



CONTROLADORIA-GERAL DA UNIÃO
Divisão de Contratações de TI
Setor de Autarquias Sul Quadra 1 Bloco A, Edifício Darcy Ribeiro - Bairro Asa sul, Brasília/DF, CEP 70070-905
Telefone: - - www.cgu.gov.br

TERMO DE REFERÊNCIA PROCESSO DE CONTRATAÇÃO

1. OBJETO DA CONTRATAÇÃO

1.1. Contratação, via Sistema de Registro de Preço, de solução de Rede LAN composta por:

- a. Equipamentos switches de acesso, de distribuição e de core;
 - b. Garantia estendida;
 - c. Transceivers;
 - d. Software de controle de acesso à rede;
 - e. Software de Gerenciamento/Administração/Orquestração da Rede;
 - f. Repasse de conhecimento; e
- conforme especificações definidas neste Termo de Referência.

2. DESCRIÇÃO DA SOLUÇÃO DE TIC

2.1. Bens e serviços que compõem a solução

Grupo	Item	Descrição	CATSER	CATMAT	ND	Unidade	Quant. Mínima	Quant. Máxima
1	1	Switch acesso - tipo 1 (sede e secundários regionais)	-	393274	44905235	Unidade	66	97
	2	Garantia estendida - switch acesso - tipo 1 - 5 anos - 8x5xNBD	27740	-	33904012	Unidade	66	97
	3	Instalação switch acesso - tipo 1	27260	-	33904021	Unidade	66	97
	4	Módulo e cabo de empilhamento para switch acesso - tipo 1	-	393274	44905235	Unidade	0	19
	5	Switch acesso - tipo 2 (principais regionais)	-	393274	44905235	Unidade	22	58
	6	Garantia estendida - switch acesso - tipo 2 - 5 anos - 8x5xNBD	27740	-	33904012	Unidade	22	58
	7	Instalação switch acesso - tipo 2	27260	-	33904021	Unidade	22	58
	8	Switch distribuição	-	393272	44905235	Unidade	6	18
	9	Garantia estendida - switch distribuição - 5 anos - 8x5xNBD	27740	-	33904012	Unidade	6	18
	10	Instalação switch distribuição	27260	-	33904021	Unidade	6	18
	11	Switch core	-	393273	44905235	Unidade	2	2
	12	Garantia estendida - switch core - 5 anos - 24x7x4	27740	-	33904012	Unidade	2	2
	13	Instalação switch core	27260	-	33904021	Unidade	2	2
	14	SFP28 25GBase-SR	-	150812	44905235	Unidade	12	40
	15	SFP 1000BaseT	-	150812	44905235	Unidade	4	14
	16	SFP 1000BaseSX	-	150812	44905235	Unidade	4	10
	17	SFP+ 10GBaseSR	-	150812	44905235	Unidade	41	99
	18	Software NAC - 5000 dispositivos - 5 anos - 24x7x4	27472	-	44904005	Unidade	1	1
	19	Instalação software NAC - 5000 dispositivos	27260	-	33904021	Unidade	1	1
	20	Software de Gerenciamento/Administração/Orquestração da Rede - 5 anos - 8x5	27472	-	44904005	Unidade	1	1
	21	Instalação do Software de Gerenciamento/Administração/Orquestração da Rede	27260	-	33904021	Unidade	1	1
	22	Repasse de conhecimento	3840	-	33904020	Unidade	1	1

3. JUSTIFICATIVA PARA A CONTRATAÇÃO

3.1. Contextualização e Justificativa da Contratação

3.1.1. A descrição da demanda e a justificativa da contratação se encontram detalhadas no Estudo Técnico Preliminar SEI 1561288.

3.1.2. Conforme referido documento, a solução de LAN (Local Area Network) cabeada para usuários da CGU é composta por uma série de equipamentos que permitem a conectividade de dispositivos diversos com a rede de dados do referido órgão.

3.1.3. Além das estações de trabalho dos colaboradores da CGU, a rede de dados também é acessada por impressoras/scanners, telefones IP, equipamentos de videoconferência, câmeras de vigilância, equipamentos de rede sem fio e diversos outros equipamentos de automação predial.

3.1.4. Em alguns casos, além de prover conectividade, os equipamentos da rede LAN também são responsáveis por prover alimentação elétrica, como no caso de telefones IP, câmeras de vigilância e equipamentos de rede sem fio.

3.1.5. Atualmente a CGU já possui uma solução de rede LAN, a qual é composta por 151 switches do tipo acesso, 7 switches do tipo distribuição e 2 switches do tipo core. Os equipamentos estão distribuídos em todas as unidades da CGU.

3.1.6. Deste volume de equipamentos, 85% (oitenta e cinco por cento) terá seu respectivo contrato de suporte finalizando em 2020. O suporte dos demais terminará em 2021, com exceção dos switches core, cujos contratos de suporte terminarão em 2024.

3.1.7. Os equipamentos que vencem em 2020 já possuem o EOL (end-of-life) anunciado pela fabricante, estes equipamentos não possuem atualizações de software desde 2016 e de segurança desde 2018, além de que o serviço de suporte de hardware finaliza em 2020.

3.1.8. Além disso, a solução atualmente utilizada pela CGU não conta com um sistema de administração centralizado. Embora os equipamentos sejam padronizados, a configuração é feita de forma individual. São utilizadas algumas ferramentas gratuitas para apoiar a execução de algumas atividades, mas não há qualquer tipo de unificação das ferramentas, as quais trabalham de forma limitada em relação aos equipamentos por serem genéricas (funcionam em qualquer tipo de equipamento).

3.1.9. Embora os equipamentos utilizados na CGU sejam configurados com diversas funcionalidades de segurança, não há autenticação dos dispositivos quando estes se conectam na rede cabeada. As restrições de acesso são implementadas pelos serviços e aplicações, além dos firewalls. Deste modo, um dispositivo qualquer pode se conectar na rede cabeada da CGU, obter um endereço IP e tentar efetuar ataques.

3.1.10. A estrutura da sede é significativamente maior do que as das regionais, de modo a justificar uma estrutura hierárquica em 3 camadas (core, distribuição e acesso). Há uma segunda unidade da CGU em Brasília, mas o objetivo é que as referidas unidades sejam unificadas em breve. As regionais possuem uma infraestrutura significativamente menor e mais simples.

3.1.11. A rede da cabeada CGU (tanto na sede quanto nas regionais) é basicamente dividida em dois tipos: dados e multimídia. Sempre que possível a segmentação entre as duas redes é feita de forma automática por negociação via LLDP dos switches com os equipamentos. De modo simplificado, quando um dispositivo não utiliza a VLAN para equipamentos multimídia (codecs de videoconferência e telefones IP) ele permanece na VLAN de dados. Embora seja recomendado separar redes diferentes

para equipamentos com características específicas, esse seria um trabalho manual e que exigiria um esforço muito grande, especialmente considerando que a CGU não possui uma solução de NAC (Network Access Control), que classifique os equipamentos de forma dinâmica. Por esse motivo, não há redes específicas para impressoras, câmeras IP e outras. A separação desses dispositivos é importante para que seja possível controlar o tráfego entre eles, principalmente porque nos últimos anos surgiram diversos ataques que utilizam alguns desses equipamentos para efetuar invasões e outros tipos de ações ilícitas.

3.1.12. A rede LAN cabeada é a base de toda a infraestrutura de qualquer rede. Além de ser um serviço essencial (deve estar sempre disponível de forma adequada), deve ser planejada considerando

demandas futuras, caso contrário pode se tornar gargalo em algum momento.

3.1.13. Por fim, ressalta-se que esta demanda não trata de uma necessidade nova, mas da manutenção de um serviço existente incluindo-se elementos que permitirão a sua evolução. Em especial trata de um serviço básico de infraestrutura, pois sem ela os usuários que estiverem nas dependências da CGU não conseguiriam acessar nenhum serviço de TI disponibilizado por esta Controladoria-Geral.

3.2. Alinhamento aos Instrumentos de Planejamento Institucionais

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	Objetivos Estratégicos
13	Racionalizar os recursos logísticos, financeiros e de TIC, com foco na sustentabilidade, segurança e efetividade.
ID	Iniciativas Estratégicas 2020
13.3	Estabelecer e aprimorar o gerenciamento dos níveis de serviço de TIC.

ALINHAMENTO AO PDTIC 2020-2021	
ID	Título da Demanda
840793	Renovação: Parque de Switches de Acesso

ALINHAMENTO AO PAC 2020	
ID	Título da Demanda
467	Switch

3.3. Estimativa da demanda

3.3.1. Conforme detalhado no Estudo Técnico Preliminar SEI 1561288, os levantamentos realizados definiram os quantitativos necessários para a substituição de toda a rede LAN da CGU considerando sua arquitetura atual. Porém, também foram identificadas potenciais demandas que poderão decorrer em função de eventuais mudanças de endereços, sejam de Unidades Regionais, seja da própria Sede da CGU.

3.3.2. A tabela constante do ANEXO 3 sintetiza a definição do quantitativo de equipamentos em função da necessidade de substituição imediata e os quantitativos definidos para comporem uma reserva

3.4. Parcelamento da Solução de TIC

3.4.1. Os itens devem ser adquiridos/contratados em um único lote, pois trata-se de uma solução unificada para toda a infraestrutura de rede LAN cabeada da CGU. Os diversos componentes possuem grande dependência entre si e há a necessidade de que a empresa Contratada seja capaz de garantir a interoperabilidade plena dos ativos.

3.4.2. Além disso:

3.4.2.1. trata-se de uma licitação aberta e o não agrupamento implicaria em risco de aquisição de equipamentos de fabricantes diferentes que provavelmente serão capazes de funcionar com interoperabilidade básica, mas sem garantia de prover funcionalidades configurações avançadas; e

3.4.2.2. os serviços de instalação e suporte (garantia estendida) devem ser exatamente compatíveis com os equipamentos contratados.

3.5. Resultados e Benefícios a Serem Alcançados

3.5.1. Os resultados pretendidos se referem a disponibilização de uma rede cabeada:

3.5.1.1. Com possibilidade de conexão para todos os servidores e colaboradores da CGU;

3.5.1.2. Com performance adequada;

3.5.1.3. Segurança no acesso;

3.5.1.4. Escalável (deve ser capaz de permitir o crescimento tanto em termos de quantidade de portas quanto em relação ao volume de tráfego sem que sejam necessárias grandes alterações);

3.5.1.5. Que possibilite a evolução das tecnologias atuais e permita a implementação de novas tecnologias e dispositivos que necessitem de conectividade de rede cabeada; e

3.5.1.6. Que permita a implantação de diversos outros serviços, tais como:

3.5.1.6.1. Solução de telefonia IP da CGU;

3.5.1.6.2. Soluções de vigilância, como os casos de AC, AP, MA, MS, PE, PB e da Sede;

3.5.1.6.3. Sistemas de controle de acesso, como os casos de AM, SC e da Sede;

3.5.1.6.4. Sistema de rede sem fio em todas as unidades da CGU;

3.5.1.6.5. Sistema de supervisão de energia ininterrupta em todas as unidades da CGU; e

3.5.1.6.6. Novas tecnologias que possam necessitar de comunicação IP utilizando a rede cabeada, como serviços de automação/manutenção predial, geradores, alarmes, sistemas de combate a incêndio dentre outras. De forma resumida, a rede LAN cabeada deve estar preparada para dispositivos do tipo IoT (Internet of Things).

4. ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos de Negócio

4.1.1. A solução de LAN cabeada para usuários da CGU deve:

- i. Estar disponível quando os usuários necessitarem. Para isso a rede deve ser construída utilizando uma arquitetura em que os equipamentos de concentração (aqueles que suportam vários usuários)
- ii. devem ser montados utilizando uma arquitetura com redundância. Os equipamentos de concentração devem possuir fontes redundantes para que possam suportar eventuais falhas dos referidos componentes;
- iii. Ter a performance adequada, sem a existência de gargalos que impeçam o acesso aos principais serviços de rede da CGU. Deste modo, a rede deve ser estruturada de modo que as interfaces de uplink e de servidores possuam maior velocidade do que as interfaces de usuários;
- iv. Ser segura, impedindo que os ataques de infraestrutura de redes possam ser mitigados de forma automática. A rede deve ser capaz de se proteger de erros que atrapalhem o funcionamento da infraestrutura, como casos de usuários que acidentalmente criem loops de camada 2 ou iniciem um servidor de DHCP em suas estações de trabalho. Cabe ressaltar que os aspectos de segurança em
- v. questão também afetam de forma significativa a disponibilidade da rede;
- vi. Ser escalável (deve ser capaz de permitir o crescimento, tanto em termos de quantidade de portas, quanto em relação ao volume de tráfego, sem que sejam necessárias grandes alterações);
- vii. Possibilitar a evolução das tecnologias atuais e permitir a implementação de novas tecnologias e dispositivos que necessitem de conectividade de rede cabeada;

4.1.2. Além dos requisitos citados anteriormente, é importante que ela permita a manutenção/implementação de diversos outros serviços de negócio, dentre os quais podemos citar:

- i. Solução de telefonia IP da CGU.
- ii. Soluções de vigilância, como os casos de AC, AP, MA, MS, PE, PB, RN e da Sede.
- iii. Sistemas de controle de acesso, como os casos de AM, SC e da Sede.
- iv. Sistema de rede sem fio em todas as unidades da CGU.
- v. Sistema de supervisão de energia ininterrupta em todas as unidades da CGU.
- vi. Novas tecnologias que possam necessitar de comunicação IP utilizando a rede cabeada, como serviços de automação/manutenção predial, geradores, alarmes, sistemas de combate a incêndio, dentre outras. De forma resumida, a rede LAN cabeada deve estar preparada para dispositivos do tipo IoT (Internet of Things).

4.2. Requisitos de Capacitação

4.2.1. Considerando a inserção de novas tecnologias, como NAC e SD-LAN, faz-se necessária a contratação de capacitação para os colaboradores da CGU na nova solução a ser adquirida. Além das novas tecnologias, é importante compreender a sintaxe de configuração dos equipamentos a serem adquiridos.

4.2.2. O detalhamento dos requisitos para a capacitação consta do Anexo 1.

4.3. Requisitos Legais

4.3.1. Os equipamentos ofertados devem ser homologados pela ANATEL no momento da assinatura do contrato.

4.4. Requisitos de Manutenção

4.4.1. Os requisitos de manutenção estão definidos no item 7.2. Níveis Mínimos de Serviço Exigidos.

4.5. Requisitos Temporais

4.5.1. Do ponto de vista técnico, a contratação é considerada prioritária tendo em vista que os equipamentos atuais estão sem suporte.

4.6. Requisitos de Segurança

4.6.1. Não se aplica.

4.7. Requisitos Sociais, Ambientais e Culturais

4.7.1. Os switches de acesso devem ocupar no máximo 1U de espaço em rack (como os equipamentos utilizados atualmente).

4.8. Requisitos de Arquitetura Tecnológica

4.8.1. A solução deve utilizar tecnologia SD-LAN na Sede.

4.8.2. Ademais, a solução de NAC deve prever integração com o Active Directory.

4.9. Requisitos de Projeto e de Implementação

4.9.1. O detalhamento dos requisitos de projeto consta do Anexo 1.

4.10. Requisitos de Implantação

4.10.1. O detalhamento dos requisitos de projeto consta do Anexo 1.

4.11. Requisitos de Garantia

4.11.1. Considerando a perspectiva da solução é de aproximadamente 10 anos, a solução deve ser adquirida com suporte para o maior prazo possível, qual seja de 60 meses.

4.11.2. Os equipamentos referentes aos itens de 1, 4, 5, 8, 11, 14 a 17 não poderão estar anúncio publicado de end-of-sales e end-of-support.

4.12. Requisitos de Experiência Profissional

4.12.1. A etapa de Planejamento deve ser executada por profissional(ais) com experiência em gerenciamento de projetos,

4.12.2. O detalhamento dos requisitos de experiência profissional consta do Anexo 1, especialmente para os profissionais responsáveis pela:

- i. Executar as etapas de Planejamento dos serviços de Instalação;
- ii. Executar as etapas Migração/Instalação (incluindo Software de Gerenciamento/Administração/Orquestração e o software de NAC); e
- iii. Ministrando o Repasse de Conhecimento.

4.13. Requisitos de Formação da Equipe

4.13.1. A etapa de Planejamento e a etapa de Implantação devem ser realizadas por profissional(ais) com certificação em roteamento/switching.

4.14. Requisitos de Metodologia de Trabalho

4.14.1. A etapa de Planejamento deve seguir a metodologia PMBOK.

4.15. Requisitos de Segurança da Informação

4.15.1. Diversos itens da aquisição/contratação em questão tratam aspectos de segurança. Destaque para a solução de NAC, a qual permitirá agregar diversas funcionalidades deste tipo, tanto nas regionais quanto na sede (neste último caso em conjunto com a solução de SD-LAN).

4.15.2. O detalhamento dos requisitos de segurança consta do Anexo 1.

5. RESPONSABILIDADES

5.1. Deveres e responsabilidades da Contratante

- a) Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;
- b) Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência ou Projeto Básico;
- c) Receber o objeto fornecido pela Contratada que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;
- d) Aplicar à Contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;
- e) Liquidar o empenho e efetuar o pagamento à Contratada, dentro dos prazos preestabelecidos em contrato;
- f) Comunicar à Contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;
- g) Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da Contratada, com base em pesquisas de mercado, quando aplicável; e
- h) Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, o código fonte de aplicações, os modelos de dados e as bases de dados, pertençam à Administração;

5.2. Deveres e responsabilidades da Contratada

- a) Indicar formalmente preposto apto a representá-lo junto à Contratante, que deverá responder pela fiel execução do contrato;
- b) Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;
- c) Reparar quaisquer danos diretamente causados à Contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela Contratante;
- d) Propiciar todos os meios necessários à fiscalização do contrato pela Contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, sempre que considerar a medida necessária;
- e) Manter, durante toda a execução do contrato, as mesmas condições da habilitação;
- f) Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;
- g) Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato; e
- h) Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração;

5.3. Deveres e responsabilidades do órgão gerenciador da ata de registro de preços

- a) Efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços;
- b) Gerenciar a ata de registro de preços;
- c) Conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;
- d) Aplicar, garantida a ampla defesa e o contraditório, as penalidades decorrentes de infrações no procedimento licitatório;
- e) Aplicar, garantida a ampla defesa e o contraditório, as penalidades decorrentes do descumprimento do pactuado na ata de registro de preços ou do descumprimento das obrigações contratuais, em relação às suas próprias contratações;
- f) Mecanismos de comunicação entre órgão gerenciador, participantes e não participantes:

Evento	Responsável	Prazo	Forma
Solicitação de adesão por órgão integrante do SISG	Órgão interessado na adesão	Dentro da vigência da ARP	Via Sistema
Solicitação de adesão por órgão NÃO integrante do SISG	Órgão interessado na adesão	Dentro da vigência da ARP	E-mail para colic@cgu.gov.br
Assinatura da ARP	Órgão Gerenciador	10 (dez) dias úteis	Via Sistema
Aplicação de penalidade em contrato decorrente da ARP	Órgão participante ou não participante que aplicou a penalidade	10 (dez) dias úteis	E-mail para cdcon@cgu.gov.br

- g) Mecanismos de controle de fornecimento:

- i. A definição da produtividade ou da capacidade mínima de fornecimento da solução de TIC;
- ii. Para o caso de substituição da solução, ou parte dela, registrada na ARP, o fornecedor deverá encaminhar a documentação técnica da nova solução para o Órgão Gerenciador da Ata, juntamente com a justificativa da necessária e imperativa substituição, que comprove que a nova solução atende aos requisitos do Termo de Referência e é compatível com as partes já instaladas.
- iii. A área técnica do órgão gerenciador terá até 30 (trinta) dias para avaliar a documentação encaminhada e poderá solicitar amostra para verificar a manutenção da compatibilidade entre as partes da solução.

6. MODELO DE EXECUÇÃO DO CONTRATO

6.1. Cronograma de Execução

6.1.1. Cronograma referente aos itens 1 a 21:

Evento	Descrição do evento	Prazo Máximo	Responsável
1	Assinatura do contrato	-	Contratada e Contratante
2	Reunião inicial	Evento 1 + 5 dias úteis	Contratada e Contratante
3	Comprovação da qualificação de profissionais	Evento 1 + 15 dias úteis	Contratada
4	Apresentação do Plano de Implantação	Evento 2 + 30 dias úteis	Contratada
5	Avaliação do Plano de Implantação	Evento 4 + 5 dias úteis	Contratante
6	Ajustes no Plano de Implantação	Evento 5 + 10 dias úteis	Contratada
7	Aprovação do Plano de Implantação	Evento 6 + 5 dias úteis	Contratante
8	Entrega dos Bens	Evento 1 + 50 dias úteis	Contratada
9	Recebimento Provisório dos Bens	Evento 8 + 5 dias úteis	Contratante
10	Início da Etapa de Implantação (exceto NAC)	Evento 7 e Evento 9 concluídos	-
11	Fim da Etapa de Implantação (exceto NAC)	Evento 10 + Tempo de Implantação (definido em tabela abaixo)	Contratada e Contratante
12	Aplicação de Licenças Definitivas e Comprovação da Vigência da Garantia Estendida (exceto NAC)	Evento 11 + 5 dias úteis	Contratada
13	Emissão de Termo de Recebimento Definitivo da Implantação (exceto NAC)	Evento 12 + 10 dias úteis	Contratante
14	Início da Etapa de Implantação NAC	Evento 13 concluído	-
15	Fim da Etapa de Implantação NAC	Evento 14 + 50 dias úteis	Contratada e Contratante
16	Aplicação de Licenças Definitivas e Comprovação da Vigência do Suporte NAC	Evento 15 + 5 dias úteis	Contratada
17	Emissão de Termo de Recebimento Definitivo NAC	Evento 16 + 10 dias úteis	Contratante

6.1.1.1. Quanto à comprovação da qualificação de profissionais

6.1.1.1.1. A Contratada terá 15 (quinze) dias úteis para apresentar os documentos que comprovem a qualificação dos profissionais responsáveis pelas etapas listadas abaixo, conforme definições constantes do Anexo 1:

- 6.1.1.1.1.1. Execução das etapas de Planejamento dos serviços de Instalação;
- 6.1.1.1.1.2. Execução das etapas Migração/Instalação (incluindo Software de Gerenciamento/Administração/Orquestração e o software de NAC); e
- 6.1.1.1.1.3. Instrução do Repasse de Conhecimento.

6.1.1.2. Quanto ao Plano de Implantação:

6.1.1.2.1. A apresentação de Plano de Implantação aprovado pela Contratante é condição necessária para o início das instalações de qualquer equipamento.

6.1.1.2.2. A Contratante poderá dispensar a elaboração do Plano de Implantação quando julgar que este documento não traz benefícios para a condução do projeto. As situações em que o plano pode ser dispensado são aquelas em que serão feitas pequenas aquisições, geralmente vinculadas a expansões. Para aquisições de grande volume e/ou que envolvam a substituição de todos os equipamentos de uma ou mais localidades, será exigida a elaboração do Plano de Implantação.

6.1.1.2.3. O Tempo de Implantação terá prazo definido na tabela abaixo, dependendo dos quantitativos e locais de instalação:

Característica do Contrato	Tempo de Implantação em Dias Úteis
Prevê instalação na Sede com mais de 20 switches	50 dias
Prevê instalação nas regionais ou Prevê instalações na Sede com até 20 switches	5 dias por localidade

6.1.1.3. Quanto aos equipamentos:

- 6.1.1.3.1. A entrega dos bens será considerada concluída quando os equipamentos contratados tiverem sido entregues nas localidades definidas, com suas respectivas notas fiscais.
- 6.1.1.3.2. Os bens serão recebidos provisoriamente no prazo de 5 (cinco) dias úteis contados a partir da entrega dos bens à Seção de Almoxarifado. O recebimento provisório será emitido por responsável, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e com a proposta.

6.1.1.4. Quanto aos serviços de instalação (exceto NAC):

- 6.1.1.4.1. O cronograma define os prazos da Etapa de Implantação, que trata do provimento dos serviços de instalação dos equipamentos e do software de gerência.
- 6.1.1.4.2. O item 9 indica o momento da contagem de prazo para Etapa de Implantação, mas algumas etapas do processo de instalação podem ser iniciadas antes deste marco. Em especial a instalação de máquinas virtuais, integrações com serviço de autenticação e correio, e solicitações de regras de firewall.
- 6.1.1.4.3. Durante a fase de implantação será permitido o uso de licenças do tipo trial.

6.1.1.5. Quanto aos serviços de garantia estendida:

- 6.1.1.5.1. Os serviços de garantia estendida deverão contar a partir da finalização da instalação de todos os equipamentos adquiridos, conforme data registrada no Termo de Recebimento. Ou seja, a finalização da última instalação será o marco de início da garantia estendida de 5 (cinco) anos para todos os equipamentos sob o mesmo contrato.

- 6.1.1.6. Os bens e a comprovação da vigência do serviço de garantia estendida poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 25 (vinte e cinco) dias úteis, a contar da notificação da Contratada, às suas custas, sem prejuízo da aplicação das penalidades.

6.1.2. Cronograma referente item 22 (Repasse de conhecimento):

Evento	Descrição do evento	Prazo Máximo	Responsável
1	Assinatura do contrato	-	Contratada e Contratante
2	Emissão de Ordem de Serviço	Qualquer momento após evento 1.	Contratada e Contratante
3	Entrega do planejamento da atividade de Repasse de Conhecimento	Evento 2 + 5 dias úteis	Contratada
4	Início da prestação do serviço	Evento 2 + 20 dias úteis	Contratada
5	Emissão de Termo de Recebimento Definitivo	Fim da prestação do serviço + 10 dias úteis	Contratante

- 6.1.2.1. Após recebimento de Ordem de Serviço solicitando o início do serviço de Repasse de Conhecimento, a Contratada deverá apresentar em até 5 (cinco) dias úteis o planejamento da atividade de Repasse de Conhecimento, considerando a data de início de atividade definida na respectiva OS.

- 6.1.2.1.1. O prazo poderá ser maior do que 20 (vinte) dias úteis conforme conveniência da Contratante;
- 6.1.2.1.2. O prazo poderá ser menor do que 20 (vinte) dias úteis conforme anuência da Contratada;

6.1.3. Locais de entrega de bens e prestação de serviços:

- 6.1.3.1. O ANEXO 2 lista os endereços das atuais unidades da CGU.

- 6.1.3.1.1. Os endereços podem eventualmente ser alterados em função de mudanças das unidades regionais, inclusive a Sede. Neste caso a Contratante deverá comunicar a Contratada.

- 6.1.3.1.2. Ressalta-se que CGU possui um único CNPJ, não possui inscrição estadual e não emite nota fiscal.

- 6.1.3.1.2.1. Não haverá aumento de prazo por qualquer dificuldade fiscal de enviar os equipamentos para as unidades regionais. Este dispositivo se aplica tanto para a entrega dos bens durante a fase de aquisição quanto para a etapa de prestação do serviço, em que pode ser necessário efetuar a substituição de equipamentos que apresentarem defeito.

- 6.1.3.2. A expectativa bens/serviços quantificados como “reserva” (ANEXO 3) sejam entregues/realizados na Sede da CGU no DF, porém podendo eventualmente ocorrer em alguma na sede da CGU em algum estado.

- 6.1.3.3. O Suporte Técnico é de responsabilidade única e exclusiva da CONTRATADA e ocorrerá às suas expensas, mesmo quando, durante o período de garantia, for necessário o transporte de equipamentos ou peças ou ainda o traslado e a estadia de técnicos da CONTRATADA ou qualquer outro tipo de serviço necessário ao cumprimento da garantia.

6.1.4. Documentação mínima exigida

- 6.1.4.1. É condição para a o recebimento de bens e software, a apresentação das respectivas notas fiscais.

6.2. Quantidade mínima de bens ou serviços para comparação e controle

- 6.2.1. Os testes de aceitação serão realizados em todos os equipamentos.

6.3. Mecanismos formais de comunicação

- 6.3.1. As tratativas realizadas entre Contratante e Contratada deverão ser formalizadas por meio de correio eletrônico incluindo:

- 6.3.1.1.. formalização das decisões acordadas em reunião inicial;
- 6.3.1.2. tratativas referentes a prazos e aceitações de bens e serviços;
- 6.3.1.3. encaminhamento de termos de aceite provisórios ou definitivos;
- 6.3.1.4. encaminhamento de Ordens de Serviço;
- 6.3.1.5. outras necessárias;

- 6.3.2. Especificamente quanto às solicitações de suporte técnico, poderão ser feitos por meio de telefone 0800, sítio da web ou e-mail indicados pela Contratada;

6.4. Manutenção de Sigilo e Normas de Segurança

- 6.4.1. A Contratada deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

- 6.4.2. O **Termo de Confidencialidade**, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da Contratada, e **Termo de Ciência**, a ser assinado por todos os empregados da Contratada diretamente envolvidos na contratação, encontram-se nos ANEXOS 4 e 5.

7. MODELO DE GESTÃO DO CONTRATO

7.1. Critérios de Aceitação e Procedimentos de Aceitação

7.1.1. São previstos quatro eventos para aceitação definitiva de bens e serviços:

7.1.1.1. Entrega de todos os bens contratados:

7.1.1.1.1. Será verificada:

7.1.1.1.1.1. Se o quantitativo de bens entregues está de acordo com o contratado; e

7.1.1.1.1.2. A aderência dos produtos com os quesitos estabelecidos no ANEXO 1 deste Termo de Referência. A verificação das características dos bens será feita em até 10 (dez) dias úteis serem cumpridos os seguintes requisitos:

7.1.1.1.1.2.1. Após a instalação de pelo menos 1 (um) exemplar de cada item adquirido;

7.1.1.1.1.2.2. Após ter sido realizada a instalação na Sede (caso a aquisição envolva equipamentos da Sede) e em pelo menos uma regional (caso a aquisição envolva equipamentos de pelo menos uma unidade regional);

7.1.1.1.1.2.3. Após ter sido realizada a instalação do Software de Gerenciamento/Administração/Orquestração de Rede (caso a aquisição envolva o referido software).

7.1.1.2. Prestação do serviço de instalação:

7.1.1.2.1. Será verificado a finalização do serviço de instalação em todos os locais contratados.

7.1.1.2.2. Compõe esta etapa:

7.1.1.2.2.1. O ajuste das datas das garantias estendidas;

7.1.1.2.2.2. A ativação do licenciamento e instalação do Software de Gerenciamento/Administração/Orquestração de Rede;

7.1.1.2.3. Quanto ao serviço de garantia estendida e licenciamento do Software de Gerenciamento, os responsáveis pela fiscalização do contrato verificarão os registros junto ao fabricante e/ou os documentos apresentados que comprovem a vigência dos serviços.

7.1.1.2.4. O serviço de garantia estendida, de duração total de 5 (cinco) anos, deverá ter sua data de início igual ou posterior a data de finalização da última instalação realizada.

7.1.1.3. Serviço de instalação do Software NAC:

7.1.1.3.1. Esta etapa inclui a ativação do licenciamento do Software NAC e sua instalação.

7.1.1.3.2. Quanto ao licenciamento do Software NAC, os responsáveis pela fiscalização do contrato verificarão os registros junto ao fabricante e/ou os documentos apresentados que comprovem a vigência dos serviços.

7.1.1.3.3. O serviço de suporte estendido, de duração total de 5 (cinco) anos, deverá ter sua data de início igual ou posterior a data de finalização de sua instalação realizada.

7.1.1.4. Serviço de Repasse de Conhecimento:

7.1.1.4.1. Para a aceitação deste a aprovação do curso ministrado pelos participantes.

7.1.1.4.2. Em até 3 (três) dias úteis após a finalização do treinamento, será emitido o Termo de Recebimento Provisório.

7.1.1.4.3. Os participantes do curso realizarão avaliação do curso ministrado, conforme formulário constante do ANEXO 6.

7.1.1.4.4. A emissão do aceite definitivo dependerá de a avaliação resultar em uma média igual ou superior a 3,5 (três e meio).

7.1.1.4.5. No caso de não alcance da média mínima estabelecida, o curso deverá ser novamente ministrado pela instituição, considerando os apontamentos recolhidos pela avaliação.

7.1.1.4.6. A nova turma será composta pelos mesmos alunos e o conteúdo será aquele que não foi satisfatório na primeira tentativa.

7.1.2. Quanto ao acompanhamento da prestação dos serviços de garantia estendida e suporte dos softwares:

7.1.2.1. Durante a vigência da garantia dos equipamentos, o serviço deverá atender o NMS estabelecido neste TR. O não atendimento dará causa para que a equipe de fiscalização inicie procedimento de sancionamento.

7.1.2.2. Durante do suporte dos softwares de NAC e de gerência, o serviço deverá atender ao respectivo NMS estabelecido neste TR. O não atendimento dará causa para que a equipe de fiscalização inicie procedimento de sancionamento.

7.2. Níveis Mínimos de Serviço Exigidos

7.2.1. Níveis de severidades

7.2.1.1. Durante a vigência do contrato de garantia estendida, a Contratada deverá fornecer atendimento técnico “on-site” observando os parâmetros a seguir.

7.2.1.1.1 **Severidade ALTA:** Esse nível de severidade é aplicado quando a solução se encontra totalmente indisponível. Há uma falha no ativo de rede ou software que deixe indisponíveis seus recursos (serviço parado). Há impacto a múltiplos usuários e/ou falha em servidor de produção que afete operações críticas da CONTRATANTE;

7.2.1.1.2. **Severidade MÉDIA:** Esse nível de severidade é aplicado quando há falha, simultânea ou não, do uso da solução, em que a solução se encontra parcialmente indisponível ou com degradação de tempo de resposta no acesso aos aplicativos, módulos ou recursos; e

7.2.1.1.3. **Severidade BAIXA:** Esse nível de severidade é aplicado quando a solução se encontra disponível, mas há ocorrência de alarmes, bem como quando é necessário realizar consulta sobre problemas ou dúvidas gerais sobre a Solução. Há um pequeno impacto a um ou mais usuários. A correção pode ser feita de forma agendada, em um momento futuro;

7.2.1.2. Será considerado horário final para dia útil, o horário de 19h00.

7.2.1.3. Será considerado para efeitos dos níveis exigidos:

7.2.1.3.1. **Prazo de término de atendimento:** tempo decorrido entre a abertura do chamado efetuada pela equipe técnica da CGU à CONTRATADA e o retorno de disponibilidade da solução.

7.2.1.4. O nível de severidade será informado pela CONTRATANTE no momento da abertura de cada chamado.

7.2.1.5. O nível de severidade poderá ser reclassificado a critério da Contratante. O nível de severidade de um acionamento poderá ser reclassificado no decorrer do atendimento e conforme a disponibilidade de recursos dos módulos e componentes da solução.

7.2.1.6. Todas as solicitações de suporte técnico devem ser registradas pela Contratada, para acompanhamento e controle da execução do serviço.

7.2.1.7. A Contratada apresentará à CGU, ao término de cada atendimento, um relatório de atendimento técnico contendo dados sobre a intervenção na solução.

7.2.1.8. A Contratada também fornecerá atendimento técnico por meio de visitas à sede da CGU, para eventuais demandas que, uma vez esgotadas as tentativas de solução por meio de contato telefônico ou correio eletrônico, ainda não tenham sido solucionadas. Sempre que demandada neste sentido, a Contratada alocará recursos para atendimento in loco, mediante prévio agendamento, para possibilitar a estruturação da visita já com a solução esquematizada. O relatório de visita deverá ser assinado pelo servidor da Contratante que solicitou o atendimento técnico.

7.2.1.9. Nos casos onde o atraso na solução dos chamados técnicos se dê pela ocorrência de “bug”, notadamente reconhecido pelo fabricante do produto, a Contratada poderá apresentar à Contratante exposição de motivos que fundamentem a ocorrência desta situação;

7.2.1.10. Caso a Contratante considere procedentes as justificativas apresentadas, poderá descontar do tempo total do chamado o tempo decorrido entre a identificação e a solução final para o “bug”.

7.2.2. Garantia estendida para os itens 1, 5 e 8, e suporte para o item 20:

7.2.2.1. A garantia estendida para os itens 1, 5 e 8 são contratados respectivamente por meio dos itens 2, 6 e 9.

7.2.2.1.1. A garantia dos módulos (itens 4, 14, 15, 16, e 17) serão providos em função da garantia contratada para o equipamento ao qual eles estarão acoplados.

7.2.2.2. Os níveis de severidade e parâmetros de suporte estabelecidos para os equipamentos também se aplicarão ao Software de Gerenciamento (item 20).

7.2.2.3. A CONTRATADA deverá cumprir prazos máximos para resposta aos acionamentos de acordo com o nível de severidade de cada chamado, conforme tabela abaixo:

Modalidade de atendimento	Evento	Prazos para os níveis de severidade		
		1 – ALTA	2 - MÉDIA	3 – BAIXA
On Site, E-mail, ou Telefone	Término de atendimento	Até o próximo dia útil para chamados abertos até 15:00 E até o 2º dia útil para chamados abertos após as 15:00	Até o 3º dia útil após a abertura do chamado	Até o 5º dia útil após a abertura do chamado

7.2.3. Garantia estendida para o item 11 e suporte para o item 18:

7.2.3.1. A garantia estendida para o item 11 é contratada por meio do item 12.

7.2.3.1.1. A garantia dos módulos (itens 4, 14, 15, 16, e 17) serão providos em função da garantia contratada para o equipamento ao qual eles estarão acoplados.

7.2.3.2. Os níveis de severidade e parâmetros de suporte estabelecidos para os equipamentos também se aplicarão ao Software NAC (item 18).

7.2.3.3. Assim, referente aos serviços contratados nos itens 12 e 18, a Contratada deverá cumprir prazos máximos para resposta aos acionamentos de acordo com o nível de severidade de cada chamado, conforme tabela abaixo:

Modalidade de atendimento	Evento	Prazos para os níveis de severidade		
		1 – ALTA	2 - MÉDIA	3 – BAIXA
On Site, E-mail, ou Telefone	Término de atendimento	4 horas	8 horas	Até o 2º dia útil após a abertura do chamado

8. GESTÃO ADMINISTRATIVA DO CONTRATO

8.1. Sanções Administrativas

8.1.1. Comete infração administrativa nos termos da Lei nº 10.520, de 2002, a CONTRATADA que:

- 8.1.1.1. Não executar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;
- 8.1.1.2. Ensejar o retardamento da execução do objeto;
- 8.1.1.3. Falhar ou fraudar na execução do contrato;
- 8.1.1.4. Comportar-se de modo inidôneo; ou
- 8.1.1.5. Cometer fraude fiscal.

8.1.2. Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à Contratada as seguintes sanções:

8.1.2.1. No caso de atraso na entrega de bens e prestações de serviços, ou não aceitação deles, serão aplicadas as seguintes sanções:

8.1.2.1.1. No caso da entrega Plano de Implantação aprovado:

- 8.1.2.1.1.1. Advertência no caso de atraso até 5 (cinco) dias úteis;
- 8.1.2.1.1.2. Multa moratória de 0,5% (cinco décimos por cento) por dia útil de atraso, contado a partir do primeiro dia útil de atraso, no caso de atraso de mais de 5 (cinco) dias úteis, limitada a incidência a 20 (vinte) dias úteis; e
- 8.1.2.1.1.3. Após o vigésimo dia de atraso e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença.
- 8.1.2.1.1.4. Para fins de sanção sobre a entrega do Plano de Implantação já aprovado pela Contratante, será considerado:
 - 8.1.2.1.1.4.1. como prazo para entrega do Plano de Implantação já aprovado pela Contratante o prazo de 55 (cinquenta e cinco) dias úteis após a assinatura do contrato; e
 - 8.1.2.1.1.4.2. como valor de referência sobre o qual se calcularão as sanções, o valor unitário contratado para o item 11.

8.1.2.1.2. No caso da entrega dos equipamentos previstos nos itens 1, 4, 5, 8, 11 e 14 a 17, e disponibilização das licenças previstas nos itens 18 e 20:

- 8.1.2.1.2.1. Advertência no caso de atraso até 10 (dez) dias úteis;
- 8.1.2.1.2.2. Multa moratória de 0,5% (cinco décimos por cento) por dia útil de atraso, contado a partir do primeiro dia de atraso, no caso de atraso de mais de 10 (dez) dias úteis, limitada a incidência a 20 (vinte) dias úteis; e
- 8.1.2.1.2.3. Após o vigésimo dia de atraso e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença.

8.1.2.1.3. No caso da instalação dos equipamentos previstos nos itens 1, 4, 5, 8, 11 e 14 a 17, e softwares previstos nos itens 18 e 20:

- 8.1.2.1.3.1. Refere-se às instalações contratadas por meio dos itens 3, 7, 10, 13, 19 e 21;
- 8.1.2.1.3.2. Advertência no caso de atraso até 10 (dez) dias úteis;
- 8.1.2.1.3.3. Multa moratória de 0,5% (cinco décimos por cento) por dia útil de atraso, contado a partir do primeiro dia de atraso, no caso de atraso de mais de 10 (dez) dias úteis, limitada a incidência a 20 (vinte) dias úteis; e
- 8.1.2.1.3.4. Após o vigésimo dia de atraso e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença.

8.1.2.1.4. No caso da aplicação das licenças definitivas e da comprovação da vigência dos serviços da garantia estendida previstos nos itens 2, 6, 9 e 12:

- 8.1.2.1.4.1. Advertência no caso de atraso até 10 (dez) dias úteis;
- 8.1.2.1.4.2. Multa moratória de 0,5% (cinco décimos por cento) por dia útil de atraso, contado a partir do primeiro dia de atraso, no caso de atraso de mais de 10 (dez) dias úteis, limitada a incidência a 20 (vinte) dias úteis; e
- 8.1.2.1.4.3. Após o vigésimo dia de atraso e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença.

8.1.2.1.5. No caso do serviço de Repasse de Conhecimento previsto no item 22:

- 8.1.2.1.5.1. Multa moratória de 5% (cinco por cento) sobre o valor do serviço em caso de atraso na execução dos serviços superior a 10 (dez) dias úteis. Após o décimo dia útil e a critério da Administração, no caso de execução com atraso, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença.
- 8.1.2.1.5.2. Multa compensatória de 10% (dez por cento) sobre o valor do serviço em caso de reprovação pela segunda vez, conforme critérios de avaliação descritos no ANEXO 6 deste TR. No caso de uma terceira reprovação, e a critério da Administração, poderá ocorrer a não-aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença.

8.1.2.2. No caso de atraso na apresentação da garantia:

- 8.1.2.2.1. multa moratória de 0,07% (sete centésimos por cento) calculados sobre o valor do contrato, por dia de atraso na apresentação da garantia (seja para reforço ou por ocasião de prorrogação), observado o máximo de 2% (dois por cento). O atraso superior a 25 (vinte e cinco) dias autorizará a Administração CONTRATANTE a promover a rescisão do contrato.

8.1.2.3. No caso de inexecução total do objeto:

8.1.2.3.1. multa compensatória de 5% (cinco por cento) sobre o valor total do contrato.

8.1.2.4. No caso de outros descumprimentos de outras obrigações cujas sanções não foram definidas neste TR:

8.1.2.4.1. multa compensatória de 0,3% sobre valor total do contrato.

8.1.2.5. No caso de descumprimento do NMS do suporte para os itens 1, 5, 8, e 20:

8.1.2.5.1. inclui-se os itens 4 e 14 a 17 se estiverem conectados aos itens 1, 5 ou 8;

8.1.2.5.2. aplicar-se-á penalidades conforme tabela abaixo, considerando tempo de atraso no término de atendimento em dias úteis:

Descumprimento	Penalidade
Entre 1 (um) e 5 (cinco) dias úteis	Multa moratória de 2% (dois por cento) sobre o valor do equipamento/software
Acima de 5 (cinco) e até 7 (sete) dias úteis	Multa compensatória de 3% (três por cento) sobre o valor do equipamento/software
Acima de 7 (sete) e até 9 (nove) dias úteis	Multa compensatória de 5% (cinco por cento) sobre o valor do equipamento/software
Acima de 9 (nove) dias úteis	Multa compensatória de 10% (dez por cento) sobre o valor do equipamento/software

8.1.2.6. No caso de descumprimento do NMS do suporte para o item 11;

8.1.2.6.1. inclui-se os itens 14 a 17 se estiverem conectados ao item 11.

8.1.2.6.2. aplicar-se-á penalidades conforme tabela abaixo, considerando tempo de atraso no término de atendimento em horas corridas:

Descumprimento	Penalidade
Entre 1 (uma) e 24 (vinte e quatro) horas	Multa moratória de 0,42% (quarenta e dois centésimos por cento) sobre o valor do equipamento, até o máximo de 10% do valor do equipamento
Acima de 24 (vinte e quatro) e até 48 (quarenta e oito) horas	Multa compensatória de 2% (dois por cento) sobre o valor do equipamento
Acima de 48 (quarenta e oito) e até 72 (setenta e duas) horas	Multa compensatória de 5% (cinco por cento) sobre o valor do equipamento
Acima de 72 (setenta e duas) horas	Multa compensatória de 10% (dez por cento) sobre o valor do equipamento

8.1.2.6.3. Em eventual caso de aplicação de multa compensatória:

8.1.2.6.3.1. esta será aplicada em conjunto com a multa moratória; e 8.1.2.6.3.2. será aplicada a de maior valor.

8.1.2.7. No caso de descumprimento do NMS do suporte para o item 18;

8.1.2.7.1. aplicar-se-á penalidades conforme tabela abaixo, considerando tempo de atraso no término de atendimento em horas corridas:

Descumprimento	Penalidade
Entre 1 (uma) e 48 (quarenta e oito) horas	Multa moratória de 0,2% (dois décimos por cento) sobre o valor do software, até o máximo de 10% do valor do software
Acima de 48 (quarenta e oito) e até 72 (setenta e duas) horas	Multa compensatória de 1% (um por cento) sobre o valor do software
Acima de 72 (setenta e duas) e até 96 (noventa e seis) horas	Multa compensatória de 3% (três por cento) sobre o valor do software
Acima de 96 (noventa e seis) horas	Multa compensatória de 6% (seis por cento) sobre o valor do software

8.1.2.7.2. Em eventual caso de aplicação de multa compensatória:

8.1.2.7.2.1. esta será aplicada em conjunto com a multa moratória; e

8.1.2.7.2.2. será aplicada a de maior valor.

8.1.2.8. Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até 2 (dois) anos.

8.1.2.9. Sanção de impedimento de licitar e contratar com órgãos e entidades da União, com o conseqüente descredenciamento no SICAF pelo prazo de até cinco anos.

8.1.2.9.1. A Sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa no subitem 8.1.1 deste Termo de Referência.

8.1.2.10. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados.

8.1.3. As penalidades de multa decorrentes de fatos diversos serão consideradas independentes entre si.

8.1.3.1. O valor de cada ocorrência referente a multas moratórias previstas nos subitens 8.1.2.1.1.2, 8.1.2.1.2.2, 8.1.2.1.3.3 e 8.1.2.1.4.2 estão limitadas a 10% (dez por cento) do valor do Item ou conjunto de Itens, conforme o caso.

8.1.4. As sanções de “advertência”, “suspensão de licitar e impedimento de contratar”, “impedimento de licitar e contratar” e “declaração de inidoneidade para licitar ou contratar” poderão ser aplicadas à CONTRATADA juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.

8.1.5. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

8.1.5.1. tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

8.1.5.2. tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

8.1.5.3. demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

8.1.6. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

8.1.7. As multas devidas e/ou prejuízos causados à Contratante serão deduzidos dos valores a serem pagos, ou recolhidos em favor da União, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa da União e cobrados judicialmente.

8.1.7.1. Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

8.1.8. Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, a União ou Entidade poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

8.1.9. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

8.1.10. Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração

pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho

fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização - PAR.

8.1.11. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

8.1.12. O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

8.1.13. As penalidades serão obrigatoriamente registradas no SICAF.

8.2. Do Pagamento

8.2.1. São previstos quatro eventos de pagamentos, conforme quesitos estabelecidos no item 7.1. Critérios de Aceitação e Procedimentos de Aceitação, sendo eles:

8.2.1.1. Ao final da entrega de todos os bens contratados;

8.2.1.2. Ao final da instalação de equipamentos e software;

8.2.1.3. Ao final da instalação do Software NAC; e

8.2.1.4. Ao final do Repasse de Conhecimento.

8.2.2. O pagamento será efetuado pela Contratante no prazo de 10 (dez) dias úteis, contados do recebimento da Nota Fiscal/Fatura.

8.2.2.1. Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal/Fatura, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

8.2.3. A emissão da Nota Fiscal/Fatura será precedida do recebimento definitivo do serviço, conforme este Termo de Referência.

8.2.4. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 29 da Lei nº 8.666, de 1993.

8.2.5. Constatando-se, junto ao SICAF, a situação de irregularidade do fornecedor contratado, deverão ser tomadas as providências previstas no do art. 31 da Instrução Normativa nº 3, de 26 de abril de 2018.

8.2.6. O setor competente para proceder o pagamento deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

8.2.6.1. o prazo de validade;

8.2.6.2. a data da emissão;

8.2.6.3. os dados do contrato e do órgão contratante;

8.2.6.4. o período de prestação dos serviços;

8.2.6.5. o valor a pagar; e

8.2.6.6. eventual destaque do valor de retenções tributárias cabíveis.

8.2.7. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

8.2.8. Nos termos do item 1, do Anexo VIII-A da Instrução Normativa SEGES/MP nº 05, de 2017, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

8.2.8.1. não produziu os resultados acordados;

8.2.8.2. deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida;

8.2.9. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

8.2.10. Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

8.2.11. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

8.2.12. Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018.

8.2.13. Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

8.2.14. Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

8.2.15. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.

8.2.15.1. Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante.

8.2.16. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, em especial a prevista no artigo 31 da Lei 8.212, de 1993, nos termos do item 6 do Anexo XI da IN SEGES/MP n. 5/2017, quando couber.

8.2.17. É vedado o pagamento, a qualquer título, por serviços prestados, à empresa privada que tenha em seu quadro societário servidor público da ativa do órgão contratante, com fundamento na Lei de Diretrizes Orçamentárias vigente.

8.2.18. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela é calculada mediante a aplicação da seguinte fórmula:

$EM = I \times N \times VP$, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = (TX/100)/365 = (6/100)/365 = 0,00016438$$

$$TX = \text{Percentual da taxa anual} = 6\%$$

8.3. Da Garantia

8.3.1. O adjudicatário prestará garantia de execução do contrato, nos moldes do art. 56 da Lei nº 8.666, de 1993, com validade durante a execução do contrato e por 90 (noventa) dias após o término da vigência contratual, em valor correspondente a 5% (cinco por cento) do valor total do contrato.

8.3.2. No prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do Contratante, contados da assinatura do contrato, a Contratada deverá apresentar comprovante de prestação de garantia, podendo optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária.

8.3.3. A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger um período de 90 dias após o término da vigência contratual, conforme item 3.1 do Anexo VII-F da IN SEGES/MP nº 5/2017.

8.3.4. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

8.3.4.1. prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

8.3.4.2. prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato;

8.3.4.3. multas moratórias e punitivas aplicadas pela Administração à Contratada; e

8.3.4.4. obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pela Contratada, quando couber.

8.3.5. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item anterior, observada a legislação que rege a matéria.

8.3.6. A garantia em dinheiro deverá ser efetuada em favor da Contratante, em conta específica na Caixa Econômica Federal, com correção monetária.

8.3.7. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Economia.

8.3.8. No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

8.3.9. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada à nova situação ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

8.3.10. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a Contratada obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, contados da data em que for notificada.

8.3.11. A Contratante executará a garantia na forma prevista na legislação que rege a matéria.

8.3.12. Será considerada extinta a garantia:

8.3.12.1. com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da Contratante, mediante termo circunstanciado, de que a Contratada cumpriu todas as cláusulas do contrato;

8.3.12.2. no prazo de 90 (noventa) dias após o término da vigência do contrato, caso a Administração não comunique a ocorrência de sinistros, quando o prazo será ampliado, nos termos da comunicação, conforme estabelecido na alínea "h2" do item 3.1 do Anexo VII-F da IN SEGES/MP n. 05/2017.

8.3.13. O garantidor não é parte para figurar em processo administrativo instaurado pela Contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à Contratada.

8.3.14. A Contratada autoriza a Contratante a reter, a qualquer tempo, a garantia, na forma prevista no neste Termo de Referência e no Contrato.

8.4. Do Reajuste de Preços

8.4.1. Não há previsão de reajuste para os contratos de correntes deste Termo de Referência.

8.5. Subcontratação

8.5.1. Não será permitida a subcontratação.

8.5.1.1. Como exceção, será permitida a subcontratação do serviço de instalação física dos equipamentos e organização do cabeamento referentes aos equipamentos constantes dos itens 3, 7, 10 e 13.

8.5.1.1.1. A instalação física de equipamentos e organização de cabeamento são atividades acessórias que não exigem conhecimento especializado e, portanto, passíveis de serem terceirizadas. Tendo em vista que o contrato abrangerá a colocação dos equipamentos todas unidades da CGU, logo, em todas as capitais do país, a subcontratação desta etapa poderá gerar economia, desde que a empresa contratada se responsabilize pela qualidade do serviço a ser prestado por subcontratada. Ressalte-se que a atividade passível de ser subcontratada não se confunde com a configuração lógica dos equipamentos, sendo esta é atividade especializada que exige conhecimento técnico específico e mais qualificado e, portanto, não é passível de ser terceirizada.

9. ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

Item	Descrição	Unidade	Valor Unitário	Quantidade Inicial	Valor Total Inicial	Quantidade Total	Valor Total Final
1	Switch acesso - tipo 1 (sede e secundários regionais)	Unidade	40.628,22	66	2.681.462,52	97	3.940.937,34
2	Garantia estendida - switch acesso - tipo 1 - 5 anos - 8x5xNBD	Unidade	7.963,42	66	525.585,72	97	772.451,74
3	Instalação switch acesso - tipo 1	Unidade	1.995,91	66	131.730,06	97	193.603,27
4	Módulo e cabo de empilhamento para switch acesso - tipo 1	Unidade	2.002,70	0	-	19	38.051,30
5	Switch acesso - tipo 2 (principais regionais)	Unidade	44.413,06	22	977.087,32	58	2.575.957,48
6	Garantia estendida - switch acesso - tipo 2 - 5 anos - 8x5xNBD	Unidade	8.804,73	22	193.704,06	58	510.674,34
7	Instalação switch acesso - tipo 2	Unidade	1.946,55	22	42.824,10	58	

							112.899,90
8	Switch distribuição	Unidade	49.527,75	6	297.166,50	18	891.499,50
9	Garantia estendida - switch distribuição - 5 anos - 8x5xNBD	Unidade	8.651,20	6	51.907,20	18	155.721,60
10	Instalação switch distribuição	Unidade	1.680,12	6	10.080,72	18	30.242,16
11	Switch core	Unidade	128.324,25	2	256.648,50	2	256.648,50
12	Garantia estendida - switch core - 5 anos - 24x7x4	Unidade	29.343,40	2	58.686,80	2	58.686,80
13	Instalação switch core	Unidade	10.398,61	2	20.797,22	2	20.797,22
14	SFP28 25GBase-SR	Unidade	3.047,58	12	36.570,96	40	121.903,20
15	SFP 1000BaseT	Unidade	814,71	4	3.258,84	14	11.405,94
16	SFP 1000BaseSX	Unidade	575,01	4	2.300,04	10	5.750,10
17	SFP+ 10GBaseSR	Unidade	1.784,41	41	73.160,81	99	176.656,59
18	Software NAC - 5000 dispositivos - 5 anos - 24x7x4	Unidade	241.922,47	1	241.922,47	1	241.922,47
19	Instalação software NAC - 5000 dispositivos	Unidade	57.110,21	1	57.110,21	1	57.110,21
20	Software de Gerenciamento/Administração/Orquestração da Rede - 5 anos - 8x5	Unidade	299.703,62	1	299.703,62	1	299.703,62
21	Instalação do Software de Gerenciamento/Administração/Orquestração da Rede	Unidade	21.423,98	1	21.423,98	1	21.423,98
22	Repasse de conhecimento	Unidade	16.070,65	1	16.070,65	1	16.070,65
Total					5.999.202,30		10.510.117,91

9.1. O valor de referência para a contratação é de R\$ 10.510.117,91 (dez milhões, quinhentos e dez mil cento e dezessete reais e noventa e um centavos).

10. ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

10.1. Adequação Orçamentária

10.1.1. O recurso proveniente para a contratação dos itens deverá ter como origem o seguinte orçamento:

- 10.1.1.1. PI: 10.01.00 - Sustentação das soluções de TI;
- 10.1.1.2. PO: #840793: Renovação: Parque de Switches de Acesso.

10.2. Cronograma Físico-Financeiro

10.2.1. Todos os eventos de pagamento estão definidos no item 8.2.1.

10.2.2. Segue abaixo o cronograma de execução físico-financeiro que considerou:

- 10.2.2.1. A contratação dos quantitativos iniciais;
- 10.2.2.2. A assinatura do contrato dentro do exercício de 2020;
- 10.2.2.3. A emissão da ordem de serviço para a prestação do serviço de Repasse de Conhecimento no início do exercício de 2021.

Evento	Prazo em dias úteis após assinatura do contrato	Exercício previsto para empenho da despesa	Exercício previsto para liquidação da despesa	Valor
Entrega de todos os bens contratados	55	2020	2021	4.327.655,58
Instalação de equipamentos e software	240	2020	2021	1.356.443,26
Instalação do Software NAC	305	2020	2022	299.032,68
Repasse de Conhecimento	35	2020	2020	16.070,65

11. DA VIGÊNCIA DO CONTRATO

11.1. Os contratos decorrentes deste Termo de Referência vigorarão por 60 (sessenta) meses, contados a partir da data de suas respectivas assinaturas, conforme orientação "BOAS PRÁTICAS, ORIENTAÇÕES E VEDAÇÕES PARA CONTRATAÇÃO DE ATIVOS DE TIC – Versão 4" (SEI 1623857).

12. DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

12.1. Tipo e Modalidade de Licitação

12.1.1. A licitação será do tipo menor preço e realizada na modalidade Pregão Eletrônico.

12.2. Da classificação dos Bens/Serviços

12.2.1. Os bens referentes aos itens 1, 4, 5, 8, 11 e 14 a 18 e 20 são classificados com bens comuns.

12.2.2. Os serviços referentes aos itens 3, 7, 10, 13, 19, 21 e 22 são classificados como serviços comuns de caráter não-continuado, sem fornecimento de mão de obra exclusiva.

12.2.3. Os serviços referentes aos itens 2, 6, 9, 12 são classificados como serviços comuns de caráter continuado, sem fornecimento de mão de obra exclusiva.

12.3. Regime

12.3.1. Quanto ao regime de execução, os serviços serão caracterizados conforme tabela a seguir:

Item	Descrição	Empreitada por Preço Unitário	Empreitada por Preço Global	Execução por Tarefa
2	Garantia estendida - switch acesso - tipo 1 - 5 anos - 8x5xNBD	X	-	-
3	Instalação switch acesso - tipo 1	-	X	-
6	Garantia estendida - switch acesso - tipo 2 - 5 anos - 8x5xNBD	X	-	-
7	Instalação switch acesso - tipo 2	-	X	-
9	Garantia estendida - switch distribuição - 5 anos - 8x5xNBD	X	-	-
10	Instalação switch distribuição	-	X	-

12	Garantia estendida - switch core - 5 anos - 24x7x4	X	-	-
13	Instalação switch core	-	X	-
19	Instalação software NAC - 5000 dispositivos	X	-	-
21	Instalação do Software de Gerenciamento/Administração/Orquestração da Rede	X	-	-
21	Instalação software de gerência/administração	X	-	-

12.4. Justificativa para a Aplicação do Direito de Preferência e Margens de Preferência

12.4.1. Verifica-se a aplicabilidade de Direito de Preferência e Margens de Preferência pela Lei Complementar nº 123/2006, conforme regras a serem definidas no respectivo Edital do certame.

12.4.2. Porém, verifica-se a **não** aplicabilidade de Direito de Preferência e Margens de Preferência preconizados pelo Decreto nº 7.174/2010, tendo em vista a necessidade de agrupamento dos itens.

12.5. Critérios de Qualificação Técnica para a Habilitação

12.5.1. Para habilitação de sua proposta, o proponente deverá apresentar a documentação abaixo com o objetivo de comprovar a sua qualificação técnica:

12.5.1.1. Declaração ou Atestado de Capacidade Técnico-Operacional, fornecido por pessoa jurídica de direito público ou privado, que comprove que o licitante prestou satisfatoriamente os seguintes serviços:

12.5.1.1.1. Provimento de pelo menos 40 (quarenta) equipamentos de switches de acesso, incluindo provimento de garantia/suporte por pelo menos um ano.

12.5.1.1.2. Provimento de 6 (seis) equipamentos de switches de distribuição, incluindo provimento de garantia/suporte por pelo menos um ano.

12.5.1.1.3. Provimento de um cluster de switches core, incluindo provimento de garantia/suporte por pelo menos um ano.

12.5.1.1.4. Provimento de software NAC (Network Access Control) para parque de pelo menos 2.500 (dois mil e quinhentos) dispositivos, incluindo provimento de garantia/suporte por pelo menos um ano.

12.5.1.1.5. Realização de implantação de pelo menos uma estrutura de redes com no mínimo 10 (dez) ativos de rede com tecnologia SDN, incluindo provimento de garantia/suporte por pelo menos um ano. Serão consideradas implementações de SDN os projetos que envolverem SD-LAN ou SDN para redes de datacenter (por similaridade). Não serão aceitos projetos com tecnologias SD-WAN.

12.6. Da proposta comercial

12.6.1. Também deverão ser apresentados documentos abaixo como parte obrigatória de sua proposta:

12.6.1.1. Declaração de estar ciente de que a CGU possui um único CNPJ, não possui inscrição estadual e não emite nota fiscal.

12.6.1.2. Declaração da licitante que ateste a não ocorrência do registro de oportunidade, de modo a garantir o princípio constitucional da isonomia e a seleção da proposta mais vantajosa para a Administração Pública, conforme disposto na Lei nº 8.666, de 1993.

12.6.1.3. Documentação que comprove o atendimento dos requisitos estabelecidos neste TR, em especial os requisitos técnicos estabelecidos no Anexo 1 deste TR, que será composta por:

12.6.1.3.1. Documento(s) público(s), emitidos pelo fabricante dos equipamentos/software, que comprovem que eles atendem cada requisito estabelecido no Anexo 1.

12.6.1.3.2. Documento, utilizando-se como modelo a planilha constata do Anexo 7, indicando em que documento/página está a informação para a comprovação do respectivo atendimento.

12.6.1.4. Para os itens de 1, 4, 5, 8, 11, 14 a 17, declaração de que os equipamentos a serem fornecidos e todos os seus componentes serão novos, de primeiro uso e estão em linha de fabricação e não há anúncio de end-of-sales e end-of-support;

13 - DOS ANEXOS

13.1. São anexos deste Termo de Referência

13.1.1. ANEXO 1 - ESPECIFICAÇÃO TÉCNICA;

13.1.2. ANEXO 2 - ENDEREÇOS;

13.1.3. ANEXO 3 - DISTRIBUIÇÃO DAS ENTREGAS DE BENS E PRESTAÇÃO DE SERVIÇO;

13.1.4. ANEXO 4 - MODELO DE TERMO DE CONFIDENCIALIDADE;

13.1.5. ANEXO 5 - MODELO DE TERMO DE CIÊNCIA;

13.1.6. ANEXO 6 - MODELO DE AVALIAÇÃO DE TREINAMENTO; e

13.1.7. ANEXO 7 - MODELO DE PLANILHA PARA COMPROVAÇÃO DE REQUISITOS.

14 – DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO

14.1. A Equipe de Planejamento da Contratação foi instituída pelos atos de Designação SEI 1514032 e 1573390.

<p>_____</p> <p>Integrante Requisitante - substituto</p> <p>Salatiel Robson Barbosa de Oliveira</p> <p>[ASSINATURA ELETRÔNICA]</p>	<p>_____</p> <p>Integrante Técnico</p> <p>Gustavo Moura de Sousa</p> <p>[ASSINATURA ELETRÔNICA]</p>	<p>_____</p> <p>Integrante Administrativo</p> <p>Fábio Luciano Ikijiri</p> <p>[ASSINATURA ELETRÔNICA]</p>
---	--	--

<p>Autoridade Máxima da Área de TIC</p> <p>Henrique Aparecido da Rocha</p>

ANEXO 1 – ESPECIFICAÇÃO TÉCNICA

1. Requisitos da solução de SDN-LAN

- 1.1. A solução de SD-LAN deverá permitir a criação de virtualização (overlay) que permita a abstração da infraestrutura física (underlay). Essa rede virtual será chamada de fabric;
- 1.2. A solução de SD-LAN deve utilizar protocolos abertos para criar o plano de controle e o plano de dados;
 - 1.2.1. Para a tecnologia de SD-LAN, o plano de controle será tratado como o conjunto de protocolos e mensagens que serão trocadas pelos dispositivos da infraestrutura (underlay) para criar a rede overlay. Alguns exemplos desses protocolos utilizados para essa funcionalidade são: MP-BGP, IS-IS e LISP;
 - 1.2.2. Para a tecnologia de SD-LAN, o plano de dados é a tecnologia de encapsulamento dos dados utilizado para garantir a segregação dos diferentes perfis de rede. Alguns exemplos dessas tecnologias são: VXLAN (Virtual eXtensible Local Area Network) e SPB (Shortest Path Bridging). A maior parte das implementações de SD-LAN utiliza VXLAN, motivo pelo qual foi utilizado como referência em alguns requisitos deste Termo de Referência, embora sejam permitidas outras tecnologias como SPB. Em função do exposto, neste Termo de Referência, onde houver referência a VXLAN, deve ser feita a leitura VLAN (ou similar).
- 1.3. A rede underlay é a infraestrutura composta por switches físicos, responsáveis pelo encaminhamento de pacotes e deverá possuir, no mínimo, as seguintes características:
 - 1.3.1. Ser baseada em protocolo IP (Fabric IP);
 - 1.3.2. Possuir suporte à endereçamento IPv4 e IPv6;
 - 1.3.3. Possuir suporte, no mínimo, aos protocolos de roteamento OSPF, BGPv4 e MP-BGP;
 - 1.3.4. Permitir a criação de uma topologia full-mesh sem loops e sem utilização do protocolo Spanning-Tree;
 - 1.3.5. Efetuar balanceamento de tráfego baseado em ECMP (Equal-Cost-Multipath);
 - 1.3.6. Ser compatível com o mecanismo de Multi-Chassis Etherchannel ou similar;
 - 1.3.7. Permitir o provisionamento, administração, automação, gerenciamento e monitoramento da saúde física dos equipamentos de forma centralizada, através de controladoras de rede, via GUI (Graphical User Interface);
 - 1.3.8. Implementar o protocolo VXLAN (ou similar) nos switches, para permitir a configuração de todas as funcionalidades necessárias para a ativação do plano de dados, denominada rede overlay.
- 1.4. A rede overlay é a abstração da infraestrutura física em uma rede virtual ou plano de dados, utilizando o protocolo VXLAN (ou similar), e deverá possuir, no mínimo, as seguintes características:
 - 1.4.1. Realizar switching de tráfego de camada 2 (intra-VXLAN) e roteamento camada 3 (inter-VXLAN);
 - 1.4.2. Realizar a função de Layer 2 Gateway, para mapear VLANs para VXLANs e vice-versa e efetuar o encapsulamento e desencapsulamento de VXLAN;
 - 1.4.3. Realizar função de Layer 3 Gateway, para permitir o roteamento entre VXLANs distintas ou entre VXLAN e VLAN e vice-versa;
 - 1.4.4. Implementar mecanismos de Plano de Controle para o protocolo VXLAN, para minimizar o tráfego de BUM (Broadcast, Unknown Layer 2 Unicast e Multicast), utilizando MP-BGP EVPN e/ou outros protocolos que executem funcionalidades semelhantes;
- 1.5. A solução de SD-LAN deve permitir o funcionamento de tráfego multicast;
- 1.6. Será considerada como controladora SD-LAN o conjunto de hardware (físico ou virtual) ou software que gerenciam e automatizam as camadas de overlay e underlay implementando todas as características descritas para os switches solicitados;
- 1.7. Considerando as camadas underlay e overlay, serão aceitos para composição da solução o arranjo do tipo hardware/software ou software/software ou hardware/hardware para definir e implementar as funcionalidades de controladora SD-LAN;
- 1.8. Em caso de perda de comunicação entre os switches e o cluster de controladoras, a rede deverá continuar a operar normalmente sem interrupção de tráfego;
- 1.9. Os equipamentos que operem como controladores devem:
 - 1.9.1. Ser totalmente compatíveis com os switches solicitados, para manutenção de compatibilidade da solução;
 - 1.9.2. Funcionar como o ponto central de administração, gerência e automação do fabric e dos seus elementos;
 - 1.9.3. Ser o ponto central de gestão e aplicação de políticas baseadas em aplicações para os recursos físicos e virtuais do fabric;
 - 1.9.4. Estabelecer e manter um modelo gráfico de abstração de todo o fabric, que permita a simplificação de sua manutenção.
 - 1.9.5. Gerenciar as mudanças de políticas no modelo gráfico de abstração da rede, impedindo, assim, que elas sejam feitas, diretamente, nos equipamentos da rede (underlay). Em outras palavras, a abstração da rede é uma entidade, completamente, separada da rede de fato e, assim, a indisponibilidade dos controladores não deve impactar o encaminhamento de tráfego dentro do fabric – caracterizando, então, o desacoplamento do plano de dados em relação ao plano de controle;
 - 1.9.6. O provisionamento, administração, automação e gerenciamento das camadas underlay e overlay poderá ser realizado através de uma ou mais soluções de controladoras de rede do mesmo fabricante;
 - 1.9.7. Devem ser instaladas sempre em pares com alta disponibilidade.
 - 1.9.8. A falha de um dos dois nós deve permitir que fabric continue funcionando sem degradação de performance (sendo permitida apenas a perda de capacidade de encaminhamento das portas relativas ao equipamento defeituoso).
 - 1.9.9. Operar de forma independente do plano de dados da rede, não podendo ser um ponto de convergência do fluxo de dados da rede do fabric;

2. Sede – SD-LAN

- 2.1. A topologia física (underlay) da sede será do tipo hierárquica (core, distribuição, acesso);
- 2.2. O fabric criado pela solução de SD-LAN deve operar em conjunto com a solução de NAC para que os dispositivos que se conectarão a camada de acesso sejam classificados nos diferentes perfis;
- 2.3. A solução de SD-LAN deve permitir a segmentação, ou seja, o controle de tráfego entre os diferentes perfis e dentro do mesmo perfil;
- 2.4. Os dispositivos finais devem ser classificados em diferentes perfis conforme definição da CONTRATANTE. Alguns exemplos de perfis que pretendem ser utilizados são: telefones IP, access-points, impressoras, câmeras de vigilância. Aos diferentes perfis deve ser possível aplicar políticas distintas, que utilizem diferentes características de controle de acesso e de filtragem de tráfego;
- 2.5. Os equipamentos de acesso farão a interface de comunicação da rede overlay com os dispositivos finais;
- 2.6. Os equipamentos de distribuição funcionarão exclusivamente como intermediários (trânsito) da rede overlay;
- 2.7. Os equipamentos de core farão a interface de comunicação da rede overlay com a rede externa ao campus. Esses equipamentos também farão o papel de controladores do fabric;
- 2.8. Topologia física da sede:
 - 2.8.1. A conexão entre os equipamentos acesso e distribuição será feita utilizando cabos UTP CAT6 (menores do que 30 metros) a pelo menos 5 Gbps;
 - 2.8.2. A conexão entre os equipamentos distribuição e core deverá ser feita a 25 Gbps utilizando fibra óptica MM (multimodo) OM3.

3. Regionais – SD-LAN ou segmentação em VLANs

- 3.1. A solução das regionais poderá ser atendida de 2 formas, quais sejam:
 - 3.1.1. Forma 1: Solução de SD-LAN semelhante ao ambiente utilizado na sede (não se trata de uma extensão da rede de overlay da sede, pois cada regional possui sua própria infraestrutura de TI). Neste caso, os equipamentos switches acesso - tipo 1 (sede e secundários regionais) farão a interface de comunicação da rede overlay com os dispositivos finais. Os equipamentos switches acesso - tipo 2 (principais regionais) farão a interface de comunicação da rede overlay com os dispositivos finais, a interface de comunicação da rede overlay com a rede externa ao campus e farão o papel de controladores do fabric;
 - 3.1.2. Forma 2: Solução tradicional de redes campus, baseadas em VLANs. Neste caso os equipamentos devem operar em conjunto com a solução de NAC para que os perfis de dispositivos que se conectarão aos switches sejam mapeados em VLANs. Neste caso o controle do tráfego entre diferentes perfis (VLANs) deve ser feito pelo Firewall existente nas unidades regionais (e que não faz parte da solução deste Termo de Referência);
- 3.2. Todas as regionais da CGU possuirão um núcleo mínimo formado por 2 (duas) unidades de switches acesso - tipo 2 (principais regionais). Esses equipamentos receberão as conexões com o firewall, as conexões com o servidor de rede de cada unidade bem como conexão de dispositivos final. Os dois equipamentos que formam esse núcleo mínimo também receberão conexões de dispositivos finais;
- 3.3. Em algumas regionais, será necessário adicionar switches que receberão apenas dispositivos finais, quais sejam: switches acesso - tipo 1 (sede e secundários regionais). As conexões dos switches tipo 2 com a pilha de switches tipo 1 devem ser feitas a pelo menos 5 Gbps (utilizando fibra ou UTP conforme o tipo da regional).

4. Considerações gerais

- 4.1. Os itens 1 e 5 possuem características semelhantes, exceto pelo módulo e cabo de empilhamento, que deve ser oferecido junto com o switch no caso do item 5. Assim, é

- importante observar que o item 1.3.4 é diferente do item 5.3.4. Ademais, o item 5.3.6 não encontra correspondente no item 1;
- 4.2. Para alguns fabricantes poderão oferecer a solução SD-LAN também para as unidades regionais e neste caso os itens 1 e 5 podem ser modelos distintos. Para outros fabricantes, o mesmo modelo de switch pode ser ofertado para os dois itens em questão. É importante observar que para fins de definição da licitante vencedora, o sistema compranet irá observar os lances ofertados de forma separada. Entretanto, na fase de análise de propostas, caso o mesmo produto foi ofertado para atender a dois itens, será observada a relação entre os itens 1, 2, 3, 4, 5, 6 e 7. Por exemplo, caso seja ofertado o mesmo modelo de switch para os itens 1 e 5, não faz sentido que o item 1 seja mais caro que o item 5, nem faz sentido que haja diferença de valor entre os itens 2 e 6;
- 4.3. O Plano de Implantação pode ser apresentado em um único documento, aproveitando os aspectos que se repetem para todos os equipamentos e para todas as localidades;
- 4.4. O AS-BUILT pode ser apresentado em um único documento, aproveitando os aspectos que se repetem para todos os equipamentos e para todas as localidades;

Item 1. Switch acesso - tipo 1 (sede e secundários regionais)

- 1.1. Características gerais e funcionalidades
- 1.1.1. Possuir pelo menos 1 (uma) fonte de alimentação interna, do tipo AC, bivolt com seleção automática de tensão (na faixa de 100 a 240 V) e frequência (de 50/60 Hz);
- 1.1.2. Deve possuir no máximo 1U (uma unidade de rack) de altura;
- 1.1.3. Permitir que seja montado em rack padrão de 19" (dezenove polegadas), incluindo todos os acessórios necessários para tal;
- 1.1.4. Possuir LEDs, por porta, que indiquem a integridade, a atividade e a velocidade de conexão do link;
- 1.1.5. Permitir o encaminhamento de "jumbo frames" em todas as portas (pacotes de 9016 bytes);
- 1.1.6. Possuir configuração de CPU e memória (RAM e Flash) suficiente para a implantação de todas as funcionalidades descritas nesta especificação;
- 1.1.7. Permitir a criação de, no mínimo, 500 (quinhentas) VLANs ativas simultaneamente baseadas em portas, com suporte a no mínimo 4.000 (quatro mil) VLANs IDs;
- 1.1.8. Suportar simultaneamente em sua memória flash (ou semelhante), duas imagens do sistema operacional entregue com a solução;
- 1.1.9. Deve implementar tecnologia para monitoramento de fluxos de tráfego como, por exemplo: IPFIX (RFC 7011), Netflow (RFC 3954), Netflow Lite, sFlow (RFC 3176), Jflow, NetStream entre outros; garantindo alta visibilidade do tráfego de rede;
- 1.1.9.1. Para cada fluxo devem ser coletadas, no mínimo, as seguintes informações: endereços IP de origem/destino, portas TCP/UDP de origem/destino, interfaces de entrada e saída do tráfego, número de pacotes transmitidos;
- 1.1.10. Deve suportar IPv4 e IPv6; N/A
- 1.1.10.1. Deverá permitir a configuração de endereços IPv6 para gerenciamento e operar em modo dual stack (IPv4 e IPv6), suportando consultas de DNS com resolução de nomes em endereços IPv6;
- 1.1.10.2. Deverá implementar ICMPv6 com as seguintes funcionalidades: ICMP Request, ICMP Reply, ICMP Neighbor Discovery Protocol (NDP), ICMP MTU Discovery.
- 1.1.11. Possuir porta de console com conector USB (de qualquer tipo), para acesso à interface de linha de comando. Serão aceitos adaptadores para o atendimento deste item.
- 1.2. Características específicas
- 1.2.1. Deve suportar o empilhamento físico, com cabos redundantes, de no mínimo 3 (três) unidades do mesmo tipo;
- 1.2.1.1. Deverá ser permitido o gerenciamento do empilhamento através de um único IP;
- 1.2.2. Permitir o espelhamento do tráfego total de uma porta ou de um grupo de portas ou de uma VLAN como origem;
- 1.2.2.1. Deve ser possível definir o sentido do tráfego a ser espelhado (somente entrada, somente saída ou ambos);
- 1.2.2.2. O destino pode ser outra porta localizada no mesmo switch ou em outro switch da mesma pilha.
- 1.3. Quantidade de portas e PoE (Power Over Ethernet) N/A
- 1.3.1. Deve possuir 48 (quarenta e oito) portas com conector RJ-45, autosensing, auto negociáveis;
- 1.3.1.1. Dessas portas, pelo menos 8 (oito) devem suportar no mínimo 100M/1G/2.5G/5G conforme os padrões IEEE 802.3u (100BaseTX), IEEE 802.3ab (1000BaseT) e IEEE 802.3bz (2.5GBaseT e 5GBaseT);
- 1.3.1.2. As demais devem suportar no mínimo 100M/1G conforme os padrões IEEE 802.3u (100BaseTX) e IEEE 802.3ab (1000BaseT);
- 1.3.1.3. Todas as portas RJ-45 devem suportar negociação automática de velocidade e de modo de operação (Half-Duplex e Full-Duplex), sem necessidade de alteração de configuração do dispositivo conectado à porta;
- 1.3.1.4. Todas as portas RJ-45 devem suportar Auto-MDIX.
- 1.3.2. Implementar Power over Ethernet (PoE) segundo o padrão IEEE 802.3af e Power over Ethernet Plus (PoE+) segundo o padrão IEEE 802.3at em todas as portas RJ-45, com um total de pelo menos 600W de potência disponível para alimentação exclusivamente das portas PoE/PoE+ através de fonte interna primária. Para atender este item, também serão aceitos equipamentos que implementem o padrão IEEE 802.3bt (PoE++);
- 1.3.3. Deve possuir 4 (quatro) slots 1/10 Gigabit Ethernet, compatíveis com os transceivers SFP e SFP+;
- 1.3.4. Deve suportar pelo menos 2 (duas) portas para empilhamento, cada uma com velocidade de no mínimo 40 (quarenta) Gbps (half-duplex) ou 80 (oitenta) Gbps (full-duplex);
- 1.3.4.1. O empilhamento pode ser realizado por módulo dedicado ou slots do tipo SFP ethernet disponíveis no equipamento (não podem ser consideradas as portas do item 1.3.1 nem do item 1.3.3 deste anexo para atender este requisito).
- 1.3.5. Deve ser possível utilizar todas as portas descritas nos itens acima de forma simultânea, ou seja, a utilização de uma porta não deve implicar a desativação ou não funcionamento de outra porta;
- 1.4. Gerenciamento
- 1.4.1. Possuir agente de gerenciamento SNMP (RFC 1157), MIB SNMP II (RFC 1213 ou suas atualizações), extensões MIB SNMP, MIB bridging (RFC 1493 ou RFC 4188), que possua descrição completa da MIB implementada no equipamento, inclusive as extensões privadas, se existirem;
- 1.4.2. Deve ser gerenciável via SNMP (v1, v2 e v3). Na versão v3 do SNMP devem ser implementados, pelo menos os seguintes modos de operação: Sem autenticação e sem privacidade (noAuthNoPriv), com autenticação e sem privacidade (authNoPriv) e com autenticação e com privacidade (AuthPriv). Deve suportar no mínimo os algoritmos criptográficos 3DES e AES128 no modo AuthPriv;
- 1.4.3. Deve permitir a transferência de arquivos através do protocolo TFTP (Trivial File Transfer Protocol) ou FTP (File Transfer Protocol) ou SFTP (SSH File Transfer Protocol);
- 1.4.4. Permitir a gravação de log externo (syslog). Deve ser possível definir o endereço IP de origem dos pacotes Syslog gerados pelo switch.
- 1.5. Capacidade
- 1.5.1. Deve possuir capacidade para pelo menos 16.000 (dezesesseis mil) endereços MAC na tabela de comutação;
- 1.5.2. Possuir uma matriz de comutação a capacidade de, no mínimo 200 (duzentos) Gbps;
- 1.5.2.1. Valor calculado considerando: 8 interfaces de 5 Gbps, 40 interfaces de 1 Gbps, 4 interfaces de 10 Gbps e 2 interfaces de 40 Gbps (empilhamento).
- 1.5.3. Possuir capacidade de encaminhamento de, no mínimo 297 (duzentos e noventa e sete) Mpps (milhões de pacotes por segundo);
- 1.6. Protocolos e padrões suportados
- 1.6.1. Implementar VLAN segundo o padrão 802.1q;
- 1.6.2. Implementar a funcionalidade de agregação de portas, segundo o padrão 802.3ad;
- 1.6.3. Implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN;
- 1.6.4. Implementar padrão IEEE 802.1p (Class of Service) para cada porta;
- 1.6.5. Implementar padrão IEEE 802.1s (Multiple Spanning Tree);
- 1.6.6. Implementar o padrão IEEE 802.3x (Flow Control);
- 1.6.7. Implementar LLDP;
- 1.6.8. Implementar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol), incluindo autenticação entre os peers. (RFC 1305, RFC 5905);
- 1.6.9. Implementar IGMP Snooping (v1, v2 e v3).
- 1.7. Segurança
- 1.7.1. Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo RADIUS;
- 1.7.2. Proteger a interface de comando do equipamento através de senha;
- 1.7.3. Implementar o protocolo SSH v2 para acesso à interface de linha de comando;
- 1.7.4. Permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet e SSH. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH;
- 1.7.5. Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;
- 1.7.6. Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;
- 1.7.7. Permitir controlar quais comandos os usuários ou grupos de usuários podem emitir;
- 1.7.8. Deve possuir funcionalidade que verifique e limite a quantidade de endereços MAC por porta de usuário. Em caso de violação das condições, deve ser possível que a interface seja bloqueada. Deve ser possível que o desbloqueio seja configurado para ocorrer de duas formas: de forma automática e periódica pelo próprio equipamento e de forma manual pelo administrador da rede. O status de bloqueio deve ser visualizado por consulta snmp.
- 1.7.9. Implementar inspeção do protocolo ARP (Address Resolution Protocol) e possuir mecanismos de proteção contra ataques do tipo "ARP Poisoning";
- 1.7.10. Promover análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu

o endereço e porta física do switch em que se localiza tal MAC;

1.7.11. Deve possuir funcionalidade que analise o tráfego de DHCP em portas de usuários, impedindo que esse tipo de porta responda requisições de DHCP bem como deve limitar a taxa de requisições de DHCP. Todo o tráfego que viola as condições deve ser descartado.

1.7.12. Deve possuir funcionalidade que analisa o tráfego de uma interface de modo a garantir que as respostas de mensagens ARP sejam exclusivamente permitidas caso o referido endereço IP tenha sido atribuído via DHCP a um equipamento de determinada interface de usuário. A funcionalidade também deve impedir que os usuários configurem endereços IP de forma estática. Todo o tráfego que viola as condições deve ser descartado.

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

1.7.14. Possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta do switch esteja colocada no modo “Fast Forwarding” (conforme previsto no padrão IEEE 802.1w). Caso seja detectado o recebimento de BPDUs do protocolo spanning-tree nessas portas ou mesmo a detecção de loops de camada 2, elas devem ser bloqueadas. Deve ser possível que o desbloqueio seja configurado para ocorrer de duas formas: de forma automática e periódica pelo próprio equipamento e de forma manual pelo administrador da rede. O status de bloqueio deve ser visualizado por consulta snmp.

1.7.15. Implementar padrão IEEE 802.1x (Port Based Network Access Control);

1.7.15.1. Deve implementar a atribuição de VLANs após a identificação do usuário, atribuição do usuário a uma VLAN “Guest” caso a máquina que esteja utilizando para acesso à Rede não tenha cliente 802.1x operacional. Caso ocorra falha de autenticação de um usuário com um cliente 802.1x operacional o mesmo deverá ser alocado em uma VLAN “quarentena” com características próprias;

1.7.15.2. Implementar “accounting” das conexões IEEE 802.1x. Deve possibilitar o registro de pelo menos as seguintes informações da conexão: nome do usuário, switch em que o computador do usuário está conectado, porta do switch usada para acesso, endereço MAC e IP da máquina, horários de início e término da conexão da sessão;

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

1.7.15.4. Deve ser possível especificar o intervalo de tempo para obrigar o cliente a se reautenticar (reautenticação periódica);

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

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

1.7.15.7. Deve encaminhar ao servidor RADIUS a solicitação de autenticação de clientes 802.1x;

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

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

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

1.7.15.11. Implementar associação automática de ACL da porta do switch através da qual o usuário requisitou acesso à rede

item 2. Garantia estendida - switch acesso - tipo 1 - 5 anos - 8x5xNBD

2.1. O serviço de garantia terá vigência de 60 (sessenta meses);

2.2. O serviço de garantia estendida se caracteriza pelos serviços de:

2.2.1. Atualização dos softwares residentes nos equipamentos;

2.2.2. Suporte técnico on-site, em modelo 8X5XNBD (oito horas por dia, cinco dias na semana com resolução no próximo dia útil).

2.3. A garantia estendida poderá ser realizada em primeira instância pela CONTRATADA, mas deverá haver a possibilidade de escalar o serviço ao fabricante sempre que necessário;

2.4. Fará parte da aceitação do serviço a comprovação do registro do serviço de garantia estendida por 60 (sessenta meses);

2.4.1. Os níveis mínimos de serviço estabelecidos para a garantia estendida estão descritos no item 7.2 do Termo de Referência assim como o cálculo das sanções por descumprimento estão descritos no item 8.1.

item 3. Instalação switch acesso - tipo 1

3.1. Planejamento

3.1.1. Deve ser executado por profissional(ais) com experiência em gerenciamento de projetos e certificação na área de roteamento/switching. Deve ser apresentado Plano de Implantação contendo pelo menos os seguintes itens:

3.1.1.1. Deve prever topologia lógica e física dos equipamentos envolvidos;

3.1.1.2. Deve prever a configuração prévia de todos os equipamentos;

3.1.1.3. Deve contemplar a elaboração de plano de testes;

3.1.1.4. Deve prever a migração de todas as VLANs, endereços IP, roteamento unicast (estático e dinâmico) e multicast (quando aplicável);

3.1.1.5. Deve prever a elaboração de plano de face do rack, antes e após a migração/instalação;

3.1.1.6. Deve prever o plano de migração (de/para) do cabeamento estruturado, incluindo posições de patch-panel e/ou DIOS;

3.1.1.7. Deve prever orientações e sugestões de eventuais ajustes nos equipamentos da CGU que serão integrados aos switches.

3.2. Migração/instalação

3.2.1. Deve ser executado por profissional(ais) com certificação na área de roteamento/switching;

3.2.2. A critério da CONTRATANTE, as etapas que envolvam risco de causar impacto no funcionamento do ambiente deve ser executada em dias e horários não úteis;

3.2.3. Deve prever a atualização do firmware dos equipamentos para a versão mais recente que seja considerada estável pelo fabricante;

3.2.4. Deve prever a remoção física dos equipamentos e cabos do sistema existente (quando for aplicável);

3.2.5. Deve prever a instalação física dos equipamentos e cabos do novo sistema;

3.2.6. Será permitida a subcontratação da instalação física dos equipamentos e organização do cabeamento;

3.2.7. Deve prever a execução do plano de testes.

3.3. As-Built

3.3.1. Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (as-built), etapas de execução e toda informação pertinente a posterior continuidade e manutenção da solução instalada;

item 4. Módulo e cabo de empilhamento para switch acesso - tipo 1

4.1. Deve ser compatível com o item 1 desta especificação técnica “Switch acesso - tipo 1 (sede e secundários regionais)”;

4.2. Deve possuir pelo menos 2 (duas) portas para empilhamento, cada uma com velocidade de no mínimo 40 (quarenta) Gbps (half-duplex) ou 80 (oitenta) Gbps (full duplex);

4.2.1. O empilhamento pode ser realizado por módulo dedicado ou slots do tipo SFP ethernet disponíveis no equipamento (não podem ser consideradas as portas do item 1.3.1 nem do item 1.3.3 deste anexo para atender este requisito).

4.3. Deve ser fornecido pelo menos 1 (um) cabo para empilhamento, com comprimento de pelo menos 50 (cinquenta) centímetros.

4.4. Caso o switch seja fornecido com módulo de empilhamento embutido ou utilize slots do tipo SPF para a configuração do empilhamento, este item deve se resumir ao fornecimento do cabo.

item 5. Switch acesso - tipo 2 (principais regionais)

5.1. Características gerais e funcionalidades

5.1.1. Possuir pelo menos 1 (uma) fonte de alimentação interna, do tipo AC, bivolt com seleção automática de tensão (na faixa de 100 a 240 V) e frequência (de 50/60 Hz);

5.1.2. Deve possuir no máximo 1U (uma unidade de rack) de altura;

5.1.3. Permitir que seja montado em rack padrão de 19” (dezenove polegadas), incluindo todos os acessórios necessários para tal;

5.1.4. Possuir LEDs, por porta, que indiquem a integridade, a atividade e a velocidade de conexão do link;

5.1.5. Permitir o encaminhamento de "jumbo frames" em todas as portas (pacotes de 9016 bytes);

5.1.6. Possuir configuração de CPU e memória (RAM e Flash) suficiente para a implantação de todas as funcionalidades descritas nesta especificação;

5.1.7. Permitir a criação de, no mínimo, 500 (quinhentas) VLANs ativas simultaneamente

baseadas em portas, com suporte a no mínimo 4.000 (quatro mil) VLANs IDs;

5.1.8. Suportar simultaneamente em sua memória flash (ou semelhante), duas imagens do sistema operacional entregue com a solução;

5.1.9. Deve implementar tecnologia para monitoramento de fluxos de tráfego como, por exemplo: IPFIX (RFC 7011), Netflow (RFC 3954), Netflow Lite, sFlow (RFC 3176), Jflow, NetStream entre outros; garantindo alta visibilidade do tráfego de rede;

5.1.9.1. Para cada fluxo devem ser coletadas, no mínimo, as seguintes informações: endereços IP de origem/destino, portas TCP/UDP de origem/destino, interfaces de entrada e saída do tráfego, número de pacotes transmitidos;

5.1.10. Deve suportar IPv4 e IPv6;

5.1.10.1. Deverá permitir a configuração de endereços IPv6 para gerenciamento e operar em modo dual stack (IPv4 e IPv6), suportando consultas de DNS com resolução de nomes em endereços IPv6;

5.1.10.2. Deverá implementar ICMPv6 com as seguintes funcionalidades: ICMP request, ICMP Reply, ICMP Neighbor Discovery Protocol (NDP), ICMP MTU Discovery.

5.1.11. Possuir porta de console com conector USB (de qualquer tipo), para acesso à interface de linha de comando. Serão aceitos adaptadores para o atendimento deste item.

5.2. Características específicas

5.2.1. Deve suportar o empilhamento físico, com cabos redundantes, de no mínimo 3 (três) unidades do mesmo tipo;

5.2.1.1. Deverá ser permitido o gerenciamento do empilhamento através de um único IP;

5.2.2. Permitir o espelhamento do tráfego total de uma porta ou de um grupo de portas ou de uma VLAN como origem;

5.2.2.1. Deve ser possível definir o sentido do tráfego a ser espelhado (somente entrada, somente saída ou ambos);

5.2.2.2. O destino pode ser outra porta localizada no mesmo switch ou em outro switch da mesma pilha.

5.3. Quantidade de portas e PoE (Power Over Ethernet)

5.3.1. Deve possuir 48 (quarenta e oito) portas com conector RJ-45, autosensing, auto negociáveis;

5.3.1.1. Dessas portas, pelo menos 8 (oito) devem suportar no mínimo 100M/1G/2.5G/5G conforme os padrões IEEE 802.3u (100BaseTX), IEEE 802.3ab (1000BaseT) e IEEE 802.3bz (2.5GBaseT e 5GBaseT);

5.3.1.2. As demais devem suportar no mínimo 100M/1G conforme os padrões IEEE 802.3u (100BaseTX) e IEEE 802.3ab (1000BaseT);

5.3.1.3. Todas as portas RJ-45 devem suportar negociação automática de velocidade e de modo de operação (Half-Duplex e Full-Duplex), sem necessidade de alteração de configuração do dispositivo conectado à porta;

5.3.1.4. Todas as portas RJ-45 devem suportar Auto-MDIX.

5.3.2. Implementar Power over Ethernet (PoE) segundo o padrão IEEE 802.3af e Power over Ethernet Plus (PoE+) segundo o padrão IEEE 802.3at em todas as portas RJ-45, com um total de pelo menos 600W de potência disponível para alimentação exclusivamente das portas PoE/PoE+ através de fonte interna primária. Para atender este item, também serão aceitos equipamentos que implementem o padrão IEEE 802.3bt (PoE++);

5.3.3. Deve possuir 4 (quatro) slots 1/10 Gigabit Ethernet, compatíveis com os transceivers SFP e SFP+;

5.3.4. Deve possuir pelo menos 2 (duas) portas para empilhamento, cada uma com velocidade de no mínimo 40 (quarenta) Gbps (half-duplex) ou 80 (oitenta) Gbps (fullduplex);

5.3.4.1. O empilhamento pode ser realizado por módulo dedicado ou slots do tipo SFP ethernet disponíveis no equipamento (não podem ser consideradas as portas do item 5.3.1 nem do item 5.3.3 deste anexo para atender este requisito).

5.3.5. Deve ser possível utilizar todas as portas descritas nos itens acima de forma simultânea, ou seja, a utilização de uma porta não deve implicar a desativação ou não funcionamento de outra porta;

5.3.6. Deve ser fornecido pelo menos 1 (um) cabo para empilhamento, com comprimento de pelo menos 50 (cinquenta) centímetros.

5.4. Gerenciamento

5.4.1. Possuir agente de gerenciamento SNMP (RFC 1157), MIB SNMP II (RFC 1213 ou suas atualizações), extensões MIB SNMP, MIB bridging (RFC 1493 ou RFC 4188), que possua descrição completa da MIB implementada no equipamento, inclusive as extensões privadas, se existirem;

5.4.2. Deve ser gerenciável via SNMP (v1, v2 e v3). Na versão v3 do SNMP devem ser implementados, pelo menos os seguintes modos de operação: Sem autenticação e sem privacidade (noAuthnPriv), com autenticação e sem privacidade (authNpPriv) e com autenticação e com privacidade (AuthPriv). Deve suportar no mínimo os algoritmos criptográficos 3DES e AES128 no modo AuthPriv;

5.4.3. Deve permitir a transferência de arquivos através do protocolo TFTP (Trivial File Transfer Protocol) ou FTP (File Transfer Protocol) ou SFTP (SSH File Transfer Protocol);

5.4.4. Permitir a gravação de log externo (syslog). Deve ser possível definir o endereço IP de origem dos pacotes Syslog gerados pelo switch.

5.5. Capacidade

5.5.1. Deve possuir capacidade para pelo menos 16.000 (dezesesseis mil) endereços MAC na tabela de comutação;

5.5.2. Possuir uma matriz de comutação a capacidade de, no mínimo 200 (duzentos) Gbps;

5.5.2.1. Valor calculado considerando: 8 interfaces de 5 Gbps, 40 interfaces de 1 Gbps, 4 interfaces de 10 Gbps e 2 interfaces de 40 Gbps (empilhamento).

5.5.3. Possuir capacidade de encaminhamento de, no mínimo 297 (duzentos e noventa e sete) Mpps (milhões de pacotes por segundo);

5.6. Protocolos e padrões suportados

5.6.1. Implementar VLAN segundo o padrão 802.1q;

5.6.2. Implementar a funcionalidade de agregação de portas, segundo o padrão 802.3ad;

5.6.3. Implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN;

5.6.4. Implementar padrão IEEE 802.1p (Class of Service) para cada porta;

5.6.5. Implementar padrão IEEE 802.1s (Multiple Spanning Tree);

5.6.6. Implementar o padrão IEEE 802.3x (Flow Control);

5.6.7. Implementar LLDP;

5.6.8. Implementar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol), incluindo autenticação entre os peers. (RFC 1305, RFC 5905);

5.6.9. Implementar IGMP Snooping (v1, v2 e v3).

5.7. Segurança

5.7.1. Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo RADIUS;

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

5.7.3. Implementar o protocolo SSH v2 para acesso à interface de linha de comando;

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

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

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

5.7.7. Permitir controlar quais comandos os usuários ou grupos de usuários podem emitir;

5.7.8. Deve possuir funcionalidade que verifique e limite a quantidade de endereços MAC por porta de usuário. Em caso de violação das condições, deve ser possível que a interface seja bloqueada. Deve ser possível que o desbloqueio seja configurado para ocorrer de duas formas: de forma automática e periódica pelo próprio equipamento e de forma manual pelo administrador da rede. O status de bloqueio deve ser visualizado por consulta snmp.

5.7.9. Implementar inspeção do protocolo ARP (Address Resolution Protocol) e possuir mecanismos de proteção contra ataques do tipo “ARP Poisoning”;

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

5.7.11. Deve possuir funcionalidade que analise o tráfego de DHCP em portas de usuários, impedindo que esse tipo de porta responda requisições de DHCP bem como deve limitar a taxa de requisições de DHCP. Todo o tráfego que viola as condições deve ser descartado.

5.7.12. Deve possuir funcionalidade que analisa o tráfego de uma interface de modo a garantir que as respostas de mensagens ARP sejam exclusivamente permitidas caso o referido endereço IP tenha sido atribuído via DHCP a um equipamento de determinada interface de usuário. A funcionalidade também deve impedir que os usuários configurem endereços IP de forma estática. Todo o tráfego que viola as condições deve ser descartado.

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

5.7.14. Possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta do switch esteja colocada no modo “Fast Forwarding” (conforme previsto no padrão IEEE 802.1w). Caso seja detectado o recebimento de BPDUs do protocolo spanning-tree nessas portas ou mesmo a detecção de loops de camada 2, elas devem ser bloqueadas. Deve ser possível que o desbloqueio seja configurado para ocorrer de duas formas: de forma automática e periódica pelo próprio equipamento e de forma manual pelo administrador da rede. O status de bloqueio deve ser visualizado por consulta snmp.

5.7.15. Implementar padrão IEEE 802.1x (Port Based Network Access Control);

5.7.15.1. Deve implementar a atribuição de VLANs após a identificação do usuário, atribuição do usuário a uma VLAN “Guest” caso a máquina que esteja utilizando para acesso à Rede não tenha cliente 802.1x operacional. Caso ocorra falha de autenticação de um usuário com um cliente 802.1x operacional o mesmo deverá ser alocado em uma VLAN “quarentena” com características próprias;

5.7.15.2. Implementar “accounting” das conexões IEEE 802.1x. Deve possibilitar o registro de pelo menos as seguintes informações da conexão: nome do usuário, switch em que o computador do usuário está conectado, porta do switch usada para acesso, endereço MAC e IP da máquina, horários de início e término da conexão da sessão;

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

5.7.15.4. Deve ser possível especificar o intervalo de tempo para obrigar o cliente a se reautenticar (reautenticação periódica);

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

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

5.7.15.7. Deve encaminhar ao servidor RADIUS a solicitação de autenticação de clientes 802.1x;

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

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

5.7.15.10. Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino, endereços MAC de origem

e destino;

5.7.15.11. Implementar associação automática de ACL da porta do switch através da qual o usuário requisitou acesso à rede

item 6. Garantia estendida - switch acesso - tipo 2 - 5 anos - 8x5xNBD

6.1. O serviço de garantia terá vigência de 60 (sessenta meses);

6.2. O serviço de garantia estendida se caracteriza pelos serviços de:

6.2.1. Atualização dos softwares residentes nos equipamentos;

6.2.2. Suporte técnico on-site, em modelo 8X5XNBD (oito horas por dia, cinco dias na semana com resolução no próximo dia útil).

6.3. A garantia estendida poderá ser realizada em primeira instância pela CONTRATADA, mas deverá haver a possibilidade de escalar o serviço ao fabricante sempre que necessário;

6.4. Fará parte da aceitação do serviço a comprovação do registro do serviço de garantia estendida por 60 (sessenta meses);

6.4.1. Os níveis mínimos de serviço estabelecidos para a garantia estendida estão descritos no item 7.2 do Termo de Referência assim como o cálculo das sanções por descumprimento estão descritos no item 8.1.

item 7. Instalação switch acesso - tipo 2

7.1. Planejamento

7.1.1. Deve ser executado por profissional(ais) com experiência em gerenciamento de projetos e certificação na área de roteamento/switching. Deve ser apresentado Plano de Implantação contendo pelo menos os seguintes itens:

7.1.1.1. Deve prever topologia lógica e física dos equipamentos envolvidos;

7.1.1.2. Deve prever a configuração prévia de todos os equipamentos;

7.1.1.3. Deve contemplar a elaboração de plano de testes;

7.1.1.4. Deve prever a migração de todas as VLANs, endereços IP, roteamento unicast (estático e dinâmico) e multicast (quando aplicável);

7.1.1.5. Deve prever a elaboração de plano de face do rack, antes e após a migração/instalação;

7.1.1.6. Deve prever o plano de migração (de/para) do cabeamento estruturado, incluindo posições de patch-panel e/ou DIOS;

7.1.1.7. Deve prever orientações e sugestões de eventuais ajustes nos equipamentos da CGU que serão integrados aos switches.

7.2. Migração/instalação

7.2.1. Deve ser executado por profissional(ais) com certificação na área de roteamento/switching;

7.2.2. A critério da CONTRATANTE, as etapas que envolvam risco de causar impacto no funcionamento do ambiente deve ser executada em dias e horários não úteis;

7.2.3. Deve prever a atualização do firmware dos equipamentos para a versão mais recente que seja considerada estável pelo fabricante;

7.2.4. Deve prever a remoção física dos equipamentos e cabos do sistema existente (quando for aplicável);

7.2.5. Deve prever a instalação física dos equipamentos e cabos do novo sistema;

7.2.6. Será permitida a subcontratação da instalação física dos equipamentos e organização do cabeamento;

7.2.7. Deve prever a execução do plano de testes.

7.3. As-Built

7.3.1. Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (as-built), etapas de execução e toda informação pertinente a posterior continuidade e manutenção da solução instalada;

item 8. Switch distribuição

8.1. Características gerais e funcionalidades

8.1.1. Possuir pelo menos 2 (duas) fontes de alimentação internas, redundantes, do tipo AC, bivolt com seleção automática de tensão (na faixa de 100 a 240 V) e frequência (de 50/60 Hz). As fontes deverão possuir alimentação independente, a fim de permitir a sua conexão a circuitos elétricos distintos. Não será permitida a utilização de fontes externas para atender este requisito;

8.1.2. Deve possuir no máximo 2U (duas unidades de rack) de altura. Para atender este item também será permitido o fornecimento de 2 (dois) switches empilhados formando um único cluster (neste caso, este e os demais requisitos se aplicam ao conjunto de equipamentos);

8.1.3. Permitir que seja montado em rack padrão de 19" (dezenove polegadas), incluindo todos os acessórios necessários para tal;

8.1.4. Possuir LEDs, por porta, que indiquem a integridade, a atividade e a velocidade de conexão do link;

8.1.5. Permitir o encaminhamento de "jumbo frames" em todas as portas (pacotes de 9016 bytes);

8.1.6. Possuir configuração de CPU e memória (RAM e Flash) suficiente para a implantação de todas as funcionalidades descritas nesta especificação;

8.1.7. Permitir a criação de, no mínimo, 1.000 (mil) VLANs ativas simultaneamente baseadas em portas, com suporte a no mínimo 4.000 (quatro mil) VLANs IDs;

8.1.8. Suportar simultaneamente em sua memória flash (ou semelhante), duas imagens do sistema operacional entregue com a solução;

8.1.9. Deve implementar tecnologia para monitoramento de fluxos de tráfego como, por exemplo: IPFIX (RFC 7011), Netflow (RFC 3954), Netflow Lite, sFlow (RFC 3176), Jflow, NetStream entre outros; garantindo alta visibilidade do tráfego de rede;

8.1.9.1. Para cada fluxo devem ser coletadas, no mínimo, as seguintes informações: endereços IP de origem/destino, portas TCP/UDP de origem/destino, interfaces de entrada e saída do tráfego, número de pacotes transmitidos;

8.1.10. Deve suportar IPv4 e IPv6; N/A

8.1.10.1. Deverá permitir a configuração de endereços IPv6 para gerenciamento e

operar em modo dual stack (IPv4 e IPv6), suportando consultas de DNS com resolução de nomes em endereços IPv6;

8.1.10.2. Deverá implementar ICMPv6 com as seguintes funcionalidades: ICMP request, ICMP Reply, ICMP Neighbor Discovery Protocol (NDP), ICMP MTU Discovery.

8.1.11. Possuir porta de console com conector USB (de qualquer tipo), para acesso à interface de linha de comando. Serão aceitos adaptadores para o atendimento deste item.

8.2. Características específicas

8.2.1. Deve suportar o empilhamento físico, com cabos redundantes, de no mínimo 2 (duas) unidades do mesmo tipo;

8.2.1.1. Deverá ser permitido o gerenciamento do empilhamento através de um único IP;

8.2.2. Permitir o espelhamento do tráfego total de uma porta ou de um grupo de portas ou de uma VLAN como origem;

8.2.2.1. Deve ser possível definir o sentido do tráfego a ser espelhado (somente entrada, somente saída ou ambos);

8.2.2.2. O destino pode ser outra porta localizada no mesmo switch ou em outro switch da mesma pilha;

8.2.3. Deve utilizar mesma família de sistema operacional dos switches do item 1 e do item 5.

8.3. Quantidade de portas

8.3.1. Deve possuir pelo menos 24 (vinte e quatro) portas com conector RJ-45, que devem suportar pelo menos 5GbaseT conforme o padrão IEEE 802.3bz;

8.3.2. Deve possuir pelo menos 2 (dois) slots SFP28 com suporte a transceivers de 1/10/25 Gbps;

8.3.3. Deve possuir pelo menos 2 (duas) portas para empilhamento, cada uma com velocidade de no mínimo 100 (cem) Gbps (half-duplex) ou 200 (duzentos) Gbps (fullduplex);

8.3.3.1. O empilhamento pode ser realizado por módulo dedicado ou slots do tipo SFP ethernet disponíveis no equipamento (não podem ser consideradas as portas do item 8.3.1 nem do item 8.3.2 deste anexo para atender este requisito).

8.3.4. Deve ser possível utilizar todas as portas descritas nos itens acima de forma simultânea, ou seja, a utilização de uma porta não deve implicar a desativação ou não funcionamento de outra porta;

8.3.5. Deve ser fornecido pelo menos 1 (um) cabo para empilhamento, com comprimento de pelo menos 50 (cinquenta) centímetros.

8.3.5.1. Caso sejam utilizados slots do tipo SFP ethernet, devem ser fornecidos cabos suficientes para atender aos requisitos de velocidade dessa interface.

8.4. Gerenciamento

8.4.1. Possuir agente de gerenciamento SNMP (RFC 1157), MIB SNMP II (RFC 1213 ou suas atualizações), extensões MIB SNMP, MIB bridging (RFC 1493 ou RFC 4188), que possua descrição completa da MIB implementada no equipamento, inclusive as extensões privadas, se existirem;

8.4.2. Deve ser gerenciável via SNMP (v1, v2 e v3). Na versão v3 do SNMP devem ser implementados, pelo menos os seguintes modos de operação: Sem autenticação e sem privacidade (noAuthnoPriv), com autenticação e sem privacidade (authNpPriv) e com autenticação e com privacidade (AuthPriv). Deve suportar no mínimo os algoritmos criptográficos 3DES e AES128 no modo AuthPriv;

8.4.3. Deve permitir a transferência de arquivos através do protocolo TFTP (Trivial File Transfer Protocol) ou FTP (File Transfer Protocol) ou SFTP (SSH File Transfer Protocol);

8.4.4. Permitir a gravação de log externo (syslog). Deve ser possível definir o endereço IP de origem dos pacotes Syslog gerados pelo switch.

8.5. Capacidade

8.5.1. Deve possuir capacidade para pelo menos 32.000 (trinta e dois mil) endereços MAC na tabela de comutação;

8.5.2. Possuir uma matriz de comutação a capacidade de, no mínimo 370 (trezentos e setenta) Gbps;

8.5.2.1. Valor calculado considerando: 24 interfaces de 5 Gbps, 2 interfaces de 25 Gbps e 2 interfaces de 100 Gbps (empilhamento).

8.5.3. Possuir capacidade de encaminhamento de, no mínimo 450 (quatrocentos e cinquenta) Mpps (milhões de pacotes por segundo);

8.5.4. Deve permitir a utilização de pelo menos 1.000 (mil) SVI (Switched Virtual Interfaces) ativas de forma simultânea;

- 8.5.5. Deve permitir que todas as portas ethernet (não inclui portas de empilhamento) sejam configuradas como roteadas.
- 8.6. Protocolos e padrões suportados
- 8.6.1. Implementar VLAN segundo o padrão 802.1q;
- 8.6.2. Implementar a funcionalidade de agregação de portas, segundo o padrão 802.3ad;
- 8.6.3. Implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN;
- 8.6.4. Implementar padrão IEEE 802.1p (Class of Service) para cada porta;
- 8.6.5. Implementar padrão IEEE 802.1s (Multiple Spanning Tree);
- 8.6.6. Implementar o padrão IEEE 802.3x (Flow Control);
- 8.6.7. Implementar LLDP;
- 8.6.8. Implementar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol), incluindo autenticação entre os peers. (RFC 1305, RFC 5905);
- 8.6.9. Implementar IGMP Snooping (v1, v2 e v3).
- 8.6.10. Implementar o protocolo multicast Protocol Independent Multicast Version2 (PIMv2) em “sparse-mode”;
- 8.6.11. Protocolo VRRP (RFC 2338 ou sua substituta, RFC 3768) ou mecanismo similar de redundância de default gateway, suportando a configuração de 64 (sessenta e quatro) grupos simultaneamente;
- 8.6.12. Implementar o protocolo IGMP v2 (RFC 2236) e v3 (RFC 3376) (o tráfego não deve ser tratado como broadcast);
- 8.6.13. DHCP Relay independente por interface virtual.
- 8.7. Qualidade de Serviços (QoS)
- 8.7.1. Possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego “real-time” (voz e vídeo);
- 8.7.2. Suportar a funcionalidade de QoS “Traffic Policing”;
- 8.7.3. Deve ser possível a especificação de banda por classe de serviço;
- 8.7.4. Suporte aos mecanismos de QoS WRR (Weighted Round Robin) ou WDRR (Weighted Deficit Round Robin);
- 8.7.5. Implementar pelo menos 8 (oito) filas de prioridade por porta de saída (egress port);
- 8.7.6. Suportar classificação de QoS baseado em lista de controles de acesso com parâmetros de camada 2, 3 e 4.
- 8.8. Segurança
- 8.8.1. Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo RADIUS;
- 8.8.2. Proteger a interface de comando do equipamento através de senha;
- 8.8.3. Implementar o protocolo SSH v2 para acesso à interface de linha de comando;
- 8.8.4. Permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet e SSH. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH;
- 8.8.5. Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;
- 8.8.6. Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;
- 8.8.7. Permitir controlar quais comandos os usuários ou grupos de usuários podem emitir;
- 8.8.8. Implementar inspeção do protocolo ARP (Address Resolution Protocol) e possuir mecanismos de proteção contra ataques do tipo “ARP Poisoning”;
- 8.8.9. Promover análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC;
- 8.8.10. Possuir suporte a mecanismo de proteção da “Root Bridge” do algoritmo “Spanning-Tree” para defesa de ataques do tipo “Denial of Service” no ambiente nível 2;
- 8.8.11. Possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta do switch esteja colocada no modo “Fast Forwarding” (conforme previsto no padrão IEEE 802.1w).
- 8.8.12. Implementar filtragem de pacotes (ACL - Access Control List), com definições de parâmetros camada 2, 3 e 4;
- 8.8.13. Permitir visualização das estatísticas de filtragem das listas de controle de acesso aplicadas;
- 8.9. Roteamento
- 8.9.1. Estático;
- 8.9.2. Dinâmico, via OSPF (RFC 2328, 3101 e 2370);
- 8.9.3. Dinâmico, via BGPv4 (RFC 4271, 3065, 4456 e 1997);
- 8.9.4. De camada de rede (nível 3) entre VLANs;
- 8.9.5. Baseado em condições de origem, com possibilidade de definição de próximo salto de camada de rede;
- 8.9.6. Baseado em política (PBR - Policy-Based Routing) para IPv4 e IPv6;
- 8.9.7. OSPFv3 e BGPv6, para rotear IPv6.

item 9. Garantia estendida - switch distribuição - 5 anos - 8x5xNBD

- 9.1. O serviço de garantia terá vigência de 60 (sessenta meses);
- 9.2. O serviço de garantia estendida se caracteriza pelos serviços de:
- 9.2.1. Atualização dos softwares residentes nos equipamentos;
- 9.2.2. Suporte técnico on-site, em modelo 8X5XNBD (oito horas por dia, cinco dias na semana com resolução no próximo dia útil).
- 9.3. A garantia estendida poderá ser realizada em primeira instância pela CONTRATADA, mas deverá haver a possibilidade de escalar o serviço ao fabricante sempre que necessário;
- 9.4. Fará parte da aceitação do serviço a comprovação do registro do serviço de garantia estendida por 60 (sessenta meses);
- 9.4.1. Os níveis mínimos de serviço estabelecidos para a garantia estendida estão descritos no item 7.2 do Termo de Referência assim como o cálculo das sanções por descumprimento estão descritos no item 8.1.

item 10. Instalação switch distribuição

- 10.1. Planejamento
- 10.1.1. Deve ser executado por profissional(ais) com experiência em gerenciamento de projetos e certificação na área de roteamento/switching. Deve ser apresentado Plano de Implantação contendo pelo menos os seguintes itens:
- 10.1.1.1. Deve prever topologia lógica e física dos equipamentos envolvidos;
- 10.1.1.2. Deve prever a configuração prévia de todos os equipamentos;
- 10.1.1.3. Deve contemplar a elaboração de plano de testes;
- 10.1.1.4. Deve prever a migração de todas as VLANs, endereços IP, roteamento unicast (estático e dinâmico) e multicast (quando aplicável);
- 10.1.1.5. Deve prever a elaboração de plano de face do rack, antes e após a migração/instalação;
- 10.1.1.6. Deve prever o plano de migração (de/para) do cabeamento estruturado, incluindo posições de patch-panel e/ou DIOs;
- 10.1.1.7. Deve prever orientações e sugestões de eventuais ajustes nos equipamentos da CGU que serão integrados aos switches.
- 10.2. Migração/instalação
- 10.2.1. Deve ser executado por profissional(ais) com certificação na área de roteamento/switching;
- 10.2.2. A critério da CONTRATANTE, as etapas que envolvam risco de causar impacto no funcionamento do ambiente deve ser executada em dias e horários não úteis;
- 10.2.3. Deve prever a atualização do firmware dos equipamentos para a versão mais recente que seja considerada estável pelo fabricante;
- 10.2.4. Deve prever a remoção física dos equipamentos e cabos do sistema existente (quando for aplicável);
- 10.2.5. Deve prever a instalação física dos equipamentos e cabos do novo sistema;
- 10.2.6. Será permitida a subcontratação da instalação física dos equipamentos e organização do cabeamento;
- 10.2.7. Deve prever a execução do plano de testes.
- 10.3. As-Built
- 10.3.1. Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (as-built), etapas de execução e toda informação pertinente a posterior continuidade e manutenção da solução instalada;

item 11. Switch core

- 11.1. Características gerais e funcionalidades
- 11.1.1. Possuir pelo menos 2 (duas) fontes de alimentação internas, redundantes, do tipo AC, bivolt com seleção automática de tensão (na faixa de 100 a 240 V) e frequência (de 50/60 Hz). As fontes deverão possuir alimentação independente, a fim de permitir a sua conexão a circuitos elétricos distintos. Não será permitida a utilização de fontes externas para atender este requisito;
- 11.1.2. Deve possuir no máximo 10U (dez unidade de rack) de altura;
- 11.1.3. Permitir que seja montado em rack padrão de 19" (dezenove polegadas), incluindo todos os acessórios necessários para tal;

- 11.1.4. Possuir LEDs, por porta, que indiquem a integridade, a atividade e a velocidade de conexão do link;
- 11.1.5. Permitir o encaminhamento de "jumbo frames" em todas as portas (pacotes de 9016 bytes);
- 11.1.6. Possuir configuração de CPU e memória (RAM e Flash) suficiente para a implantação de todas as funcionalidades descritas nesta especificação;
- 11.1.7. Permitir a criação de, no mínimo, 1.000 (mil) VLANs ativas simultaneamente baseadas em portas, com suporte a no mínimo 4.000 (quatro mil) VLANs IDs;
- 11.1.8. Suportar simultaneamente em sua memória flash (ou semelhante), duas imagens do sistema operacional entregue com a solução;
- 11.1.9. Deve implementar tecnologia para monitoramento de fluxos de tráfego como, por exemplo: IPFIX (RFC 7011), Netflow (RFC 3954), Netflow Lite, sFlow (RFC 3176), Jflow, NetStream entre outros; garantindo alta visibilidade do tráfego de rede;
- 11.1.9.1. Para cada fluxo devem ser coletadas, no mínimo, as seguintes informações: endereços IP de origem/destino, portas TCP/UDP de origem/destino, interfaces de entrada e saída do tráfego, número de pacotes transmitidos;
- 11.1.10. Deve suportar IPv4 e IPv6;
- 11.1.10.1. Deverá permitir a configuração de endereços IPv6 para gerenciamento e operar em modo dual stack (IPv4 e IPv6), suportando consultas de DNS com resolução de nomes em endereços IPv6;
- 11.1.10.2. Deverá implementar ICMPv6 com as seguintes funcionalidades: ICMP request, ICMP Reply, ICMP Neighbor Discovery Protocol (NDP), ICMP MTU Discovery.
- 11.1.11. Possuir porta de console com conector USB (de qualquer tipo), para acesso à interface de linha de comando. Serão aceitos adaptadores para o atendimento deste item.
- 11.2. Características específicas
- 11.2.1. Deve suportar o empilhamento físico, com cabos redundantes, de no mínimo 2 (duas) unidades do mesmo tipo;
- 11.2.2. Deverá ser permitido o gerenciamento do empilhamento através de um único IP;
- 11.2.3. Permitir o espelhamento do tráfego total de uma porta ou de um grupo de portas ou de uma VLAN como origem;
- 11.2.3.1. Deve ser possível definir o sentido do tráfego a ser espelhado (somente entrada, somente saída ou ambos);
- 11.2.3.2. O destino pode ser outra porta localizada no mesmo switch ou em outro switch da mesma pilha;
- 11.2.4. Deve utilizar mesma família de sistema operacional dos switches do item 1, do item 5 e do item 8.
- 11.3. Quantidade de portas
- 11.3.1. Deve possuir pelo menos 24 (vinte e quatro) slots SFP28 com suporte a transceivers de 10/25 Gbps;
- 11.3.2. Deve possuir pelo menos 2 (duas) portas para empilhamento, cada uma com velocidade de no mínimo 100 (cem) Gbps (half-duplex) ou 200 (duzentos) Gbps (full-duplex);
- 11.3.2.1. O empilhamento pode ser realizado por módulo dedicado ou slots do tipo SFP ethernet disponíveis no equipamento (não podem ser consideradas as portas do item 11.3.1, deste anexo, para atender este requisito).
- 11.3.2.2. Caso sejam utilizados slots do tipo SFP ethernet, será permitida a utilização de múltiplas interfaces para atender o requisito de throughput solicitado.
- 11.3.3. Deve ser possível utilizar todas as portas descritas nos itens acima de forma simultânea, ou seja, a utilização de uma porta não deve implicar a desativação ou não funcionamento de outra porta;
- 11.3.4. Deve ser fornecido pelo menos 1 (um) cabo para empilhamento, com comprimento de pelo menos 50 (cinquenta) centímetros.
- 11.3.4.1. Caso sejam utilizados slots do tipo SFP ethernet, devem ser fornecidos cabos suficientes para atender aos requisitos de velocidade da interface de empilhamento.
- 11.4. Gerenciamento
- 11.4.1. Possuir agente de gerenciamento SNMP (RFC 1157), MIB SNMP II (RFC 1213 ou suas atualizações), extensões MIB SNMP, MIB bridging (RFC 1493 ou RFC 4188), que possua descrição completa da MIB implementada no equipamento, inclusive as extensões privadas, se existirem;
- 11.4.2. Deve ser gerenciável via SNMP (v1, v2 e v3). Na versão v3 do SNMP devem ser implementados, pelo menos os seguintes modos de operação: Sem autenticação e sem privacidade (noAuthNoPriv), com autenticação e sem privacidade (authNoPriv) e com autenticação e com privacidade (AuthPriv). Deve suportar no mínimo os algoritmos criptográficos 3DES e AES128 no modo AuthPriv;
- 11.4.3. Deve permitir a transferência de arquivos através do protocolo TFTP (Trivial File Transfer Protocol) ou FTP (File Transfer Protocol) ou SFTP (SSH File Transfer Protocol);
- 11.4.4. Permitir a gravação de log externo (syslog). Deve ser possível definir o endereço IP de origem dos pacotes Syslog gerados pelo switch.
- 11.5. Capacidade
- 11.5.1. Deve possuir capacidade para pelo menos 32.000 (trinta e dois mil) endereços MAC na tabela de comutação;
- 11.5.2. Possuir uma matriz de comutação a capacidade de, no mínimo 800 (oitocentos) Gbps;
- 11.5.2.1. • Valor calculado considerando: 24 interfaces de 25 Gbps e 2 interfaces de 100 Gbps (empilhamento).
- 11.5.3. Possuir capacidade de encaminhamento de, no mínimo 1.488 (mil quatrocentos e oitenta e oito) Mpps (milhões de pacotes por segundo);
- 11.5.4. Deve permitir a utilização de pelo menos 1.000 (mil) SVI (Switched Virtual Interfaces) ativas de forma simultânea;
- 11.5.5. Deve permitir que todas as portas ethernet (não inclui portas de empilhamento) sejam configuradas como roteadas.
- 11.6. Protocolos e padrões suportados
- 11.6.1. Implementar VLAN segundo o padrão 802.1q;
- 11.6.2. Implementar a funcionalidade de agregação de portas, segundo o padrão 802.3ad;
- 11.6.3. Implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN;
- 11.6.4. Implementar padrão IEEE 802.1p (Class of Service) para cada porta;
- 11.6.5. Implementar padrão IEEE 802.1s (Multiple Spanning Tree);
- 11.6.6. Implementar o padrão IEEE 802.3x (Flow Control);
- 11.6.7. Implementar LLDP;
- 11.6.8. Implementar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol), incluindo autenticação entre os peers. (RFC 1305, RFC 5905);
- 11.6.9. Implementar IGMP Snooping (v1, v2 e v3).
- 11.6.10. Implementar o protocolo multicast Protocol Independent Multicast Version2 (PIMv2) em "sparse-mode";
- 11.6.11. Protocolo VRRP (RFC 2338 ou sua substituta, RFC 3768) ou mecanismo similar de redundância de default gateway, suportando a configuração de 255 (duzentos e cinquenta e cinco) grupos simultaneamente;
- 11.6.12. Implementar o protocolo IGMP v2 (RFC 2236) e v3 (RFC 3376) (o tráfego não deve ser tratado como broadcast);
- 11.6.13. DHCP Relay independente por interface virtual.
- 11.7. Qualidade de Serviços (QoS) N/A
- 11.7.1. Possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego "real-time" (voz e vídeo);
- 11.7.2. Suportar a funcionalidade de QoS "Traffic Policing";
- 11.7.3. Deve ser possível a especificação de banda por classe de serviço;
- 11.7.4. Suporte aos mecanismos de QoS WRR (Weighted Round Robin) ou WDRR (Weighted Deficit Round Robin);
- 11.7.5. Implementar pelo menos 8 (oito) filas de prioridade por porta de saída (egress port);
- 11.7.6. Suportar classificação de QoS baseado em lista de controles de acesso com parâmetros de camada 2, 3 e 4.
- 11.7.7. Qualidade de Serviços (QoS)
- 11.8. Segurança
- 11.8.1. Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo RADIUS;
- 11.8.2. Proteger a interface de comando do equipamento através de senha;
- 11.8.3. Implementar o protocolo SSH v2 para acesso à interface de linha de comando;
- 11.8.4. Permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet e SSH. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH;
- 11.8.5. Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;
- 11.8.6. Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;
- 11.8.7. Permitir controlar quais comandos os usuários ou grupos de usuários podem emitir;
- 11.8.8. Implementar inspeção do protocolo ARP (Address Resolution Protocol) e possuir mecanismos de proteção contra ataques do tipo "ARP Poisoning";
- 11.8.9. Promover análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC;
- 11.8.10. Possuir suporte a mecanismo de proteção da "Root Bridge" do algoritmo "Spanning-Tree" para defesa de ataques do tipo "Denial of Service" no ambiente nível 2;
- 11.8.11. Possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta do switch esteja colocada no modo "Fast Forwarding" (conforme previsto no padrão IEEE 802.1w).
- 11.8.12. Implementar filtragem de pacotes (ACL - Access Control List), com definições de parâmetros camada 2, 3 e 4;
- 11.8.13. Permitir visualização das estatísticas de filtragem das listas de controle de acesso aplicadas;
- 11.9. Roteamento
- 11.9.1. Estático;

- 11.9.2. Dinâmico, via OSPF (RFC 2328, 3101 e 2370);
- 11.9.3. Dinâmico, via BGPv4 (RFC 4271, 3065, 4456 e 1997);
- 11.9.4. De camada de rede (nível 3) entre VLANs;
- 11.9.5. Baseado em condições de origem, com possibilidade de definição de próximo salto de camada de rede;
- 11.9.6. Baseado em política (PBR - Policy-Based Routing) para IPv4 e IPv6;
- 11.9.7. OSPFv3 e BGPv6, para rotear IPv6.

item 12. Garantia estendida - switch core - 5 anos - 24x7x4

- 12.1. O serviço de garantia terá vigência de 60 (sessenta meses);
- 12.2. O serviço de garantia estendida se caracteriza pelos serviços de:
 - 12.2.1. Atualização dos softwares residentes nos equipamentos;
 - 12.2.2. Suporte técnico on-site, em modelo 24x7x4 (vinte e quatro horas por dia, sete dias na semana com resolução em quatro horas);
- 12.3. A garantia estendida poderá ser realizada em primeira instância pela CONTRATADA, mas deverá haver a possibilidade de escalar o serviço ao fabricante sempre que necessário;
- 12.4. Fará parte da aceitação do serviço a comprovação do registro do serviço de garantia estendida por 60 (sessenta meses);
 - 12.4.1. Os níveis mínimos de serviço estabelecidos para a garantia estendida estão descritos no item 7.2 do Termo de Referência assim como o cálculo das sanções por descumprimento estão descritos no item 8.1.

item 13. Instalação switch core

- 13.1. Planejamento
 - 13.1.1. Deve ser executado por profissional(ais) com experiência em gerenciamento de projetos e certificação na área de roteamento/switching. Deve ser apresentado Plano de Implantação contendo pelo menos os seguintes itens:
 - 13.1.1.1. Deve prever topologia lógica e física dos equipamentos envolvidos;
 - 13.1.1.2. Deve prever a configuração prévia de todos os equipamentos;
 - 13.1.1.3. Deve contemplar a elaboração de plano de testes;
 - 13.1.1.4. Deve prever a migração de todas as VLANs, endereços IP, roteamento unicast (estático e dinâmico) e multicast (quando aplicável);
 - 13.1.1.5. Deve prever a elaboração de plano de face do rack, antes e após a migração/instalação;
 - 13.1.1.6. Deve prever o plano de migração (de/para) do cabeamento estruturado, incluindo posições de patch-panel e/ou DIOs;
 - 13.1.1.7. Deve prever orientações e sugestões de eventuais ajustes nos equipamentos da CGU que serão integrados aos switches.
 - 13.2. Migração/instalação
 - 13.2.1. Deve ser executado por profissional(ais) com certificação na área de roteamento/switching;
 - 13.2.2. A critério da CONTRATANTE, as etapas que envolvam risco de causar impacto no funcionamento do ambiente deve ser executada em dias e horários não úteis;
 - 13.2.3. Deve prever a atualização do firmware dos equipamentos para a versão mais recente que seja considerada estável pelo fabricante;
 - 13.2.4. Deve prever a remoção física dos equipamentos e cabos do sistema existente (quando for aplicável);
 - 13.2.5. Deve prever a instalação física dos equipamentos e cabos do novo sistema;
 - 13.2.6. Será permitida a subcontratação da instalação física dos equipamentos e organização do cabeamento;
 - 13.2.7. Deve prever a execução do plano de testes.
 - 13.3. As-Built
 - 13.3.1. Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (as-built), etapas de execução e toda informação pertinente a posterior continuidade e manutenção da solução instalada;

item 14. SFP28 25GBase-SR

- 14.1. Transceiver SFP28 para conexão de fibras ópticas;
- 14.2. Deve ser compatível com o padrão 25GBase-SR para fibras multimodo;
- 14.3. Deve possuir conector LC;
- 14.4. Velocidade de 25 Gbps;
- 14.5. Deve ser compatível com os equipamentos dos itens 8 e 11.

item 15. SFP 1000BaseT

- 15.1. Transceiver SFP para conexão de cabos de par metálico;
- 15.2. Deve ser compatível com o padrão 1000Base-T (802.3ab) para cabos UTP;
- 15.3. Deve possuir conector RJ-45;
- 15.4. Velocidade de 1 Gbps;
- 15.5. Deve ser compatível com os equipamentos dos itens 1, 5, 8 e 11.

item 16. SFP 1000BaseSX

- 16.1. Transceiver SFP para conexão de fibras ópticas;
- 16.2. Deve ser compatível com o padrão 1000Base-SX para fibras multimodo;
- 16.3. Deve possuir conector LC;
- 16.4. Velocidade de 1 Gbps;
- 16.5. Deve ser compatível com os equipamentos dos itens 1, 5, 8 e 11.

item 17. SFP+ 10GBaseSR

- 17.1. Transceiver SFP+ para conexão de fibras ópticas;
- 17.2. Deve ser compatível com o padrão 10GBase-SR para fibras multimodo;
- 17.3. Deve possuir conector LC;
- 17.4. Velocidade de 10 Gbps;
- 17.5. Deve ser compatível com os equipamentos dos itens 1, 5, 8 e 11.

item 18. Software NAC - 5000 dispositivos - 5 anos - 24x7x4

- 18.1. Características gerais
 - 18.1.1. Não serão aceitos sistemas baseados em software de código aberto (open source) de uso genérico;
 - 18.1.2. A solução deve ser composta pelo Sistema de Gerenciamento Centralizado e Sistema de Controle de Acesso;
 - 18.1.3. A solução deverá ser fornecida na forma Appliance Virtual ou software sendo executado em sistemas operacionais Windows Server ou Centos:
 - 18.1.3.1. A solução pode ser executada no ambiente virtualizado da CONTRATANTE;
 - 18.1.3.2. Caso a solução seja fornecida na forma de Appliance Virtual, as máquinas virtuais devem ser compatíveis com Vmware ESXi versão 6.7 ou superior;
 - 18.1.3.3. Caso a solução seja fornecida em máquinas virtuais Windows Server, não é necessário fornecer licenças para o referido sistema operacional. As versões permitidas do Windows Server são 2016 e 2019;
 - 18.1.3.4. Caso a solução seja fornecida em máquinas virtuais Centos, esta deve ser compatível com a versão 7 ou superior;
 - 18.1.4. Caso os requisitos acima não sejam atendidos deve ser previsto por conta da CONTRATADA o fornecimento de hardware redundante para o funcionamento da solução;
 - 18.1.5. O software de NAC deve ser do mesmo fabricante da solução de rede ofertado nos demais itens deste Termo de Referência. Também será aceito software de NAC de empresas que possuam acordo formal de interoperabilidade que garanta a operação e evolução conjunta dos componentes da solução;
 - 18.1.6. Serão admitidas soluções que possuam banco de dados proprietários, desde que estejam instalados em Appliances Virtuais;
 - 18.1.7. Todos os componentes que farão parte da estrutura da solução, deverão suportar redundância em um conjunto de, no mínimo, 02 (dois) componentes;
 - 18.1.8. No caso de falha de um dos componentes do conjunto, o outro deve ser capaz de assumir todas as operações e funcionalidades de forma automática e sem interrupção dos serviços. Não serão aceitos sistemas que operem em redundância manual;
 - 18.1.9. Os componentes devem possuir contas administrativas que permitam a segregação de funções de monitoramento e administração;
 - 18.1.9.1. A solução deverá ter capacidade de segregação de perfis de acesso, permitindo diferentes níveis de acesso à console de gerenciamento, em que cada perfil possa ter permissões específicas associadas à sua função;
 - 18.1.9.2. Todos os acessos administrativos devem ser autenticados e criptografados.
- 18.2. Console de Gerenciamento N/A
 - 18.2.1. A solução deverá ser administrável remotamente por meio de interface gráfica (GUI) web, utilizando HTTPS;
 - 18.2.2. A solução deverá conter mecanismo de comunicação em tempo real entre servidor e clientes, para entrega de configurações e políticas;

- 18.2.3. A solução deve ser capaz de admitir integração com MS-AD (Microsoft Active Directory) para login único de usuário (Single Sign On = SSO);
- 18.2.4. Deve permitir aplicar regras diferenciadas com base em grupos de usuários e grupos de máquinas;
- 18.2.5. Capacidade de criação de contas de usuário com, pelo menos, 03 (três) diferentes níveis de acesso com perfis que permitam: administração, auditoria e operação;
- 18.2.6. Todos os registros de logs da solução devem ser compatíveis com o padrão syslog, e enviados para pelo menos 2 (dois) servidores de log, atendendo, no mínimo, uma das seguintes RFCs: RFC 3164, RFC 5424 ou RFC 5426;
- 18.2.7. Suportar execução manual e/ou programada de backup das configurações e da base de dados;
- 18.2.8. Possuir recursos nativos (próprios da solução) para a replicação do banco de dados entre os servidores de gerenciamento;
- 18.2.9. Em caso de contingência operacional (caso algum dos componentes centrais da solução venha a falhar), a parte restante da solução deverá assumir o processamento do(s) componente(s) afetado(s) em 100% (cem por cento) sem perda de desempenho;
- 18.2.10. Trabalhar com, pelo menos, 02 (dois) nós em alta disponibilidade. Caso solicitado pela CONTRATANTE, deve ser permitido que os nós estejam localizados em regiões geograficamente distintas e em sub-redes diferentes;
- 18.2.11. Permitir o gerenciamento e configuração centralizada de todos os componentes da solução;
- 18.2.12. Suportar o sincronismo de tempo via NTP (Network Time Protocol).
- 18.3. Solução de Gerenciamento de Equipamentos N/A
- 18.3.1. Ter conformidade com a IEEE 802.1X, SNMP v2 e SNMP v3 e Change of Authorization –COA;
- 18.3.2. Alterar configurações nos switches de forma remota e centralizada, realizando mudança de VLAN/VXLAN e ACL de acordo com a política definida, com ou sem o uso de 802.1x;
- 18.3.3. Receber eventos SNMP passivo (recebimento de traps) e executar consultas ativas de SNMP (pela leitura de MIBs em TCP e/ou UDP);
- 18.3.4. A solução deve possuir mecanismo de detecção de comportamento de dispositivo, ou seja, avaliar as comunicações dos diversos dispositivos.
- 18.3.5. Autenticar e autorizar usuários administrativos por meio dos protocolos LDAP e/ou TACACS+ e/ou similar.
- 18.3.6. A funcionalidade de controle de acesso deve ser implementada sem o uso de agentes;
- 18.3.7. A ferramenta deve ser capaz de identificar dispositivos de modo automatizado e suportar no mínimo as seguintes técnicas para identificação:
- 18.3.7.1. HTTP User-Agent (via Port Mirror e Redirect);
- 18.3.7.2. MAC OUI;
- 18.3.7.3. DHCP (via DHCP Relay);
- 18.3.7.4. Radius;
- 18.3.7.5. Receber eventos SNMP passivo (recebimento de traps) e executar consultas ativas de SNMP (pela leitura de MIBs em TCP e/ou UDP);
- 18.3.7.6. Scan de Rede (via NMAP);
- 18.3.8. A solução deve ser capaz de efetuar a autenticação dos endpoints com qualquer certificado em conformidade com o padrão X.509 ou PEM.
- 18.3.9. A solução deve ser capaz de validar o certificado em uma pki interna e/ou Active Directory.
- 18.3.10. A solução deve suportar busca em Lista de Certificados Revogados (LCR) por meio de HTTP, OCSP ou LDAP.
- 18.4. Controle básico de acesso a rede
- 18.4.1. Implementar o bloqueio de acesso à rede, das máquinas que não estiverem em conformidade com as políticas do controle de acesso.
- 18.4.2. Suportar protocolo EAP e PEAP.
- 18.4.3. Permitir a recepção de requisições DHCP.
- 18.4.4. A solução deverá efetuar as verificações de conformidade das máquinas que acessem a rede corporativa de forma a permitir, bloquear ou redirecionar as conexões de acordo com as políticas de segurança implementadas. As verificações de que tratam este item estão relacionadas ao controle de acesso.
- 18.4.5. A solução deverá permitir a criação de políticas com base em grupos do MS-AD (Microsoft Active Directory). A solução deve permitir a leitura de grupos dentro de grupos, até identificar objetos finais com pelos menos 3 (três) níveis;
- 18.5. Relatórios e Monitoramento
- 18.5.1. A solução deverá oferecer alertas na console de gerência e enviar via SMTP/e-mail;
- 18.5.2. A solução deverá possibilitar aos administradores do sistema a geração de relatórios customizados exportáveis nos formatos PDF, CSV e/ou TXT;
- 18.5.3. A solução deverá fornecer funcionalidades de relatórios gráficos, incluindo:
- 18.5.3.1. Tipos de dispositivos;
- 18.5.3.2. FABRICANTE do dispositivo;
- 18.5.3.3. Sistema Operacional;
- 18.5.3.4. Endereço IP associado;
- 18.5.3.5. Informação detalhada dos usuários;
- 18.5.3.6. Políticas em uso;
- 18.5.3.7. Regras de Controle de Acesso.
- 18.5.4. A solução deverá gerar e armazenar trilhas de auditoria que permitam o rastreamento de ações efetuadas em todos os seus componentes. Os registros de logs devem conter a identificação do evento, data e hora, identificação do usuário e endereço IP do dispositivo;
- 18.5.5. Centralizar os logs dos componentes da solução em um único ponto, ou permitir a exportação dos logs via syslog.
- 18.5.6. Possuir ferramenta para acompanhamento de eventos e estatística de logs.
- 18.5.6.1. Os acessos à administração e configuração, bem como as alterações realizadas durante o acesso, devem ser registrados em log, informando no mínimo: hora, data, IP de origem e usuário.
- 18.6. Licenças, Garantia Estendida e Direito de Atualização
- 18.6.1. O licenciamento deve ser de uso permanente/perpétuo, com garantia estendida por 60 (sessenta meses);
- 18.6.1.1. O termo permanente/perpétuo indica que o software não poderá parar de funcionar ou limitar o uso de suas funcionalidades após finalizada a garantia estendida;
- 18.6.2. O serviço Garantia Estendida e Direito de Atualização se caracteriza pelos serviços de:
- 18.6.2.1. Atualização do(s) software(s) desde que não haja mudança de licenças;
- 18.6.2.2. Suporte técnico on-site, em modelo 24x7x4 (vinte e quatro horas por dia, sete dias na semana com resolução em quatro horas);
- 18.6.3. Após avaliações realizadas após a emissão do ETP, optou-se pelo aumento da abrangência do suporte para o período de 24x7x4, tendo em vista os possíveis impactos no acesso à infraestrutura de rede em caso de mal funcionamento desta solução.
- 18.6.4. A garantia estendida poderá ser realizada em primeira instância pela CONTRATADA, mas deverá haver a possibilidade de escalar o serviço ao fabricante sempre que necessário;
- 18.6.5. Fará parte da aceitação do serviço a comprovação do registro da garantia estendida por 60 (sessenta meses) junto ao fabricante;
- 18.6.6. Os níveis mínimos de serviço estabelecidos para a garantia estendida estão descritos no item 7.2 do Termo de Referência assim como o cálculo das sanções por descumprimento estão descritos no item 8.1.
- 18.6.7. O licenciamento deve-se realizar de forma global. Todos os appliances/software consomem licenças de um servidor centralizado;
- 18.6.8. A licença será contabilizada por dispositivo, independentemente do modo de acesso. Exemplo: BYOD, Guest, Suplicante 802.1x, MAC etc.
- 18.6.8.1. Caso o fabricante ofereça licenças diferenciadas conforme o tipo de dispositivo, devem ser oferecidas pelo menos 1.000 (mil) licenças BYOD, pelo menos 1.000 (mil) licenças Guest e pelo menos 5.000 (cinco mil) licenças para os demais métodos de autenticação.

item 19. Instalação software NAC - 5000 dispositivos

- 19.1. Planejamento
- 19.1.1. Deve ser executado por profissional(ais) com experiência em gerenciamento de projetos e certificação na área de roteamento/switching. Deve ser apresentado Plano de Implantação contendo pelo menos os seguintes itens:
- 19.1.2. Deve prever topologia lógica dos softwares envolvidos;
- 19.1.3. Deve prever a configuração prévia de todos os softwares;
- 19.1.4. Deve contemplar a elaboração de plano de testes;
- 19.2. Instalação
- 19.2.1. Deve ser executado por profissional(ais) com certificação na área de roteamento/switching;
- 19.2.2. A critério da CONTRATANTE, as etapas que envolvam risco de causar impacto no funcionamento do ambiente deve ser executada em dias e horários não úteis;
- 19.2.3. Deve prever a execução do plano de testes.
- 19.3. As-Built
- 19.3.1. Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (as-built), etapas de execução e toda informação pertinente a posterior continuidade e manutenção da solução instalada;

item 20. Software de Gerenciamento/Administração/Orquestração da Rede - 5 anos - 8x5xNBD

- 20.1. Características gerais
- 20.1.1. A prestação do serviço consiste na disponibilização ser sistema que seja capaz de gerenciar/administrar/orquestrar os switches LAN desta especificação técnica (itens 1,

- 5, 8 e 11)
- 20.1.2. Deve incluir a disponibilização de software que deverá ser do mesmo fabricante dos switches;
- 20.1.3. Será permitido o atendimento deste item com a utilização de mais de um software;
- 20.1.4. Devem prever por conta da CONTRATADA as licenças para os dispositivos previstos nesta especificação técnica. Poderão ser utilizadas licenças de cada dispositivo sejam previstas nos itens de cada equipamento;
- 20.1.5. A solução poderá ser fornecida na forma Appliance Virtual ou software sendo executado em sistemas operacionais Windows Server ou Centos:
- 20.1.5.1. Nestes casos, o serviço pode ser executado no ambiente virtualizado da CONTRATANTE;
- 20.1.5.2. Caso o serviço seja fornecido na forma de Appliance Virtual, as máquinas virtuais devem ser compatíveis com Vmware ESXi versão 6.7 ou superior;
- 20.1.5.3. Caso o serviço seja fornecido em máquinas virtuais Windows Server, não é necessário fornecer licenças para o referido sistema operacional. As versões permitidas do Windows Server são 2016 e 2019;
- 20.1.5.4. Caso o serviço seja fornecido em máquinas virtuais Centos, esta deve ser compatível com a versão 7 ou superior;
- 20.1.6. Caso os requisitos acima não sejam atendidos ou a solução exija o uso de hardware dedicado, deve ser previsto por conta da CONTRATADA o fornecimento de hardware redundante para o funcionamento da solução;
- 20.1.7. Deve possuir interface web acessível via HTTPS;
- 20.1.8. Disponibilizar os relatórios fornecidos/gerados via interface gráfica;
- 20.1.9. Deve incluir todas as licenças de softwares auxiliares como sistemas operacionais e bancos de dados (quando aplicável);
- 20.2. Requisitos específicos
- 20.2.1. Deve funcionar como coletor para monitoramento de fluxos de tráfego como, por exemplo: IPFIX (RFC 7011), Netflow (RFC 3954), Netflow Lite, sFlow (RFC 3176), Jflow, NetStream entre outros; garantindo alta visibilidade do tráfego de rede;
- 20.2.2. Possibilitar o gerenciamento de inventário da rede, permitindo o armazenamento de várias cópias das configurações dos dispositivos e oferecendo, inclusive, opções para comparar configurações de diferentes datas para visualizar alterações realizadas;
- 20.2.3. Implementar mecanismos de Zero Touch Provisioning para descoberta automática e provisionamento de novos elementos de rede.
- 20.2.3.1. Este mesmo recurso também deve permitir a substituição de equipamentos defeituosos sem necessidade de configuração prévia do novo dispositivo;
- 20.2.3.2. O provisionamento dos equipamentos deverá ocorrer com processo que garanta a autenticidade do novo equipamento. Deverá estar previsto um acesso inicial seguro com suporte a chaves assimétricas e/ou certificados assinados;
- 20.2.4. Permitir a exibição da topologia da rede; a descoberta dos equipamentos (e suas interligações) deve ser feita obrigatoriamente de forma automática, permitindo também sua configuração/personalização manual;
- 20.2.5. Exibir as representações gráficas dos equipamentos, mostrando o estado operacional das portas, permitindo inclusive a configuração e monitoramento em tempo real;
- 20.2.6. Permitir a configuração de diferentes perfis de usuários, tornando possível a criação de perfis administrativos e de perfis operacionais (visualização);
- 20.2.7. Prover detecção de falhas em tempo real, além de oferecer relatórios e regras de tratamento de alarmes pré-configuradas para ações de intervenção;
- 20.2.8. Permitir a monitoração do estado das portas, realizando a intervenção de ativação e suspensão da porta na rede;
- 20.2.9. Possuir mecanismo de detecção de problemas de encaminhamento e/ou perdas de pacotes, permitindo, assim, uma rápida análise da situação e um isolamento dos problemas de conectividade. Deve permitir o monitoramento de um fluxo de uma determinada comunicação informando se houver perda de pacotes em algum ponto do caminho desde a origem até o destino;
- 20.2.10. Deve permitir a definição de localização física (endereço) dos sítios onde os equipamentos serão instalados;
- 20.2.11. Possibilitar carregar planta baixa ou imagem de fundo, além de cadastrar andares para sítios com mais de um pavimento;
- 20.2.12. Possuir repositório de imagem de software de todos os componentes de rede centralizado;
- 20.2.13. Deverá se integrar totalmente ao sistema de NAC, especialmente para as definições de segmentação (essas funcionalidades podem ser atendidas pela ferramenta de NAC);
- 20.2.13.1. A funcionalidade de segmentação deve permitir definir as regras de acesso entre os diferentes perfis (nos dois sentidos);
- 20.2.13.2. Deve ser possível definir as regras de acesso entre um determinado perfil e o ambiente externo ao fabric (no caso das redes SD-LAN) (nos dois sentidos);
- 20.2.13.3. Deve ser permitido criar regras de acesso com base em portas TCP e UDP;
- 20.2.13.4. Dever ser permitido criar perfis de usuário com base em grupos do AD e com base em endereço da rede.
- 20.2.14. Deverá possuir um dashboard específico para monitoramento dos equipamentos de cliente (essas funcionalidades podem ser atendidas pela ferramenta de NAC);
- 20.2.14.1. Visualização de tempo de conexão dos clientes;
- 20.2.14.2. Pelos menos as seguintes informações dos clientes (usuário, endereço IP e taxa de utilização para transmissão/recepção (TX/RX)). O usuário precisar ser fornecido apenas quando se tratar de uma estação de trabalho;
- 20.2.15. Possibilitar a configuração e a visualização dos parâmetros de camada de rede (nível 3), como endereços IPv4 e IPv6 e redundância de roteamento (VRRP ou similar);
- 20.2.16. Possibilitar o gerenciamento de inventário da rede, permitindo o armazenamento de várias cópias das configurações dos dispositivos e oferecendo, inclusive, opções para comparar configurações de diferentes datas para visualizar alterações realizadas;
- 20.2.17. Todo gerenciamento do software dos equipamentos deve ser provido pelo Sistema de Gerenciamento. O software deve ser capaz de realizar o upgrade de software nos equipamentos fornecidos;
- 20.2.18. Deve permitir a administração da solução de SD-LAN e da LAN.
- 20.3. Licenças, Garantia Estendida e Direito de Atualização
- 20.3.1. O licenciamento deve ser de uso permanente/perpétuo, com garantia estendida por 60 (sessenta meses);
- 20.3.1.1. O termo permanente/perpétuo indica que o software não poderá parar de funcionar ou limitar o uso de suas funcionalidades após finalizada a garantia estendida;
- 20.3.2. O serviço Garantia Estendida e Direito de Atualização se caracteriza pelos serviços de:
- 20.3.2.1. Atualização do(s) software(s) desde que não haja mudança de licenças;
- 20.3.2.2. Suporte técnico on-site, em modelo 8X5XNBD (oito horas por dia, cinco dias na semana com resolução no próximo dia útil).
- 20.3.3. A garantia estendida poderá ser realizada em primeira instância pela CONTRATADA, mas deverá haver a possibilidade de escalar o serviço ao fabricante sempre que necessário;
- 20.3.4. Fará parte da aceitação do serviço a comprovação do registro da garantia estendida por 60 (sessenta meses) junto ao fabricante;
- 20.3.5. Os níveis mínimos de serviço estabelecidos para a garantia estendida estão descritos no item 7.2 do Termo de Referência assim como o cálculo das sanções por descumprimento estão descritos no item 8.1.

item 21. Instalação software de gerência/administração/orquestração

- 21.1. Planejamento
- 21.1.1. Deve ser executado por profissional(ais) com experiência em gerenciamento de projetos e certificação na área de roteamento/switching. Deve ser apresentado Plano de Implantação contendo pelo menos os seguintes itens:
- 21.1.2. Deve prever topologia lógica dos softwares envolvidos;
- 21.1.3. Deve prever a configuração prévia de todos os softwares;
- 21.1.4. Deve contemplar a elaboração de plano de testes;
- 21.2. Instalação
- 21.2.1. Deve ser executado por profissional(ais) com certificação na área de roteamento/switching;
- 21.2.2. A critério da CONTRATANTE, as etapas que envolvam risco de causar impacto no funcionamento do ambiente deve ser executada em dias e horários não úteis;
- 21.2.3. Deve prever a execução do plano de testes.
- 21.3. As-Built
- 21.3.1. Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (as-built), etapas de execução e toda informação pertinente a posterior continuidade e manutenção da solução instalada;

item 22. Repasse de conhecimento

- 22.1. Características gerais
- 22.1.1. O serviço de transferência deve consistir na oferta de curso presencial, em Brasília/DF, com abordagem prática voltada a todos os requisitos funcionais da solução contratada;
- 22.1.2. Os serviços se realização de forma presencial em Brasília-DF; N/A
- 22.1.3. A turma será composta por 06 (seis) alunos oficiais, mais 2 (dois) alunos na condição de ouvintes;
- 22.1.4. Os locais de realização das aulas serão providos pela CONTRATADA; N/A
- 22.1.5. O material didático, meios audiovisuais e estrutura de TI necessária para realização do curso serão providos pela CONTRATADA;
- 22.1.6. O curso será ministrado em língua portuguesa;
- 22.1.7. Deverá utilizar a infraestrutura física de responsabilidade da CONTRATADA e deverá ser do tipo hands-on;
- 22.1.8. Deve empregar laboratório (que pode ser físico ou virtual) com pelo menos 1 (um) POD por aluno. O laboratório deve utilizar equipamentos do mesmo fabricante, com as mesmas funcionalidades e interface/sintaxe dos utilizados para atender aos itens 1, 5, 8 e 11.

- 22.1.9. O processo de transferência de conhecimentos deverá ser ministrado por instrutor(es) com conhecimento sobre a solução, de forma a garantir que todos os requisitos necessários para operação, gerência e manutenção da solução sejam ministrados com a carga horária adequada;
- 22.1.10. A carga horária mínima do curso deve ser de 60 (sessenta) horas, que devem ministradas em dia úteis e durante apenas um dos períodos do dia. Deste modo, o curso deve ter a duração de 15 (quinze) dias úteis consecutivos;
- 22.1.11. Ao término do processo de transferência de conhecimentos, a CONTRATADA deverá realizar uma avaliação de satisfação em relação ao curso, como conteúdo, instalações, material didático e de aplicação à prática profissional, bem como do(s) instrutor(es). Esta avaliação utilizará o modelo constante do Anexo 6. Caso o curso seja considerado insatisfatório, a CONTRATADA deverá realizar um novo processo de transferência de conhecimentos, com a finalidade de atender as demandas não supridas inicialmente. Um relatório contendo a avaliação de satisfação dos alunos deverá ser enviado a CONTRATANTE;
- 22.1.12. A CONTRATANTE não assumirá os custos de licenças e/ou softwares extras, diárias e transporte dos instrutores, assim como outros custos relativos a esta capacitação. Todos os custos devem ser previstos pela CONTRATADA da solução na elaboração de suas propostas;
- 22.1.13. Não serão de responsabilidade da CONTRATADA os custos de transporte e diárias dos participantes da CONTRATANTE.
- 22.1.14. Excepcionalmente, e à conveniência da CONTRATANTE, o repasse de conhecimento poderá ser realizado de forma remota. Neste caso, toda a infraestrutura necessária para replicar o ambiente de treinamento em ambiente virtual será de responsabilidade da CONTRATADA.
- 22.2. Tópicos mínimo a serem abordados
- 22.2.1. Empilhamento de switches;
- 22.2.2. Configuração de VLANs nos switches;
- 22.2.3. Configuração de interfaces físicas, virtuais, L2 (acesso e trunk) e L3 nos switches;
- 22.2.4. Boas práticas de segurança em portas de acesso nos switches;
- 22.2.5. Roteamento estático e OSPF nos switches;
- 22.2.6. Listas de controle de acesso nos switches;
- 22.2.7. Configuração de VRRP nos switches LAN;
- 22.2.8. Configuração de NTP, syslog, LLDP, DHCP Relay, SNMPv2 nos switches;
- 22.2.9. Configuração de espelhamento de portas nos switches;
- 22.2.10. Configurar tecnologia para monitoramento de fluxos de tráfego;
- 22.2.11. Configuração de PIM e IGMP nos switches;
- 22.2.12. Configuração de jumbo frames nos switches;
- 22.2.13. Configuração do acesso via SSH e utilizando AAA nos switches;
- 22.2.14. Realização das seguintes operações pelo software de gerência:
- 22.2.14.1. Adicionar um switch existente ao software gerência;
- 22.2.14.2. Substituir um switch utilizando o mecanismo de Zero Touch Provisioning;
- 22.2.14.3. Alterar a configuração de um switch LAN;
- 22.2.14.4. Verificar a saúde de um equipamento;
- 22.2.14.5. Verificar o histórico de alterações das configurações de um equipamento;
- 22.2.14.6. Criação de um template com as configurações mínimas que devem ser aplicadas a um conjunto de equipamentos. Aplicação do template e validação de que as funcionalidades são aplicadas/conferidas em todos os equipamentos do grupo selecionado;
- 22.2.14.7. Verificação do status de um cliente;
- 22.2.14.8. Criação de um mapa mostrando as conexões entre os equipamentos.
- 22.2.15. NAC
- 22.2.15.1. Principais conceitos;
- 22.2.15.2. Criação de diferentes perfis de controle de acesso;
- 22.2.15.3. Aplicação de políticas de controle de acesso em um switch LAN
- 22.2.15.4. Funcionamento da solução em redes tradicionais;
- 22.2.15.5. Funcionamento da solução integrada a um fabric SD-LAN;
- 22.2.16. Segmentação
- 22.2.16.1. Principais conceitos;
- 22.2.16.2. Funcionamento da solução em redes tradicionais;
- 22.2.16.3. Funcionamento da solução integrada a um fabric SD-LAN;
- 22.2.16.4. Criação de regras de acesso entre dois perfis;
- 22.2.16.5. Criação de regras de acesso para o tráfego que entra e sai do fabric.
- 22.2.17. SD-LAN
- 22.2.17.1. Principais conceitos/protocolos/tecnologias envolvidas;
- 22.2.17.2. Criação de um fabric;
- 22.2.17.3. Adicionando um equipamento ao fabric;
- 22.2.17.4. Configuração das controladoras em alta disponibilidade;

ANEXO 2 - ENDEREÇOS

Controladoria-Geral da União - Sede

SAS, Quadra 01, Bloco A, Edifício Darcy Ribeiro

Brasília/DF - CEP: 70070-905

Tel (61) 2020-6712

Controladoria-Geral da União – IDC/Embratel

SCS Quadra 05, Bloco D e E – Setor Comercial Sul

Brasília/DF - CEP: 70.305-000

Tel (61) 2106-8178

Controladoria-Geral da União – Data Center/Serpro

SERPRO, SGAN 601 – Módulo V – Asa Norte – Brasília/DF

Brasília/DF - CEP: 70836-900

Controladoria Regional da União no Estado do Acre

End.: Via Chico Mendes, n.º 2.896 – Triângulo Novo.

Rio Branco/AC - CEP: 69.906-302

Tel: (68) 3321-2491 (Recepção) / (68) 3321-2631 (Gabinete) / (68) 3321-2638 (NAOP)

E-mail: cguac@cgu.gov.br

Controladoria Regional da União no Estado de Alagoas

End.: Avenida Comendador Gustavo Paiva, n.º 2.789, Ed. Norcon Empresarial - Salas 409 a 414 – Mangabeiras.

Maceió/AL - CEP: 57.038-000 / (82) 4009-6350

E-mail: cgual@cgu.gov.br

Controladoria Regional da União no Estado do Amapá

End.: Avenida Duque de Caxias n.º 116, Centro

Macapá/AP - CEP: 68.900-071

Tel: (96) 2101-9230 ramais: 9231 / 9232 / 9233 / 9234 / 9235 / 9236

E-mail: cguap@cgu.gov.br

Controladoria Regional da União no Estado do Amazonas

End.: Rua Salvador, 440, Sala 705, Condomínio Soberane, Adrianópolis

Manaus/AM - CEP: 69.057-040

Tel: (92) 2129-0163

E-mail: cguam@cgu.gov.br

Controladoria Regional da União no Estado da Bahia

End.: Avenida Frederico Pontes, s/n.º, Ed. Min. da Fazenda, 2º andar, Sala 200 - Comércio

Salvador/BA - CEP: 40.015-902

Tel: (71) 3254-5211 / (71) 3254-5212

E-mail: cguba@cgu.gov.br

Controladoria Regional da União no Estado do Ceará

End.: Rua Barão de Aracati, n.º 909, 8º andar - Bairro Aldeota

Fortaleza/CE - CEP: 60.115-081

Tel: (85) 3878-3800

E-mail: cguce@cgu.gov.br

Controladoria Regional da União no Estado do Espírito Santo

End.: Rua Pietrangelo de Biase, n.º 56, 4º andar, Sala 404 - Centro

Vitória/ES - CEP: 29.010-190

Tel: (27) 3211-5269

E-mail: cgues@cgu.gov.br

Controladoria Regional da União no Estado de Goiás

End.: Nona Avenida, Quadra A34, Lote 01/11, sala 216, Setor Leste Universitário

Goiânia/GO - CEP: 74.603-010

Tel: (62) 3621-3151 / (62) 3621-3184

Fax: (62) 3621-3182

E-mail: cgugo@cgu.gov.br

Controladoria Regional da União no Estado do Maranhão

End.: Avenida dos Holandeses, lote 08, Quadra 35, 1º, 2º e 3º Pavimentos - Bairro do Calhau

São Luís/MA - CEP: 65.071-380

Tel: (98) 3194-2000 / (98) 3268-4088

E-mail: cguma@cgu.gov.br

Controladoria Regional da União no Estado do Mato Grosso do Sul

End.: Rua Joaquim Murtinho, nº 65 - Centro

Campo Grande/MS - CEP: 79.002-100

Tel: (67) 3303-4450

E-mail: cgums@cgu.gov.br

Controladoria Regional da União no Estado do Mato Grosso

End.: Avenida Vereador Juliano da Costa Marques, 99, Centro Político Administrativo (CPA)

Cuiabá/MT - CEP: 78.049-937

Tel: (65) 2193-2437 / (65) 3615-2243

E-mail: cgumt@cgu.gov.br

Controladoria Regional da União no Estado de Minas Gerais

End.: Rua Timbiras, nº 1.778, Lourdes

Belo Horizonte/MG - CEP: 30.140-061

Tel: (31) 3888-3254

E-mail: cgumg@cgu.gov.br

Controladoria Regional da União no Estado do Pará

End.: Avenida Boulevard Castilhos Franca, nº 708 – 3º e 4º andar – Centro

Belém/PA - CEP: 66.010-020

Telefone: (91) 3205-8394/3222-9446

E-mail: cgupa@cgu.gov.br

Controladoria Regional da União no Estado da Paraíba

End.: Avenida Presidente Epitácio Pessoa – Térreo nº 3883, Bairro Miramar. Ed. Sede da CGU.

João Pessoa/PB - CEP: 58.032-000

Tel: (83) 2108-3047/ (83) 2108-3046

E-mail: cgupb@cgu.gov.br

José William Gomes da Silva

Controladoria Regional da União no Estado do Paraná

End.: Rua Marechal Deodoro, nº 555, 5º andar

Curitiba/PR - CEP: 80.020-911

Tel: (41) 4501-7900

E-mail: cgupr@cgu.gov.br

Controladoria Regional da União no Estado de Pernambuco

End.: Avenida Conde da Boa Vista, nº 800, Ed. Apolônio Sales, 10º andar - Boa Vista

Recife/PE - CEP: 50.060-004

Tel: (81) 2138-0202

E-mail: cgupe@cgu.gov.br

Controladoria Regional da União no Estado do Piauí

End.: Rua Mundinho Almeida, 105 - Noivos

Teresina/PI - CEP: 64046-140

Tel: (86) 4009-4853 / (86) 4009-4850 / (86) 3215-8131

E-mail: cgupi@cgu.gov.br

Controladoria Regional da União no Estado do Rio de Janeiro

End.: Avenida Presidente Antônio Carlos, nº 375, Ed. Palácio da Fazenda, 7º andar, Sala 711 - Centro

Rio de Janeiro/RJ - CEP: 20.020-010

Tel: (21) 3805-3700 / (21) 3805-3702 / (21) 3805-3707

E-mail: cgurj@cgu.gov.br

Controladoria Regional da União no Estado do Rio Grande do Norte

End.: Avenida: Hermes da Fonseca, nº 792 – Bairro: Tirol

Natal/RN - CEP: 59.020-095

Tel: (84) 3343-4732, (84) 3343-4740, (84) 3343-4747

E-mail: cgurn@cgu.gov.br

Controladoria Regional da União no Estado do Rio Grande do Sul

End.: Avenida Loureiro da Silva, nº 445, Ed. Ministério da Fazenda, 7º andar, Sala 704

Porto Alegre/RS - CEP: 90.013-900

Tel: (51) 3290-4762 / (51) 3290-4712

E-mail: cgurs@cgu.gov.br

Controladoria Regional da União no Estado de Rondônia

End.: Avenida Calama, nº 3.775 - Bairro da Embratel

Porto Velho/RO - CEP: 76.820-781

Tel: (69) 2181-8251/ (69) 2181-8261 / (69) 2181-8263

E-mail: cguro@cgu.gov.br

Controladoria Regional da União no Estado de Roraima

End.: Avenida Capitão Ene Garcez, nº 1.024 - São Francisco

Boa Vista/RR - CEP: 69.305-135

Tel.: (95) 3212-5220 (Gabinete) / (95) 3212-5229 (Apoio) / (95) 3212-5223 (NAP)

E-mail: cgurr@cgu.gov.br

Controladoria Regional da União no Estado de Santa Catarina

End.: Rua Conselheiro Mafra, 784 – Ático – Centro

Florianópolis/SC - CEP: 88010-102

Tel.: (48) 3298-7600 / 7607 (VOIP: 7600)

E-mail: cgusc@cgu.gov.br

Controladoria Regional da União no Estado de São Paulo

End.: Avenida Paulista, 1.804 - 18º Andar - Bela Vista

São Paulo/SP - CEP: 01.310-922

Tel: 2313-7802, 2313-7803

E-mail: cgusp@cgu.gov.br

Controladoria Regional da União no Estado de Sergipe

End.: Praça Graccho Cardoso, nº 44 - Bairro São José

Aracaju/SE - CEP: 49.015-180

Tel: (79) 4009-2178

E-mail: cguse@cgu.gov.br**Controladoria Regional da União no Estado de Tocantins**

End.: Quadra 103 Norte, Rua NO 05, Lote 13, Ed. Ranzi - Centro

Palmas/TO - CEP: 77.001-020

Tel.: (63) 3232-9350 (Geral) / (63) 3232-9354 (NAP) / (63) 3232-9355 (Gabinete)

E-mail: cguto@cgu.gov.br**ANEXO 3 - DISTRIBUIÇÃO DAS ENTREGAS DE BENS E PRESTAÇÃO DE SERVIÇO**

Item	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
DF Sede	55	55	55					6	6	6	2	2	2	16	10	6	14	1	1	1	1
AC					2	2	2										2				
AL					2	2	2										2				
AM	1	1	1		2	2	2										2				
AP					2	2	2										2				
BA	1	1	1		2	2	2										6				
CE	1	1	1		2	2	2										2				
ES					2	2	2										2				
GO	1	1	1		2	2	2										2				
MA	2	2	2	2	2	2	2										6				
MG	5	5	5	4	2	2	2										2				
MS					2	2	2										2				
MT					2	2	2										2				
PA	2	2	2	2	2	2	2										6				
PB					2	2	2										2				
PE	1	1	1		2	2	2										2				
PI	1	1	1		2	2	2										6				
PR	1	1	1		2	2	2										2				
RJ	3	3	3	3	2	2	2										6				
RN	4	4	4	4	2	2	2										2				
RO					2	2	2										2				
RR					2	2	2										2				
RS	1	1	1		2	2	2										2				

Subcláusula Segunda - A CONTRATADA compromete-se a não utilizar, bem como a não permitir que seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos utilizem, de forma diversa da prevista no contrato de prestação de serviços à CGU, as informações controladas reveladas.

Subcláusula Terceira - A CONTRATADA deverá cuidar para que as informações reveladas fiquem limitadas ao conhecimento dos diretores, consultores, prestadores de serviços, empregados e/ou prepostos que estejam diretamente envolvidos nas discussões, análises, reuniões e demais atividades relativas à prestação de serviços à CGU, devendo cientificá-los da existência deste Termo e da natureza confidencial das informações controladas reveladas.

Subcláusula Quarta - A CONTRATADA possuirá ou firmará acordos por escrito com seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente Termo.

Subcláusula Quinta - A CONTRATADA obriga-se a informar imediatamente à CGU qualquer violação das regras de sigilo estabelecidas neste Termo que tenha tomado conhecimento ou ocorrido por sua ação ou omissão, independentemente da existência de dolo.

CLÁUSULA QUARTA - DO DESCUMPRIMENTO

A quebra do sigilo das informações controladas reveladas, devidamente comprovada, sem autorização expressa da CGU, possibilitará a imediata rescisão de qualquer contrato firmado entre a CGU e a CONTRATADA sem qualquer ônus para a CGU. Nesse caso, a CONTRATADA estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CGU, inclusive os de ordem moral, bem como as responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo.

CLÁUSULA QUINTA - DO RETORNO DAS INFORMAÇÕES

A CONTRATADA devolverá imediatamente à CGU, ao término do Contrato, todo e qualquer material de propriedade desta, inclusive registro de documentos de qualquer natureza que tenham sido criados, usados ou mantidos sob seu controle ou posse, bem como de seus empregados, prepostos ou prestadores de serviço, assumindo o compromisso de não utilizar qualquer informação considerada confidencial, nos termos do presente TERMO DE CONFIDENCIALIDADE, a que teve acesso em decorrência do vínculo contratual com a CGU.

CLÁUSULA SEXTA - DA VIGÊNCIA

O presente Termo tem natureza irrevogável e irretratável, permanecendo em vigor a partir de sua assinatura e enquanto perdurar a natureza sigilosa ou restrita da informação, inclusive após a cessação da razão que ensejou o acesso à informação.

CLÁUSULA SÉTIMA - DAS DISPOSIÇÕES FINAIS

Os casos omissos neste TERMO DE CONFIDENCIALIDADE, assim como as dúvidas surgidas em decorrência da sua execução, serão resolvidos pela CGU.

Por estarem de acordo, a CONTRATADA, por meio de seu representante, firma o presente TERMO DE CONFIDENCIALIDADE, lavrando em duas vias de igual teor e forma.

Brasília, DF, _____ de _____ de _____.

<REPRESENTANTE DA CONTRATADA>	
<VÍNCULO DO REPRESENTANTE COM A CONTRATADA>	
RG:	
CPF:	
DE ACORDO:	
(integrantes da equipe técnica da CONTRATADA)	
Nome:	Nome:
RG:	RG:

ANEXO 5 – MODELO DE TERMO DE CIÊNCIA

INTRODUÇÃO
Visa obter o comprometimento formal dos empregados da contratada diretamente envolvidos no projeto sobre o conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes na Instituição.

IDENTIFICAÇÃO			
Contrato N°:			
Objeto:			
Contratante:	Controladoria-Geral da União		
Gestor do Contrato:		Matr.:	
Contratada:		CNPJ:	
Preposto da Contratada:		CPF:	

Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer o teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes na Contratante:

1. [Portaria CGU n° 2042/2017](#): Institui a Política de Segurança da Informação e das Comunicações - POSIC - na CGU;
2. [Norma Complementar n° 05/2017](#): Estabelece as diretrizes para o uso dos recursos de Tecnologia da Informação e Comunicação no âmbito da CGU; e
3. [Código de Conduta da CGU](#);

CIÊNCIA	
CONTRATADA – Empregados	
_____	_____
<Nome>	<Nome>
Matrícula: <Matr.>	Matrícula: <Matr.>
_____	_____
<Nome>	<Nome>
Matrícula: <Matr.>	Matrícula: <Matr.>
_____	_____
<Nome>	<Nome>
Matrícula: <Matr.>	Matrícula: <Matr.>

ANEXO 6 - MODELO DE AVALIAÇÃO DE TREINAMENTO

Tópicos a serem avaliados	CrITÉrios a serem avaliados	MÉdia de Avaliação por Categoria	MÉdia Geral
Em relação ao curso	Coerência entre o proposto e o realizado	Média das notas igual ou superior a 3.	Média das notas igual ou superior a 3,5.
	Material entregue no primeiro dia de treinamento?		
	Cumprimento do conteúdo programático		
	Aderência dos exercícios de laboratório ao conteúdo proposto		
Em relação ao Material Didático	Conteúdo contempla toda a ementa do Curso	Média das notas igual ou superior a 3.	
	Qualidade de Impressão		
	Clareza		
	Corretude		
Em relação ao Instrutor	Coerência com a versão da ferramenta/equipamento.	Média das notas igual ou superior a 3.	
	Clareza e Didática		
	Estímulo à participação do grupo		
	Esclarecimento de dúvidas		
	Foco na apresentação do tema		
	Administração do tempo previsto		
Em relação às instalações	Domínio do tema	Média das notas igual ou superior a 3.	
	POD		
	Equipamentos Disponibilizados		
	Sala de Aula		

As notas utilizadas no formulário para avaliação de cada critério do curso deverão ser as seguintes:

- 1 - Muito Insatisfeito
- 2 - Insatisfeito
- 3 - Indiferente
- 4 - Satisfeito
- 5 - Muito Satisfeito

Após o recebimento da planilha contendo as notas dos participantes do treinamento, deve-se adotar os seguintes critérios para o cômputo da nota:

- As notas dos ouvintes devem ser descartadas;

- Calcular a média ponderada das notas.
 - Equipes diretamente envolvidas tem peso 2
 - Equipes convidadas, peso 1.
- Quanto às médias:
 - A média de cada um dos grupos (Curso, Material e Instrutor) tem que ser superior a 3;
 - A média geral deve ser superior a 3,5.

 Documento assinado eletronicamente por **FABIO LUCIANO IKIJIRI, Agente Administrativo**, em 16/11/2020, às 16:38, conforme horário oficial de Brasília, com fundamento no art. 6º, §1º, do Decreto nº 8.539, de 08 de outubro de 2015.

 Documento assinado eletronicamente por **SALATIEL ROBSON BARBOSA DE OLIVEIRA, Integrante Requisitante, Substituto**, em 16/11/2020, às 17:09, conforme horário oficial de Brasília, com fundamento no art. 6º, §1º, do Decreto nº 8.539, de 08 de outubro de 2015.

 Documento assinado eletronicamente por **GUSTAVO MOURA DE SOUSA, Integrante Técnico**, em 16/11/2020, às 17:41, conforme horário oficial de Brasília, com fundamento no art. 6º, §1º, do Decreto nº 8.539, de 08 de outubro de 2015.

 Documento assinado eletronicamente por **HENRIQUE APARECIDO DA ROCHA, Diretor de Tecnologia da Informação**, em 17/11/2020, às 09:07, conforme horário oficial de Brasília, com fundamento no art. 6º, §1º, do Decreto nº 8.539, de 08 de outubro de 2015.



A autenticidade deste documento pode ser conferida no site <https://sei.cgu.gov.br/conferir> informando o código verificador 1722174 e o código CRC 050DE9F4