) horas após a abertura do chamado	Até 48 (quarenta e oito) horas contadas após início do atendimento	Até 15 (quinze) dias contadas após início do atendimento
3 Baixa	Chamados com o objetivo de sanar dúvidas quanto ao uso ou implementação do produto	Remoto	No máximo 24 (vinte quatro) horas após a abertura do chamado	No máximo 72 (setenta e duas) horas contadas após início do atendimento	-

(*) dependerá de necessidade de intervenção física

2.4.17.2. 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.

2.4.17.3. 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.

2.4.17.4. 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.

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

2.4.17.6. 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.

2.4.17.7. 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.

2.4.17.8. 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.

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

2.4.17.10. 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 na Tabela 6:

Tabela 6. Tipos de manutenções a serem prestadas pelo suporte técnico

Manutenção	Forma de Atendimento	Objetivo
Preventiva	Mensais ou a critério do CONTRATANTE via telefone, e-mail ou	Aquela que é realizada para aumentar a confiabilidade, evitar a ocorrência de falhas ou suas consequências e prolongar sua vida útil.

Manutenção	Forma de Atendimento	Objetivo
	presenciais.	
Corretiva	Presencial, <i>e-mail</i> ou telefone.	Aquela destinada a sanar incidentes apresentados no funcionamento do equipamento, compreendendo configurações, ajustes, reparos e correções necessárias para o perfeito funcionamento do <i>técnica/software</i> .

2.4.18. Transferência de Conhecimento

2.4.18.1. 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.

2.4.18.2. A transferência de conhecimento deverá ser:

2.4.18.2.1. presencial ou à distância preferencialmente;

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

2.4.18.2.1.1.1. 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.

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

2.4.18.2.3. difundido para até 15 (quinze) pessoas.

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

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

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

2.4.18.5.1. 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);

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

2.4.18.6. 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.

2.4.18.7. 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.

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

2.4.18.9. 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.

2.4.19. A CONTRATADA deve também atender, sempre que couber, os requisitos dispostos nos itens 4 e 5.

3. SERVIÇOS

3.1. INSTALAÇÃO E CONFIGURAÇÃO DOS ATIVOS DE REDE

3.1.1. 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 4.

3.1.2. A CONTRATADA deve obedecer todos os requisitos previstos no item 2.4, com exceção do subitem 2.4.10.

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

3.1.3.1. instalação e configuração dos equipamentos adquiridos nas Organizações;

3.1.3.2. acompanhamento dos serviços de instalação e configuração;

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

3.1.3.4. acompanhamento dos processos de gerenciamento dos serviços.

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

3.1.5. Os serviços deverão ser planejados conforme cronograma previsto em Plano de Implantação, cujos requisitos adicionais estão enumerados no item 3.1.6.

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

3.1.6.1. 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.

3.1.6.2. 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.

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

- 3.1.6.3.1. 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.
- 3.1.6.3.2. 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.
- 3.1.6.4. 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.
- 3.1.6.5. 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:
 - 3.1.6.5.1. Plano de Roteamento: que expõe o respectivo plano de custos dos caminhos de rede, de forma a permitir o balanceamento do tráfego;
 - 3.1.6.5.2. 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;
 - 3.1.6.5.3. 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;
 - 3.1.6.5.4. Plano de QoS: que inclui, dentre outros, as configurações necessárias para tratamento do tráfego de voz sobre IP (VoIP), *traffic shapping* etc;
 - 3.1.6.5.5. 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;
 - 3.1.6.5.6. 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;
 - 3.1.6.5.7. Plano de Segurança:
 - 3.1.6.5.7.1. 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;
 - 3.1.6.5.7.2. 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;
 - 3.1.6.5.7.3. deve-se definir fluxos e respectivos controles, podendo haver a necessidade de se definir VLANS;
 - 3.1.6.5.7.4. atentar para autenticação, autorização e *accounting* previsto no item 4.2.5.
 - 3.1.6.5.8. Plano de Reação Contra Ataques Cibernéticos: considerando inclusive, mas não limitado, o *Controller/Trigger Router* através da técnica *Remotely Triggered Black Hole (RTBH) filtering*;
 - 3.1.6.5.9. Plano de Monitoramento, que de prever:
 - 3.1.6.5.9.1. 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) e o Flexible NetFlow (FnF), com o intuito de garantir o adequado monitoramento dos equipamentos adquiridos;

3.1.6.5.9.2. 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 mensagem e o SNMPv3 ou *Model Drive Telemetry (Streaming Telemetry)*;

3.1.6.5.9.3. a configuração de ferramenta para gerenciamento (exemplo: Netbox) de IP, VLAN, VRF, componentes, *hacks*, conexão (de rede e elétrica), senhas, etc, dos ativos em questão;

3.1.6.5.9.4. 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;

3.1.6.5.9.5. 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, Loss de portadoras e Potência RF;

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

3.1.6.5.10. 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;

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

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

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

3.1.6.5.12. Plano de Transição, conforme descrito no item 3.1.7.

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

3.1.6.7. 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:

3.1.6.7.1. Laboratório físico, reaproveitando os equipamentos que serão substituídos ou remanejados, conforme item 3.1.6.5.10; e

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

3.1.7. Plano de Transição

3.1.7.1. 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.

3.1.7.2. Esse plano deve incluir, dentre outros:

3.1.7.2.1. entrega de versões finais da documentação;

3.1.7.2.2. transferência das responsabilidades entre as empresas;

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

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

3.1.7.2.5. transferência de perfis de acesso;

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

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

3.1.7.2.8. devolução de recursos, se for o caso.

3.1.8. Transferência de Conhecimento

3.1.8.1. 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:

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

3.1.8.1.1.1. 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;

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

3.1.8.1.1.3. Deve observar as regras previstas no ANO (vide 3.1.6.5.11); e

3.1.8.1.1.4. 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.

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

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

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

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

3.1.8.1.3.1. 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) e o Flexible NetFlow (FnF), com o intuito de garantir o adequado monitoramento dos equipamentos adquiridos;

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

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

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

3.1.8.1.4.2. abordar tópicos como MPLS com 6VPE;

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

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

3.1.8.1.4.3.2. servidores web ou e-mail e DNS;

3.1.8.1.4.3.3. equipamentos de segurança;

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

3.1.8.1.4.3.5. demais estações de trabalho;

3.1.8.1.4.3.6. dispositivos de VoIP e Videoconferência.

3.1.8.1.4.4. Deve observar as regras previstas no ANO (vide 3.1.6.5.11); e

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

3.1.9. A CONTRATADA deve também atender, sempre que couber, os requisitos dispostos nos itens 4 e 5.

3.2. SERVIÇO DE SUPORTE TÉCNICO PARA A NOVA ROD

3.2.1. 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.

3.2.2. Esses processos:

3.2.2.1. 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.

3.2.2.2. estão definidos ao longo desse apêndice, mas o detalhamento será delineado no Plano de Liberação (vide item 3.2.23).

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

3.2.3. 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.

3.2.3.1. 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.

3.2.3.2. 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).

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

3.2.5. Os serviços deverão ser planejados conforme cronograma previsto em Plano de Liberação (vide item 3.2.23), que será elaborado pela CONTRATADA, nos moldes preconizados pelas boas práticas do ITIL v3 ou v4.

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

3.2.6.1. Design atual da ROD;

3.2.6.2. As-built da ROD; e

3.2.6.3. 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.

3.2.7. 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.

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

3.2.8.1. atendimento dos chamados;

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

3.2.8.3. 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;

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

3.2.8.5. acompanhamento dos processos de gerenciamento dos serviços de TI suportados pela ROD.

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

3.2.10. Não haverá relação de subordinação e dependência entre os empregados integrantes da equipe da CONTRATADA e o CONTRATANTE.

- 3.2.11. 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.
- 3.2.12. A CONTRATADA deverá garantir os níveis mínimos de serviços, no que couber e sempre que possível, definidos no ADENDO E.
- 3.2.13. A CONTRATADA deverá oferecer uma Central de Serviços (CS) que executará as tarefas previstas no item 2.4.16.
- 3.2.14. O serviço de suporte técnico deverá contemplar ainda, dentre outras, atividades tais como:
 - 3.2.14.1. 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;
 - 3.2.14.2. 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
 - 3.2.14.3. Apoio técnico na recuperação de ambientes em caso de panes ou perda de dados, sendo que o *backup* das configurações é de responsabilidade da CONTRATADA, devendo, para tanto, usar os equipamentos do CONTRATANTE.
- 3.2.15. Gerenciamento de configuração
 - 3.2.15.1. 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.
 - 3.2.15.1.1. Engloba, ainda, a configuração dos parâmetros como os limites para que um alarme seja ativado e uma notificação seja enviada.
 - 3.2.15.2. 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.
 - 3.2.15.3. Suas principais funções são:
 - 3.2.15.3.1. coleta de informações;
 - 3.2.15.3.2. controle de inventário;
 - 3.2.15.3.3. início e encerramento das operações dos elementos gerenciados;
 - 3.2.15.3.4. alteração da configuração dos elementos; e
 - 3.2.15.3.5. geração de relatórios.
 - 3.2.15.4. Indicadores a serem elaborados semestralmente:
 - 3.2.15.4.1. Índice de Evolução de Itens de Configuração: Histórico semestral do número de IC registrados.
 - 3.2.15.4.2. Índice de não-conformidades de IC: Número de IC não-conformes com o Plano de Configuração/Número de IC Auditados no período
- 3.2.16. Gerenciamento de incidentes e problemas
 - 3.2.16.1. O objetivo deste gerenciamento é detectar e isolar possíveis incidentes e problemas que possam causar falhas significativas à ROD.
 - 3.2.16.2. Quando ocorrer um incidente ou problema, a CONTRATADA deve:

- 3.2.16.2.1. registrar o incidente ou problema;
- 3.2.16.2.2. determinar o local da falha;
- 3.2.16.2.3. isolar, para que o componente possa continuar a funcionar sem interferências;
- 3.2.16.2.4. reconfigurar a rede a fim de minimizar o impacto da operação sem o componente que falhou;
- 3.2.16.2.5. reparar o componente com problemas para restaurar a rede ao seu estado anterior;
- 3.2.16.2.6. gerar Base de Dados de Erros Conhecidos (BDEC).

3.2.16.3. Indicadores a serem elaborados bimestralmente:

- 3.2.16.3.1. 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
- 3.2.16.3.2. Índice de Resolução de Incidentes: Número de Incidentes Fechados no período (IF)/Número de Incidentes (I)
 - 3.2.16.3.2.1. $I = \text{Aberto} + \text{Em andamento} + \text{Resolvido} + \text{IF}$
- 3.2.16.3.3. Índice de Problemas Solucionados: Números de Problemas Fechados no período (PF)/Número de Problemas (P)
 - 3.2.16.3.3.1. $P = \text{Aberto} + \text{Em andamento} + \text{PF}$

3.2.17. Gerenciamento de Mudança

- 3.2.17.1. 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.
- 3.2.17.2. 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.
- 3.2.17.3. Suas principais funções são:
 - 3.2.17.3.1. Registrar Mudança;
 - 3.2.17.3.2. Avaliar Mudanças;
 - 3.2.17.3.3. Planejar e propor a mudança;
 - 3.2.17.3.4. Gerenciar e realizar a liberação;
 - 3.2.17.3.5. Revisar Mudança se for o caso; e
 - 3.2.17.3.6. Encerrar Mudança.
- 3.2.17.4. Indicadores a serem elaborados semestralmente:
 - 3.2.17.4.1. Índice de Evolução de Mudanças: Histórico do número de Mudanças Registradas nos últimos seis meses
 - 3.2.17.4.2. Índice de Mudanças Emergenciais Aprovadas: Número de Mudanças Emergenciais registradas/Número de Mudanças Registrados
 - 3.2.17.4.3. Índice de Mudanças Aprovadas: Número de Mudanças Aprovadas no período (MA)/Número de Mudanças (M)

3.2.18. Gerenciamento de desempenho

- 3.2.18.1. O objetivo deste gerenciamento é garantir a qualidade de exigida para a ROD.
- 3.2.18.2. Suas principais atividades são:
 - 3.2.18.2.1. monitorar o desempenho;
 - 3.2.18.2.2. caracterizar recarga de trabalho;

- 3.2.18.2.3. ajustar parâmetros;
- 3.2.18.2.4. identificar gargalos e corrigi-los;
- 3.2.18.2.5. comparar desempenho entre sistemas alternativos;
- 3.2.18.2.6. dimensionar os componentes do sistema;
- 3.2.18.2.7. gerar previsão de crescimento e tendências.

3.2.18.3. 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.

3.2.18.4. Indicadores a serem elaborados trimestralmente:

- 3.2.18.4.1. 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.)

3.2.19. Central de Serviços (CS)

3.2.19.1.1. 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.

3.2.19.1.2. A CS pode ser composta pela mesma equipe já caracterizada no item 3.2.8.

3.2.19.1.3. 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).

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

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

3.2.19.1.4.1. solicitações de suporte técnico; e

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

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

3.2.20. Monitoramento

3.2.20.1. 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 previso no item 3.1.6.5.9.

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

3.2.20.2. Todas as *views* de monitoramento devem estar disponibilizadas ao CONTRATANTE.

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

3.2.20.4. 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),

3.2.20.5. Deve contabilizar indicadores dos enlaces WAN, como perda de pacote, latência e jitter, gerando relatórios mensais.

3.2.20.6. 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.

3.2.20.7. Deve monitorar a “saúde” de todos equipamentos e enlaces que compõem a Nova ROD.

3.2.20.8. 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>>.

3.2.20.9. Esse sítio eletrônico deve ser elaborado pela CONTRATADA, e deve conter ainda:

3.2.20.9.1. informações sobre eventuais mudanças que possam causar degradação ou indisponibilidade da ROD, incluindo o cronograma das preventivas;

3.2.20.9.2. a situação dos enlaces e ativos em tempo real, mostrando em cores distintas o estado desses itens, como disponibilidade, indisponibilidade, inativo, etc;

3.2.20.9.3. os diagramas *on-line* apresentados no ADENDO D.

3.2.20.10. Os detalhes e ajustes desses relatórios serão definidos no Plano de Liberação.

3.2.20.11. 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.

3.2.21. Chamados

3.2.21.1. O atendimento aos chamados, que é remoto, serão classificados conforme o seu nível de severidade, a critério do CONTRATANTE, e devem ser executados de acordo com a Tabela 7.

Tabela 7. Descrição do nível de severidade

Nível	Descrição	Período	Tempo de Atendimento	Tempo de Resolução (Incidente)	Tempo para Solução Definitiva (Problema)
1 Alta	Chamados associados às situações de alto impacto, incluindo os casos de interrupção significativa do negócio e de degradação severa de desempenho	7h-19h	Até 20 (vinte) minutos após a abertura do chamado	Até 2 (duas) horas após início do atendimento	Até 5 (cinco) dias após início do atendimento
		19h-7h ou dia não útil	Até 1 (uma) hora após a abertura do chamado	Até 4 (quatro) horas após início do atendimento	
2 Média	Chamados referentes às situações de baixo impacto ou para aqueles problemas que se apresentam de forma intermitente	7h-19h	Até 1 (uma) hora após a abertura do chamado	Até 5 (cinco) horas após início do atendimento	Até 15 (quinze) dias após início do atendimento
		19h-7h ou dia não útil	Até 4 (quatro) horas após a abertura do chamado	Até 20 (vinte) horas após início do atendimento	
3 Baixa	Chamados com o objetivo de sanar dúvidas quanto ao uso ou implementação do produto	-	Até um dia útil após a abertura do chamado	No máximo 5 dias úteis	-

(*) dependerá de necessidade de intervenção física

3.2.21.2. 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.

3.2.21.3. 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.

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

3.2.21.5. 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.

3.2.21.6. 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.

3.2.22. Dos Relatórios Técnicos e documentos

3.2.22.1. 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.

3.2.22.2. 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.

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

3.2.22.4. 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 os prazos a partir da assinatura do contrato.

3.2.22.5. 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.

3.2.22.6. A CONTRATADA deverá atualizar o Plano de Transição (item 3.2.6.3) e seus anexos até três meses antes do encerramento do contrato.

3.2.23. Plano de Liberação (ou Plano de Inserção)

3.2.23.1. 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;

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

3.2.23.3. 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;

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

3.2.24. Período de Funcionamento Experimental

3.2.24.1. 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.

- 3.2.24.2. 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.
- 3.2.24.3. 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.
- 3.2.24.4. Durante o PFE, devem ser sanados eventuais problemas de implantação e operação que venham surgir.
- 3.2.24.5. O PFE é considerado finalizado se, após 15 (quinze) dias corridos, não for identificado pelo CONTRATANTE quaisquer problemas no serviço prestado.
- 3.2.24.6. 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.**
- 3.2.24.7. 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.
- 3.2.24.8. O Termo de Recebimento Provisório deve incluir a data em que o PFE foi finalizado, a fim de aferir o seu encerramento.

3.2.24.9. 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.

3.3. TREINAMENTOS OFICIAIS DA CISCO

3.3. Conforme justificado no item 3.1.1 do TR, é necessária a capacitação avançada para a equipe técnica do MD **sob a ótica do fabricante** do equipamento adquirido, este da empresa Cisco Systems.

3.4. Os treinamentos necessários da Cisco são:

3.4.1. Curso 300-501 SPCOR: Implementing and Operating Cisco Service Provider Network Core Technologies

3.4.2. Curso 300-510 SPRI: Implementing Cisco Service Provider Advanced Routing Solutions

3.4.3. Curso 300-515 SPVI: Implementing Cisco Service Provider VPN Services (SPVI)

3.4.4. Curso 350-701 SCOR: Implementing and Operating Cisco Security Core Technologies (SCOR)

3.4.5. Curso 350-801 CLCOR: Implementing and Operating Cisco Collaboration Core Technologies (CLCOR).

3.4.6. Condições Gerais dos para a realização dos treinamentos:

3.4.6.1. Os treinamentos devem ser oficiais do fabricante, podendo ser ministrados por um parceiro de treinamento certificado.

3.4.6.2. As ementas dos treinamentos devem conter as ementas oficiais do fabricante.

3.4.6.3. A carga horária dos treinamentos deve ser conforme estabelecida pelo fabricante, devendo o mesmo atestar que é compatível com a ementa definida.

- 3.4.6.4. Esses treinamentos devem ser realizados no formato Ensino à Distância (EAD).
- 3.4.6.5. 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.
- 3.4.6.6. O ambiente virtual dos treinamentos é de responsabilidade da CONTRATADA.
- 3.4.6.7. Deve haver *hands-on*, cujos laboratórios poderão ser baseados em equipamentos físicos ou virtuais.
- 3.4.6.8. 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.
- 3.4.6.9. Os treinamentos devem ser ministrados em português.
- 3.4.6.10. 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 instruídos não necessitem de qualquer outra bibliografia de apoio.
- 3.4.6.11. Deverá ser emitido certificado de participação ao final do curso a cada participante, detalhando programa e carga horária.
- 3.4.6.12. 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.
- 3.4.7. Deve ser fornecido o voucher mais atual para certificação, com validade de, no mínimo, 6 (seis) meses, para cada aluno do treinamento contratado.
- 3.4.8. Pode ser fornecido o ambiente de *e-learning* CISCO, com instrutor em português, sendo que, nesse caso:
 - 3.4.8.1. o instrutor deve usar o material do ambiente, inclusive os laboratórios;
 - 3.4.8.2. não há a obrigatoriedade, por parte da CONTRATADA, de entregar o material impresso; e
 - 3.4.8.3. 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.

4. DAS CONDIÇÕES DE RECEBIMENTO E HABILITAÇÕES

4.1. CONDIÇÕES DE RECEBIMENTO DOS EQUIPAMENTOS E DOS SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO

4.1.1. Condições Gerais

- 4.1.1.1. A instalação e a configuração devem ser feitas pelos técnicos da CONTRATADA, e estes devem ser certificados pelo fabricante dos produtos.
- 4.1.1.2. A implantação do equipamento ou solução será dado apenas após o ateste das características especificadas.
- 4.1.1.3. O CONTRATANTE indicará, a seu critério, equipe de profissionais de seu quadro para acompanhar e executar a entrega e a instalação da solução, em conjunto com os profissionais da equipe da CONTRATADA.

- 4.1.1.4. Todas as atividades de instalação e implantação desempenhadas pela CONTRATADA deverão ter, como preocupação primária, a transferência do conhecimento à equipe indicada pelo CONTRATANTE a acompanhar cada atividade.
- 4.1.1.5. As entregas e os serviços de instalação, configuração e implantação devem ser realizados em horários que não prejudiquem os processos de negócio do CONTRATANTE. O CONTRATANTE coordenará os horários para a realização dos serviços, presencial ou remotamente.

4.1.2. Dos Equipamentos (itens 1 e 2 da Tabela 4)

- 4.1.2.1. Os equipamentos devem ser novos, de primeiro uso e estar em linha de fabricação na data de entrega da solução.
- 4.1.2.2. Os equipamentos (*hardware*) e funcionalidades (*técnica/software*) ofertados na composição dos itens não devem estar listados como “*End of Sale*” e “*End of Life*” pelo fabricante até a data da abertura das propostas;
- 4.1.2.3. Para atendimento do Inciso III, Art. 3º do Decreto 7.174/2010, quando da entrega dos equipamentos, a CONTRATADA deverá comprovar a origem dos bens importados e apresentar comprovante de quitação dos tributos de importação a eles referentes, sob pena de suspensão do(s) pagamento(s), rescisão contratual e multa;
- 4.1.2.4. Antes da entrega e instalação do equipamento, a CONTRATADA deve avaliar as condições elétricas do local, de modo a evitar eventuais problemas de sobrecarga na rede ou queima de equipamento. Em caso de infortúnio provocado pela inobservância dessas condições, a CONTRATADA será responsabilizada.
- 4.1.2.5. O CONTRATANTE será responsável pelo provimento de energização e pontos de rede para instalação dos equipamentos, além da disponibilização de *racks*, *patch-panels*, distribuidores internos ópticos (DIO).
 - 4.1.2.5.1. Entretanto, cabe à CONTRATADA o fornecimento de cabos, cordões ópticos e adaptadores que vierem a ser necessários para a instalação e funcionamento dos equipamentos.
- 4.1.2.6. A CONTRATADA deve identificar os equipamentos a serem instalados, incluindo o cabeamento de rede.
- 4.1.2.7. Os equipamentos devem ser fornecidos conforme a voltagem onde eles serão instalados.
- 4.1.2.8. Os equipamentos deverão ser fornecidos com todos os itens acessórios de *hardware*, *firmware* e *técnica/software* necessários à sua perfeita instalação e funcionamento, incluindo cabos, conectores, interfaces, suportes, *drivers* de controle, programas de configuração, etc.
- 4.1.2.9. Deverá ser realizada a instalação, configuração e ativação de todos os *técnica/software* que acompanhem o equipamento, quando for o caso. Junto aos *técnica/software* fornecidos com os equipamentos, deverão ser fornecidos os respectivos Cartões de Registro.
- 4.1.2.10. Os equipamentos deverão estar acompanhados de sua documentação técnica completa e atualizada, contendo os manuais, guias de instalação e outros pertinentes. A documentação deverá ser fornecida em sua forma original, não sendo aceitas cópias de qualquer tipo.

- 4.1.2.11. Todas as características exigidas deverão ser comprovadas, independente da descrição da proposta, como catálogos, manuais e fichas de especificação técnica, sob pena, na falta destes, de não aceitação do equipamento ofertado.

4.1.3. Dos serviços de instalação e configuração

- 4.1.3.1. Quando solicitado, os serviços deverão ser testados e validados pelo CONTRATANTE. Para tanto, todos os serviços devem ser acompanhados por uma equipe técnica indicada pelo CONTRATANTE e só serão aceitos após a entrega e VALIDAÇÃO da solução.
- 4.1.3.2. O equipamento entregue só será considerado instalado quando ele estiver acondicionado respectivo local, cabeado, com capacidade de permitir acesso remoto por parte da equipe do CONTRATANTE, com as configurações inseridas e ativo em plenas condições de funcionamento.

4.2. SEGURANÇA DA INFORMAÇÃO

4.2.1. 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.

4.2.2. 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.

4.2.3. 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.

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

4.2.5. Da autenticação, autorização e *accounting*

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

4.2.5.2. 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.

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

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

4.2.5.5. 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.

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

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

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

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

4.2.5.10. 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).

4.2.5.11. 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.

4.2.6. Da Configuração e Backup

4.2.6.1. 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.

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

4.2.6.3. 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.

4.2.6.4. 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.

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

4.2.6.6. 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.

4.2.7. Logs e Auditoria

4.2.7.1. 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.

4.2.7.2. Os equipamentos devem ter o armazenamento local de *logs*, com informação completa de horário (*timestamp*).

4.2.7.3. Enviar esses *logs* para um servidor centralizado através do protocolo Syslog.

4.2.7.4. 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 inválidas, 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.

4.2.7.5. Os *logs* não deverão possuir senhas de usuários ou serviços.

4.2.8. Outros requisitos

4.2.8.1. 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.

- 4.2.8.2. A solução deve prover um meio de desabilitar os serviços não utilizados e todos os serviços desnecessários à operação devem ser desativados.
- 4.2.8.3. A CONTRATADA deve sugerir um modelo de configuração segura do equipamento, a qual deverá ser homologada pela equipe do CONTRATANTE.
- 4.2.8.4. 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.
- 4.2.8.5. Deve sincronizar de horário através dos protocolos NTP ou SNTP do CONTRATANTE
- 4.2.8.6. 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. CONSIDERAÇÕES FINAIS

- 5.1. As especificações serão conferidas por meio de verificação técnica dos *hardware*, manuais técnicos correspondentes às placas lógicas e periféricos, folhetos do fabricante contendo características técnicas e teste com *técnica/software* capaz de reconhecer a configuração do equipamento. Não serão aceitas cópias de manuais técnicos e discos de configuração/CD-ROM, mas somente exemplares originais.
- 5.2. Toda a documentação técnica deve ter nível de detalhes adequado para suportar a operação, administração, manutenção, customização, configuração dos produtos, assim como a integração destes com outros sistemas e desenvolvimentos futuros.
- 5.3. A transferência de tecnologia poderá, desde que de comum acordo, ser convertida em vagas para participação em eventos, nacional ou internacional, de atualização tecnológica promovidos pela CONTRATADA ou pelo fabricante da solução.
- 5.4. Durante a vigência do contrato e da garantia, poderão ser disponibilizadas, desde que de comum acordo, vagas anuais para participação em eventos técnicos, nacionais ou internacionais, sem custo adicional ao CONTRATANTE, para atualização tecnológica.
- 5.4.1. Entende-se por eventos de técnicos: *Workshops*, Seminários, Fóruns, Feiras Tecnológicas, Visitas técnicas e/ou Treinamento em Fábricas, Datacenters e/ou Laboratórios do fabricante/fornecedor da solução, entre outros com o mesmo propósito.
- 5.5. Todas as despesas para a realização e participação dos empregados indicados pelo CONTRATANTE (inscrição, passagem, hospedagem e locomoção) deverão ser integralmente custeados pela CONTRATADA.
- 5.6. Toda documentação citada nesta especificação a ser elaborada pela CONTRATADA deve conter no mínimo:
 - 5.6.1. Introdução;
 - 5.6.2. Propósito;
 - 5.6.3. Definições, Acrônimos e Abreviações, como:
 - 5.6.3.1. Contratada;
 - 5.6.3.2. N° do Contrato;
 - 5.6.3.3. Área Requisitante da Solução;
 - 5.6.3.4. Gestor do Contrato;
 - 5.6.3.5. Fiscal Requisitante;
 - 5.6.3.6. Fiscal Técnico; e
 - 5.6.3.7. Fiscal Administrativo.

- 5.6.4. Referências, em especial dos documentos da aquisição;
 - 5.6.5. Conteúdo principal, observado os parâmetros de cada documento definidos a seguir; e
 - 5.6.6. Critérios de Aceitação.
- 5.7. Caso essa documentação não seja aprovada pelo pelos técnicos do MD, a empresa deverá refazer a documentação sem ônus para o CONTRATANTE.
- 5.8. Toda essa documentação deve ser entregue impressa e em mídia digital (pdf e editável).
- 5.9. A emissão dos Termos de Aceite Definitivo, bem como o desembolso financeiro, estará também condicionada ao fornecimento de documentação prevista e, ainda, às observações e eventuais pendências apontadas no Termo de Recebimento Provisório.
- 5.10. O fornecimento dos cabos necessários para a interligação dos equipamentos é de responsabilidade da CONTRATADA.
- 5.11. Fica a critério do CONTRATANTE autorizar ou não a execução de uma atividade prevista nesta especificação, principalmente para os estágios da presente solução de TI que são dependentes. Assim, a CONTRATADA não poderá requerer pagamentos caso o cadenciamento das atividades não seja cumprido adequadamente.
- 5.12. Na hipótese da CONTRATADA não sanar as pendências relacionadas ao fornecimento dos bens e serviços previstos, serão iniciados os procedimentos de penalidades previstas na seção 7 do TR e no ADENDO E.