



Advocacia-Geral da União
Secretaria de Governança e Gestão Estratégica
Departamento de Tecnologia da Informação

TERMO DE REFERÊNCIA COMPRAS DE TIC – LEI 14.133/2021

Processo Administrativo nº 00693.000791/2023-11

Referência: Arts. 12 a 24 da Instrução Normativa SGD/ME nº 94, de 2022

DATA	VERSÃO	DESCRIÇÃO	AUTOR
03/10/2023	1.0	Criação do documento	Equipe de Planejamento da Contratação
10/11/2023A	2.0	Finalização da primeira versão do documento	Equipe de Planejamento da Contratação
04/12/2023	3.0	Segunda versão do documento, adequação para atendimento das recomendações do Parecer nº 00543/2023/CGSEM/SCGP/CGU/AGU	Equipe de Planejamento da Contratação
02/01/2024	4.0	Evento de Suspensão publicado para readequação dos artefatos	Equipe de Planejamento da Contratação
19/04/2024	5.0	Versão de readequação dos artefatos	Equipe de Planejamento da Contratação

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Registro de Preços para eventual contratação de solução de rede unificada, com fornecimento de equipamentos, incluindo serviços de instalação, configuração, suporte técnico, manutenção e garantia, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

GRUPO	ITEM	DESCRIÇÃO	CATSER/ CATMAT	MÉTRICA	CÓD. PMC-TIC	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	1	Switch Datacenter - Tipo 1 (Spine)	393273	Und	N/A	4	R\$ 200.663,83	R\$ 802.655,32

	2	Switch Datacenter - Tipo 2 (Leaf)	393273	Und	N/A	14	R\$ 147.067,75	R\$ 2.058.948,50
	3	Switch Acesso tipo 3 (24 portas PoE Base T)	393273	Und	N/A	230	R\$ 15.681,91	R\$ 3.606.839,30
	4	Switch Acesso tipo 4 (48 portas PoE Base T)	393273	Und	N/A	100	R\$ 21.390,86	R\$ 2.139.086,00
	5	Interface Ótica (transceiver) 100Gbe QSFP28 100GBase-SR4 MPO	393273	Und	N/A	60	R\$ 8.799,31	R\$ 527.958,60
	6	Interface Ótica (transceiver) 40Gbe QSFP28+ 40GBase-SR4 MPO	393273	Und	N/A	40	R\$ 5.827,38	R\$ 233.095,20
	7	Interface Ótica (transceiver) 25Gbe SFP28+ 25GBase-SR	27464	Und	N/A	240	R\$ 3.787,34	R\$ 908.961,60
	8	Interface Ótica (transceiver) 10Gbe QSFP28	27464	Und	N/A	60	R\$ 1.240,00	R\$ 74.400,00
	9	Access Point Tipo 1 (4x4)	415564	Und	N/A	160	R\$ 8.963,98	R\$ 1.434.236,80
	10	Access Point Tipo 2 (2x2)	415564	Und	N/A	550	R\$ 5.071,08	R\$ 2.789.094,00
	11	Solução de Gerenciamento e Controladora	415564	Und	N/A	1	R\$ 689.336,96	R\$ 689.336,96
	12	Solução de NAC	415564	Und	N/A	5000	R\$ 559,84	R\$ 2.799.200,00
	13	Cabo DAC para Empilhamento (Switches Tipo 3 e 4) ou Fibra	415564	Und	N/A	170	R\$ 509,00	R\$ 86.530,00
	14	Cabo Ótico 100 Gbe QSFP28 15 mts – MPO	415564	Und	N/A	60	R\$ 1.600,00	R\$ 96.000,00

	15	Cabo Ótico 40 Gbe QSFP28 10 mts - MPO	415564	Und	N/A	40	R\$ 1.400,00	R\$ 56.000,00
	16	Cabo Ótico 25 Gbe SFP28 10 mts	415564	Und	N/A	240	R\$ 163,11	R\$ 39.146,40
	17	Cabo Ótico 10 Gbe SFP+ Base-SR MMF LC 10 mts	415564	Und	N/A	40	R\$ 163,11	R\$ 6.524,40
	18	Serviço de Instalação e Configuração dos Switches de Datacenter Tipos 1 e 2	26972	Und	N/A	18	R\$ 28.272,36	R\$ 508.902,48
	19	Serviço de Instalação e Configuração dos Switches de Acesso Tipos 3 e 4	26972	Und	N/A	330	R\$ 993,00	R\$ 327.690,00
	20	Serviço de Instalação e Configuração dos Access Point Tipos 1 e 2	26972	Und	N/A	710	R\$ 975,00	R\$ 692.250,00
TOTAL GERAL								R\$ 19.876.855,56

1.2. O objeto desta contratação não se enquadra como sendo bem de luxo, conforme Decreto 10.818, de 27 de setembro de 2021.

1.3. O(s) bens e serviços objeto desta contratação são de natureza comum, nos termos do Inciso XIII, art. 6º, da Lei nº 14.133, de 2021, pautando-se na premissa que a contratação se baseia em padrões de desempenho e qualidade objetivamente definidos no TERMO DE REFERÊNCIA e seus APÊNDICES, por meio de especificações reconhecidas e usuais do mercado.

1.4. O serviço objeto deste TERMO DE REFERÊNCIA é enquadrado como sob demanda atrelado a aquisição dos itens 1 a 17 tendo em vista que, para cada equipamento, é necessário estar atrelado ao serviço de instalação e configuração, itens 18, 19 e 20, conforme descrito no Estudo Técnico Preliminar.

1.5. O prazo de vigência da Ata de Registro de preços será de 12 (doze) meses e poderá ser prorrogado, por igual período, desde que comprovado o preço vantajoso, na forma do artigo 84 da Lei nº 14.133, de 2021.

1.6. O prazo de vigência da contratação é de 12 (doze) meses, contados da data de sua assinatura, na forma do artigo 105 da Lei nº 14.133, de 2021.

1.8. O fornecimento de bens não contempla item de Catálogo de Soluções de TIC com Condições Padronizadas publicados pelo Órgão Central do SISP, previsto na Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.

1.7. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

2.1. A aquisição a ser contratada trata-se de solução de rede unificada, com fornecimento de equipamentos, incluindo serviços de instalação, configuração, suporte técnico, manutenção e garantia por 60 (sessenta) meses, conforme condições e exigências estabelecidas neste instrumento.

2.2. A AGU, possui dois datacenters, sendo que o principal fica no edifício Sede II, e o secundário no edifício Sede I. Além desses 2 (dois) prédios a AGU possui uma distribuição nacional em 148 (cento e quarenta e oito) unidades, conforme APÊNDICE “B”. Para a demanda do datacenter, itens 1 e 2 serão apenas para os 2 (dois) datacenters localizados em Brasília e para os demais itens 3 e 4 serão para as unidades de Brasília e demais localidades.

2.3. Por medida de segurança, em virtude da criticidade dos dados trafegados e armazenados no ambiente de infraestrutura da AGU, a instalação e configuração deverá ser projetizada para oferecer a menor tempo de parada, se necessário, que deverá ser feita com agendamento prévio.

2.4. O sistema de gerenciamento deve ser redundante, tolerante a falhas, funcionando em alta disponibilidade (HA) permitindo que toda a solução seja resiliente a falhas. Deverá possuir funcionalidades/recursos de segurança que impeça acesso não autorizado e minimamente protegido contra ataques. Como o projeto é de rede unificada o sistema de gerenciamento deverá prover, em apenas uma plataforma, o gerenciamento de toda solução e que contemple, minimamente, os requisitos necessários para atendimento das necessidades da AGU. Vislumbra-se também a necessidade de visualização em tempo real do status de funcionamento de toda a solução, onde

também possa ser acompanhado o status operacional da solução. No tocante aos recursos de segurança intrínsecos à solução objeto dessa contratação prevê-se a composição com uma solução de NAC para controlar todo o acesso à rede além de funcionalidades adicionais de segurança que permitam que a AGU possa criar regras de acesso e postura, de comunicação ponto-a-ponto entre dispositivos clientes de rede, ativação/desativação de porta do switch de maneira automática além de mudança de VLAN de maneira dinâmica, dentre outras funcionalidades e que a solução consiga tratar todas as conexões por meio de Inteligência Artificial identificando por meio de comportamento desvios das atividades fim da casa reconhecidamente sendo identificadas e tratadas de maneira automatizada. Assim, a contratada deverá garantir a plena disponibilidade da funcionalidade dessa ferramenta de gerenciamento além de total integração com a solução a ser adquirida.

2.5. De maneira complementar e não menos importante, faz-se necessário que a solução seja suportada por 60 (sessenta) meses com garantia em todos os seus componentes que compõe a solução e que após o período de garantia supra a solução não perca nenhuma de suas funcionalidades. Nesse caso será admitido que, passados os 60 (sessenta) meses de suporte e garantia a solução perca, evidentemente, apenas as atualizações de firmware, versões e correções além do suporte técnico.

2.6. Os componentes de software que constituem a solução a ser fornecida não devem expirar após o término da garantia ou o período de suporte do fabricante aos componentes da solução, ou seja, as licenças devem ser perpétuas.

2.7. Os produtos que compõem a solução não devem estar com término de comercialização (*End-of-Sale*) anunciado, isto é, devem estar em produção e serem comercializados pelo fabricante no momento da assinatura do Pedido de Compra/Contrato. Após ser anunciado o término da comercialização (*End-of-Sale*) dos produtos que o compõem a solução, o suporte (*End-of-Support*) deverá permanecer por, no mínimo, o período de vigência da garantia.

2.8. Todos os custos referentes ao fornecimento dos equipamentos e serviços devem estar previamente agregados na composição dos preços dos itens informados na PROPOSTA DE PREÇOS dos Licitantes, devidamente evidenciados conforme exigências contidas no item 8 deste documento. Não haverá pagamento adicional por nenhum outro insumo ou serviço além daqueles previstos no objeto da contratação. Todos os materiais, peças e componentes a serem disponibilizados no escopo da contratação devem ser novos, não reconicionados, de primeiro uso além de serem originais do mesmo fabricante da solução.

2.9. O TERMO DE REFERÊNCIA foi elaborado a partir do Estudo Técnico Preliminar da Contratação (ETPC) e contém os elementos necessários e suficientes, com adequado nível de precisão, para caracterizar o objeto da pretensão contratação. Seu conteúdo está estruturado em dois núcleos: o conteúdo mestre, que reúne as definições acerca dos termos e condições contratuais (condições gerais, modelo de execução e modelo de gestão) e o conteúdo complementar, que reúne os detalhes relacionados à especificação técnica de cada item do objeto (documentos de apoio).

2.10. Destacamos que a solução de rede datacenter, acesso e wireless trata-se de aquisição de equipamentos que compõe uma solução de rede unificada, conforme descrito no Estudo Técnico Preliminar que subsidia esta contratação. Assim destacamos que o pagamento dos serviços dispostos nos itens 18, 19 e 20 deverá ocorrer sob demanda, sempre que necessário para proceder com a instalação e configuração da solução, aferindo-se os Níveis Mínimos de Serviços NMS exigidos para cada entrega.

2.11. A descrição da solução como um todo encontra-se pormenorizada no APÊNDICE “A” deste TERMO DE REFERÊNCIA.

3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

3.1. Nos termos do art. 131 da Constituição, a Advocacia-Geral da União (AGU) é a instituição que, diretamente ou através de órgão vinculado, representa a União, judicial e extrajudicialmente, cabendo-lhe, nos termos da lei complementar que dispuser sobre sua organização e funcionamento, as atividades de consultoria e assessoramento jurídico do Poder Executivo.

3.2. A AGU é uma Instituição prevista pela Constituição Federal, e tem natureza de Função Essencial à Justiça, não se vinculando, por isso, a nenhum dos três Poderes que representa.

3.3. O Advogado-Geral da União, dentre outras atribuições, deve assessorar direta, imediata e pessoalmente o Presidente da República, dirigir a AGU e representar a União junto ao Supremo Tribunal Federal.

3.4. A motivação da presente pretensão contratual decorre da necessidade de garantir a continuidade dos serviços prestados pelo DTI a AGU. Importante salientar que o ambiente de rede da AGU encontra-se boa parte sem suporte técnico e garantia, sem funcionalidades de gerenciamento mínimo e, ainda, com a necessidade de atualização tecnológica e expansão da rede sem fio (wireless).

3.5. Cabe salientar que a confiabilidade dos sistemas e informações críticas e sensíveis de Estado custeadas pela Advocacia-Geral da União depende, essencialmente, da plena e perfeita operação da infraestrutura de conectividade (rede de dados) da AGU.

3.6. O estudo aplicado no ETP, demonstrou ainda, que o ambiente de infraestrutura de rede da AGU além de estar completamente defasado tecnologicamente possui equipamentos em final em final de vida pelo Fabricante. Outro aspecto é no que tange ao sistema de gerenciamento inexistente que dificulta minimamente a identificação de equipamentos de rede além de todas as outras atividades comuns na Administração de Rede. Da forma que se encontra, o ambiente de rede está demasiadamente vulnerável. O ambiente necessita, ainda, de uma expansão da comunicação sem fio para as unidades da AGU. Algo que deve ser tratado de maneira unificada com a necessidade já exposta em tempo de Estudo Técnico.

3.7. Desta feita, com a crescente demanda de recursos de rede e, ainda, do crescimento exponencial das vulnerabilidades e de seus exploradores (*hackers*) faz-se imprescindível que o ambiente de rede com fio e sem fio funcione de forma ininterrupta, com segurança, controle, gerenciamento além de eficiência e eficácia, a fim de evitar prejuízos imensuráveis para a instituição e todos os usuários, conforme condições, quantidades e exigências estabelecidas neste instrumento e seus anexos.

3.8. O conjunto das características e especificações necessárias e suficientes para definir a solução de TIC a ser contratada (requisitos) foi elaborado de acordo com o Estudo Técnico Preliminar e seus anexos, considerando o disposto no art. 16 da IN-94/2022/SGD, estão descritos neste TERMO DE REFERÊNCIA, da seguinte forma:

- a) Requisitos Técnicos da Solução no APÊNDICE “A”.
- b) Localidades e quantitativos por tipo de equipamento no APÊNDICE “B”.

3.9. O objeto da contratação encontra-se alinhado ao Plano Diretor de Tecnologia da Informação e Comunicação da AGU - PDTIC 2023-2025, ao Planejamento Estratégico Institucional - PEI, de acordo com o Mapa Estratégico da AGU 2023-2025, e ao Plano de Contratações Anual - PCA 2024, conforme tabela abaixo:

ID PCA no PNCP	Data de publicação no PNCP	Id do item no PCA	Classe/Grupo:	Identificador da Futura Contratação
26994558000123-0-	19/05/2023	90/2024	7050	110792-90112/2024

000008/2024			
ALINHAMENTO AOS PLANOS ESTRATÉGICOS			
ID	Objetivos Estratégicos		
OE.05	Garantir a infraestrutura de TI apropriada às necessidades da AGU do Plano Estratégico Institucional		
ALINHAMENTO AO PDTIC 2023-2025			
ID	Ação do PDTIC	ID	Meta do PDTIC associada
A.02	Entregar produtos e serviços de TI que gerem valor à AGU.	IE.03	Aprimorar a infraestrutura de TI das unidades da AGU

3.10. A contratação não tem por objeto a oferta de serviços públicos digitais, mas os serviços objeto da contratação pode ser eventualmente utilizados para construção de serviços públicos digitais, ocasião na qual serão integrados à plataforma gov.br.

3.11. Parcelamento da Solução de TIC

3.11.1. O parcelamento da solução não se aplica, sendo o modelo definido para esta contratação o mais adequado tecnicamente, sem restringir ou prejudicar a competitividade do certame e, consequentemente, visando promover maior vantajosidade para a Administração.

3.12. Resultados e Benefícios a Serem Alcançados

3.12.1. Dentre os principais resultados a serem alcançados com a contratação, pode-se destacar:

- Manter a disponibilidade dos serviços de rede de dados;
- Atender às necessidades de negócio, garantindo infraestrutura de TI adequada para a execução das atividades da AGU;
- Mitigar possíveis riscos, danos ou indisponibilidade a prestação de serviços de TI, decorrentes de problemas técnicos identificados nos equipamentos;
- Permitir a criação de condições favoráveis para manter os níveis de desempenho e disponibilidade exigidos;
- Garantir a continuidade do funcionamento dos sistemas da AGU, dentre eles do SAPIENS;
- Manter o volume de absorção das várias demandas do ambiente de TIC relativas à solução de infraestrutura de comunicação de dados, com adequada disponibilidade e integridade no tráfego de dados e de informações;

- g) Dotar a AGU de serviços especializados com o objetivo de assegurar o pleno funcionamento dos seus ativos de comunicação;
- h) Prover solução confiável para interconectar os ativos de rede;
- i) Manter o pleno funcionamento da infraestrutura e dos sistemas internos da AGU
- j) Corrigir os problemas identificados colocando os ambientes 100% integrados e operacionais;
- k) Prover o ambiente de uma plataforma única de gerenciamento e gestão dos ativos de rede;
- l) Modernização dos ambientes de rede;
- m) Disponibilização de ambiente de rede sem fio em todas as unidades da AGU;
- n) Garantia da continuidade das operações tecnológicas da AGU;
- o) Facilidade de custeamento e orçamentação;
- p) Facilidade na gestão e fiscalização do contrato;
- q) Racionalizar o uso de recursos orçamentários e promover melhoria da eficiência administrativa;
- r) Tolerância a mudanças na infraestrutura;
- s) Resiliência do ambiente de rede da AGU;
- t) Provisão e manutenção de infraestrutura de TI adequada, disponível e segura para suportar as demandas de negócio;
- u) Garantia da disponibilidade e a continuidade dos equipamentos e sistemas de TI;
- v) Promover adequações técnicas e gerenciais em relação ao atual modelo de serviço mantido pela AGU;
- w) Promova a governança de TIC baseada em boas práticas;
- x) Flexibilidade e escalabilidade;
- y) Garantia da disponibilidade e integridade da informação, mitigando riscos de inoperabilidade prolongada dos serviços;

- z) Ampliar o controle e o gerenciamento dos recursos tecnológicos de rede;
- aa) Implantação simplificada;
- bb) Maior segurança;
- cc) Simplificação e conformidade;
- dd) Acesso seguro consistente;
- ee) Facilidade de implementação e de gerenciamento; e
- ff) Adoção de tecnologias de ponta.

4. REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos do negócio

4.1.1. A presente contratação orienta-se pelos seguintes requisitos de negócio:

- a) Atualização/modernização tecnológica de todo o ambiente de redes da AGU;
- b) Garantir o funcionamento das unidades da AGU;
- c) Tratar todo o tráfego de rede interna com segurança e gestão;
- d) Garantir a resiliência de rede;
- e) Ampliar o ambiente de rede sem fio para todas as unidades da AGU;
- f) Aumentar a performance de rede melhorando a experiência dos usuários;
- g) Manter a solução de redes sustentadas, atualizadas e com suporte técnico (garantia);
- h) Prover uma infraestrutura de rede com maior escalabilidade que acompanhe os movimentos de crescimento e diminuição de unidades físicas da AGU;
- i) Redução de custos;
- j) Suportar os projetos de modernização e expansão de funcionalidades;
- k) Garantir conformidade com os acordos de nível de serviço, em que os equipamentos requerem operação contínua 24 horas por 7 dias por semana, no caso dos switches de datacenter;
- l) Melhor gerenciamento dos riscos;

- m) Redução dos incidentes e indisponibilidades de sistemas da AGU onde a causa está relacionada com a rede melhorando, ainda, a performance dessas aplicações para os usuários da AGU;
- n) Melhor eficiência;
- o) Visibilidade e controle; e
- p) Segurança no tratamento dos dados trafegados protegendo o perímetro de ações indesejadas e realizadas por pessoas mal-intencionadas (hackers) e pela disseminação de malwares (ex. Ramsonware).

4.1.2. Deverão ser observados os regulamentos, normas e instruções de segurança da informação e comunicações adotadas, incluindo, mas não se limitando, ao definido na Política de Segurança da Informação e Comunicações e suas Normas Complementares, durante a execução dos serviços nas instalações da AGU.

4.1.3. Deverá ser garantida a disponibilidade, integridade, confidencialidade e sigilo dos documentos e informações inerentes ao contrato e seus serviços, podendo ser responsabilizado legalmente quem porventura causar perdas e danos à AGU e a terceiros.

4.1.4. Devem ser utilizadas ferramentas de proteção e segurança de informações a fim de evitar qualquer acesso não autorizado aos sistemas e softwares, seja em relação ao que eventualmente estejam sob sua responsabilidade direta ou que foram disponibilizados, ainda que por meio de link.

4.1.5. Quando solicitado formalmente pela contratante, deverão ser realizadas, prioritária e concomitantemente, alterações para sanar possíveis problemas de segurança ou de vulnerabilidade nos referidos sistemas ou softwares utilizados para execução do serviço contratado.

4.1.6. Informar à AGU, formalmente e tempestivamente, sobre quaisquer necessidades de atualização ou mudança na configuração dos serviços prestados.

4.1.7. Prestar os esclarecimentos necessários, bem como informações concernentes à natureza e andamento dos serviços executados, ou em execução.

4.1.8. Garantir a integridade e disponibilidade dos documentos e informações que, em função do Contrato, estiverem sob a sua guarda, sob pena de responder por eventuais perdas e/ou danos causados à AGU e a terceiros.

4.1.9. Não divulgar, mesmo que em caráter estatístico, quaisquer informações originadas na AGU, sem prévia autorização.

4.1.10. Prover segurança através da utilização de identificação individual dos profissionais envolvidos na execução dos serviços.

4.1.11. Os profissionais deverão utilizar a conta de domínio que lhe for atribuída, de forma controlada e intransferível, mantendo secreta a sua respectiva senha, pois todas as ações efetuadas através desta, serão de responsabilidade do profissional do provedor da solução.

4.1.12. Deverá acatar e obedecer às normas de utilização e segurança das instalações da AGU.

4.1.13. Deverá manter os seus profissionais informados quanto às normas disciplinares, exigindo sua fiel observância, especialmente quanto à utilização e segurança das instalações.

4.1.14. Quando aplicável, o provedor da solução deverá realizar transferência de conhecimentos tecnológicos para usuários internos e/ou equipe técnica do requisitante nas soluções entregues, conforme definição, sem custo adicional, a fim de garantir a necessária independência do requisitante em relação ao provedor.

4.1.15. Entendemos, ainda, que os requisitos necessários e suficientes à escolha da solução estão presentes ao longo do Estudo Técnico, deste TERMO DE REFERÊNCIA e, ainda, descritos no APÊNDICE “A”. De maneira não exaustiva, seguem, abaixo, alguns deles:

- a) **Eficiência:** Atendimento pleno às necessidades de negócio da AGU aumentando a disponibilidade e garantindo qualidade e segurança da informação;
- b) **Eficácia:** Resolver os atuais problemas de rede reportados à AGU;
- c) **Otimização de custos:** Contratação de uma solução que atenda às necessidades;
- d) **Visibilidade:** Apoiar a gestão fornecendo completa visibilidade no funcionamento e no acesso aos recursos de infraestrutura de rede da AGU; e
- e) **Disponibilidade Nacional:** Fornecimento, instalação e configuração da solução em ambiente nacional da AGU.

4.1.16. A CONTRATADA deverá instalar fisicamente/logicamente e configurar toda a solução, executando-as com pessoal técnico comprovadamente qualificado, sem qualquer despesa adicional

para a AGU, incluindo toda a mão de obra e o material necessário à execução dos serviços, tais como suprimentos, peças, componentes e acessórios.

4.1.17. Nos valores da contratação deverão estar inclusos todas as despesas incidentes na prestação dos serviços tais como salários, vales refeição e/ou alimentação, seguros, impostos, taxas, contribuições, indenizações, transporte, ferramentas, instalação e desinstalação de componentes, assistência técnica, manutenções preventiva e corretiva dos equipamentos, bem como todas as peças de reposição, sistemas, acessórios, materiais e insumos necessários para o pleno funcionamento deles.

4.1.18. O objeto a ser contratado trata-se de aquisição de bens e serviços comuns sem fornecimento de mão de obra em regime de dedicação exclusiva, pois, possui padrões de desempenho e qualidade objetivamente definidos, mediante as especificações usuais do mercado.

4.1.19. A prestação desses serviços visa atender as demandas de ambiente de infraestrutura de rede da AGU. A solução definida no TERMO DE REFERÊNCIA busca obter a proposta mais vantajosa para a AGU, avaliando os ganhos de escala.

4.1.20. Entende-se por “materiais necessários para a execução dos serviços” todas as peças, ferramentas, equipamentos, instrumentos, materiais de consumo, acessórios, transporte e outros insumos não explícitos imprescindíveis para execução na estrutura da AGU do serviço de manutenção contratado com qualidade, segurança e em conformidade com as normas técnicas aplicáveis.

4.2. Requisitos de Capacitação

4.2.1. Faz-se necessário que ocorra a transferência de conhecimentos para possibilitar às equipes técnicas a gestão e acompanhamento/gestão da solução.

4.3. Requisitos Legais

4.3.1. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), Instrução Normativa SEGES/MP nº 5, de 25 de maio de 2017, Instrução Normativa SEGES/ME nº 77/2022, Decreto nº 11.462, de 31 de março de 2023, e a outras legislações aplicáveis;

4.3.2. Lei nº 12.682, de 9 de julho de 2012, que dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos;

4.3.3. Decreto-Lei nº. 200 de 25 de fevereiro de 1967, que dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências;

4.3.4. Decreto nº 6.605, de 14 de outubro de 2008, que dispõe sobre o Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira - CG ICPBrasil, sua Secretaria-Executiva e sua Comissão Técnica Executiva - COTEC;

4.3.5. Decreto nº 7.174, de 12 de maio de 2010, que regulamenta a contratação de bens e serviços de informática e automação pela Administração Pública Federal;

4.3.6. Decreto nº 10.543, de 13 de novembro de 2020, que dispõe sobre o uso de assinaturas eletrônicas na administração pública federal e regulamenta o art. 5º da Lei nº 14.063, de 23 de setembro de 2020, quanto ao nível mínimo exigido para a assinatura eletrônica em interações com o ente público.

4.3.7. Deverão ser cumpridos os procedimentos, normas, modelos e regulamentos vigentes na AGU.

4.4. **Requisitos de Manutenção**

4.4.1. Devido às características da solução, durante o período de garantia, 60 (sessenta meses), a Contratada deverá prover a manutenção necessária visando a correção de erros, problemas e vícios identificados durante o uso da solução. Para tanto deverá disponibilizar um canal de comunicação por meio de, no mínimo, telefone e e-mail.

4.5. **Requisitos Temporais**

4.5.1. O fornecimento da solução deverá ocorrer no prazo máximo de 90 (noventa) dias corridos a contar do recebimento da abertura da Ordem de Fornecimento de Bens (OFB) e/ou da Ordem de Serviço (OS), emitida pela Contratante, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pelo Contratado e autorizado pela Contratante

4.5.2. Considerando que os itens dispostos nesse TERMO DE REFERÊNCIA (bens e serviços), dependem um do outro para a correta entrega é imprescindível que os prazos de abertura das Ordens de Serviço de fornecimento dos bens e dos serviços ocorram no mesmo período e que a entrega coincida.

4.5.3. Na contagem dos prazos estabelecidos neste TERMO DE REFERÊNCIA, quando não expressados de forma contrária, excluir-se-á o dia do início e incluir-se-á o do vencimento, na forma do artigo 183, da Lei 14.133 de 2021.

4.5.4. Todos os prazos citados, quando não expresso de forma contrária, serão considerados em dias corridos. Ressaltando que serão contados os dias a partir da hora em que ocorrer o incidente até a mesma hora do último dia, conforme os prazos.

4.5.5. Na entrega dos equipamentos, deverão ser observados também os prazos estabelecidos no APÊNDICE “A” deste TERMO DE REFERÊNCIA.

4.6. **Requisitos de Segurança e Privacidade**

4.6.1. A CONTRATADA deverá respeitar as normas nacionais de proteção de dados e informações vigentes, sobretudo considerando a possibilidade de custódia de conhecimentos, informações e dados pelo prestador de serviços, observadas as seguintes diretrizes:

- a) Garantia de aplicabilidade da legislação brasileira sobre os princípios, diretrizes e responsabilidades relacionados à segurança da informação e à proteção de dados.
- b) Garantia que, em qualquer hipótese, a Administração tem a tutela absoluta sobre os conhecimentos, informações e dados produzidos pelos serviços.
- c) Vedado o uso corporativo dos conhecimentos, informações e dados pelo prestador de serviço.
- d) Possuir Plano de Continuidade, Recuperação de Desastres e Contingência de Negócio, que possa ser testado regularmente, objetivando a disponibilidade dos dados e serviços em caso de interrupção.
- e) Desenvolver e colocar em prática procedimentos de respostas a incidentes relacionados com os serviços.

4.6.2. A CONTRATADA deverá seguir as normas internas de segurança da informação da AGU, bem como suas atualizações.

4.6.3. A CONTRATADA será expressamente responsabilizada quanto à manutenção de sigilo absoluto sobre quaisquer dados, informações, códigos-fonte e artefatos, contidos em quaisquer documentos e em quaisquer mídias, de que venham a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto divulgar, reproduzir ou utilizar, sob pena de aplicação de sanção e outras penalidades previstas na legislação vigente, independente da classificação de sigilo conferida pela AGU a tais documentos.

4.6.4. A CONTRATADA não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, da AGU sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos.

4.6.5. Cada profissional da CONTRATADA deverá assinar termo declarando estar ciente de que a estrutura computacional disponibilizada pela AGU não poderá ser utilizada para fins particulares, e que a navegação em sítios da Internet e as correspondências em meio eletrônico utilizando o endereço da AGU ou acessadas a partir dos seus equipamentos poderão ser auditadas.

4.6.6. Cada profissional da CONTRATADA deverá assinar termo de compromisso declarando total obediência às normas de segurança vigentes ou que venham a ser implantadas, a qualquer tempo, na AGU.

4.7. Requisitos Sociais, Ambientais e Culturais

4.7.1. A CONTRATADA deverá adotar práticas de sustentabilidade ambiental na execução do objeto, no que couber, conforme disposto na Instrução Normativa SLTI/MP nº 1/2010 e Decreto no 7.746/2012, da Casa Civil, da Presidência da República.

4.7.2. A CONTRATADA deverá assegurar a viabilidade técnica e o adequado tratamento do impacto ambiental específicos, inclusive:

- a) baixo impacto sobre recursos naturais como flora, fauna, ar, solo e água;
- b) preferências para materiais, tecnologias e matérias-primas de origem local;
- c) maior eficiência na utilização de recursos naturais como água e energia;
- d) maior geração de empregos, preferencialmente com mão de obra local;
- e) maior vida útil e menor custo de manutenção de bens;
- f) uso de inovações que reduzam a pressão sobre recursos naturais;
- g) origem sustentável dos recursos naturais utilizados nos bens e serviços;
- h) adotar práticas de gestão que garantam os direitos trabalhistas e o atendimento às normas internas e de segurança e medicina do trabalho para seus empregados;
- i) administrar situações emergenciais de acidentes com eficácia, mitigando os impactos aos empregados, colaboradores, usuários e ao meio ambiente;

- j) conduzir suas ações em conformidade com os requisitos legais e regulamentos aplicáveis, observando também a legislação ambiental para a prevenção de adversidades ao meio ambiente e à saúde dos trabalhadores e envolvidos na prestação dos serviços;
- k) realizar um programa interno de treinamento de seus empregados, nos três primeiros meses de execução contratual, para redução de consumo de energia elétrica, de redução de consumo de água e redução da produção de resíduos sólidos, observadas as normas ambientais vigentes;
- l) disponibilizar os Equipamentos de Proteção Individual (EPIs), quando aplicável, para a execução das atividades de modo confortável, seguro e de acordo com as condições climáticas, favorecendo a qualidade de vida no ambiente de trabalho;
- m) orientar sobre o cumprimento, por parte dos funcionários, das Normas Internas e de Segurança e Medicina do Trabalho, tais como prevenção de incêndio nas áreas da prestação de serviço, zelando pela segurança e pela saúde dos usuários;
- n) respeitar as Normas Brasileiras - NBR publicadas pela Associação Brasileira de Normas Técnicas sobre resíduos sólidos;
- o) orientar seus empregados para a destinação dos resíduos recicláveis descartados aos devidos coletores de resíduos recicláveis existentes nas dependências da AGU.

4.7.3. A licitante deverá apresentar Declaração de Sustentabilidade Ambiental, conforme modelo constante deste TERMO DE REFERÊNCIA no APÊNDICE “E”, a ser apresentado na fase de aceitação da proposta.

4.7.4. A exigência visa atender aos dispositivos normativos, acima enumerados, bem como demais normativos acerca dos critérios de sustentabilidade socioambiental, de forma a estabelecer que a licitante promova ações ambientais por meio de treinamento de seus colaboradores, pela conscientização de todos os envolvidos na prestação dos serviços, visando o cumprimento das ações estabelecidas neste TERMO DE REFERÊNCIA, que se estenderão na gestão contratual, refletindo na responsabilidade da Administração no desempenho do papel de consumidor potencial e na responsabilidade ambiental e socioambiental entre as partes.

4.7.5. Os serviços devem estar aderentes às seguintes diretrizes sociais, ambientais e culturais.

4.7.6. Os funcionários da CONTRATADA deverão vestir-se de maneira condizente com a atividade a ser desempenhada e com os padrões adotados pela AGU;

4.7.7. Outros padrões sociais, ambientais e culturais que venham a ser definidos ou que se mostrem pertinentes para essa contratação.

4.8. Requisitos da Arquitetura Tecnológica

4.8.1. Os serviços deverão ser executados observando-se as diretrizes de arquitetura tecnológica estabelecidas pela área técnica da Contratante.

4.8.2. A adoção de tecnologia ou arquitetura diversa deverá ser autorizada previamente pela AGU. Caso não seja autorizada, é vedado à Contratada adotar arquitetura, componentes ou tecnologias diferentes daquelas definidas pela Contratante.

4.8.3. Durante o período de garantia caberá à CONTRATADA toda a manutenção decorrente de defeitos que resultem em funcionamento incorreto ou em desconformidade com as especificações e padrões determinados para AGU, desde que o erro ou falha, comprovadamente, não se dê em função de falhas nas especificações feitas para AGU.

4.8.4. O atendimento e a efetiva solução dos chamados para execução de correções de defeitos em serviços já entregues deverão ocorrer no prazo negociado e formalizado entre a AGU e a CONTRATADA. O não cumprimento dos prazos estabelecidos sujeita a CONTRATADA às penalidades previstas.

4.9. Requisitos de Projeto e de Implementação

4.9.1. Os serviços deverão observar integralmente os requisitos de projeto e de implementação descritos a seguir:

4.9.1.1. Os serviços serão fiscalizados conforme Modelos de Execução e Gestão definidos neste TERMO DE REFERÊNCIA e no Plano de Fiscalização, ou instrumento similar, a ser elaborado e atualizado durante o monitoramento da execução do contrato.

4.9.1.2. O Plano de Instalação da solução a ser fornecida deverá conter, de forma detalhada:

4.9.1.2.1. Descrição dos equipamentos e softwares que deverão ser instalados;

4.9.1.2.2. Pré-requisitos para a instalação: deverão ser descritos todos os recursos e condições que deverão ser providos pela AGU, necessários para que a CONTRATADA possa realizar os serviços de instalação;

4.9.1.2.3. Relação dos especialistas certificados da CONTRATADA alocados nos processos de instalação;

4.9.1.2.4. Relatórios das visitas técnicas de pré-instalação;

4.9.1.2.5. Visão geral da arquitetura da solução que será implantada;

4.9.1.2.6. Descrição das etapas do processo de instalação, detalhando as opções de configuração adotadas;

4.9.1.2.7. Cronograma de execução; e

4.9.1.2.8. Necessidade de atualização de versões dos produtos a serem fornecidos.

4.9.2. No prazo de até 5 (cinco) dias úteis, a partir do recebimento formal do Plano de Instalação, a AGU deverá se manifestar sobre sua aprovação. Caso seja necessário, será concedido à CONTRATADA um novo prazo de até 5 (cinco) dias úteis para eventuais ajustes e reapresentação da documentação reprovada. A versão definitiva do plano de instalação será a versão aprovada pela Equipe Técnica da AGU.

4.9.3. A instalação, migração e configuração dos equipamentos somente será iniciada após a aprovação pela AGU no prazo definido pela AGU no momento de aprovação do Plano de Instalação elaborado pela CONTRATADA, prazo este que será utilizado para elaboração pela AGU do Padrão de Instalação (PIN), o qual especificará a integração da solução do fornecedor com os ambientes da AGU.

4.10. Requisitos de Implantação

4.10.1. Os serviços de instalação e migração deverão observar integralmente os requisitos de implantação estabelecidos no APÊNDICE “A”, deste TERMO DE REFERÊNCIA, bem como nos subitens descritos a seguir:

4.10.1.1. O planejamento para implantar a Solução de Tecnologia da Informação - STI objeto deste TERMO DE REFERÊNCIA deverá ser viabilizado sem ônus adicional à AGU e será baseado em reuniões técnicas e repasse de documentos e/ou manuais específicos das tecnologias envolvidas neste objeto.

4.10.1.2. A CONTRATADA deverá realizar a instalação “assistida” de todo componente de hardware e software, incluindo sua configuração, interligação física (cabeamento) e lógica à rede de dados da AGU e migração da configuração dos equipamentos atuais para os novos, que será acompanhada por analistas da AGU. Todo processo de instalação deverá atender ao especificado no Plano de Instalação aprovado pela AGU, conforme descrito no subitem 4.9, acima, deste TERMO DE REFERÊNCIA.

4.10.1.3. A instalação deve ser realizada por profissionais especializados, em conformidade com as certificações disponíveis pelo fabricante da solução contratada.

4.10.1.3.1. As certificações exigidas no subitem anterior devem estar válidas durante o período de prestação dos serviços de instalação, migração e configuração.

4.10.1.4. A CONTRATADA deverá providenciar a aplicação de todas as correções e atualizações de software liberados até a data da instalação, incluindo a atualização de firmware dos componentes de hardware que compõem a solução, bem como a integração de todos os módulos da solução, salvo solicitação da AGU por outra versão. A CONTRATADA deverá encaminhar documento, em meio eletrônico, que comprove a aplicação das atualizações em todos os produtos instalados.

4.10.1.5. Constatada a ocorrência de divergência na especificação técnica ou qualquer outro defeito de operação durante a instalação dos equipamentos, fica a CONTRATADA obrigada a providenciar a sua correção ou, a critério da AGU, a substituição dos produtos adquiridos.

4.10.1.6. Os serviços de instalação deverão ocorrer, preferencialmente, em dias úteis, no horário compreendido entre 9h e 18h, salvo definição contrária, realizada em comum acordo entre a AGU e a CONTRATADA e deverão ser agendados previamente com a AGU. Nesse caso questões relacionadas a indisponibilização do ambiente serão levadas em consideração para agendamentos fora da janela temporal informada.

4.10.1.7. Para os serviços de instalação dos ambientes de Datacenter localizados em Brasília/DF deverão ocorrer em dias não úteis podendo ser finais de semana e feriados ou em períodos noturnos/madrugada agendados previamente entre a AGU e a CONTRATADA conforme explicitado no item 4.11.18. deste TERMO DE REFERÊNCIA.

4.11. Requisitos de Garantia e Manutenção

4.11.1. O prazo de garantia contratual dos serviços, complementar à garantia legal, será de, no mínimo, 60 (sessenta) meses, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo de cada OFB e/ou OS, nos termos especificados em Requisitos Temporais.

4.11.2. A garantia será prestada com vistas a manter os produtos fornecidos, hardware ou software, em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o Contratante.

4.11.3. A garantia abrange a realização da manutenção corretiva dos bens pelo próprio Contratado, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas e/ou recomendação do fabricante.

4.11.4. Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias.

4.11.5. As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento.

4.11.6. Uma vez notificado, a Contratada realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo definidos nesse termo, contados a partir da data de retirada do equipamento das dependências da Administração pela Contratada ou pela assistência técnica autorizada.

4.11.7. O prazo de reparação ou substituição, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada do Contratado, aceita pelo Contratante.

4.11.8. Na hipótese do subitem acima, a Contratada deverá disponibilizar equipamento equivalente, de especificação igual ou superior ao anteriormente fornecido, para utilização em caráter provisório pelo Contratante, de modo a garantir a continuidade dos trabalhos administrativos durante a execução dos reparos.

4.11.9. Decorrido o prazo para reparos e substituições sem o atendimento da solicitação do Contratante ou a apresentação de justificativas pela Contratada, fica o Contratante autorizado a contratar empresa diversa para executar os reparos, ajustes ou a substituição do bem ou de seus componentes, bem como a exigir do Contratado o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia dos equipamentos.

4.11.10. O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade do Contratado.

4.11.11. A garantia legal ou contratual do objeto tem prazo de vigência própria e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

4.11.12. A CONTRATADA deverá garantir ainda:

- a) Que na execução dos serviços não serão violados quaisquer direitos de titularidade de terceiros;
- b) Que a solução desenvolvida e implantada é original;
- c) Que a utilização pela CONTRATADA da solução desenvolvida em virtude da presente proposta não lesionará qualquer direito de terceiros ou da CONTRATADA, obrigando-se a CONTRATADA a indenizar a(s) Parte(s) prejudicada(s) em caso de violação de quaisquer das garantias acima;
- d) O regular funcionamento das Soluções, desde que mantidas as condições estabelecidas no momento da implantação e desde que as Soluções sejam utilizadas de acordo com os manuais e especificações técnicas a elas referentes.

4.11.13. As manutenções corretivas decorrentes de falhas na prestação de serviço por parte da CONTRATADA serão realizadas sem ônus para AGU. Os demais casos serão de responsabilidade única e exclusiva do AGU.

4.11.14. O direito da AGU é à garantia cessará caso o software ou artefato seja alterado pelo própria CONTRATADA ou por empresa por este autorizada.

4.11.15. A prestação dos serviços relacionados à garantia não deve imputar qualquer custo adicional à AGU.

4.11.16. A modalidade de atendimento deverá ser em regime 12x5 (12h por dia x 5 dias da semana), de segunda a sexta (7h às 19h), excluindo os feriados nacionais.

4.11.17. Para os itens 1 e 2 solução *Spine-Leaf* de Datacenter a modalidade de atendimento deverá ser em regime 24x7 (24h por dia x 7 dias da semana), de segunda a domingo (00h às 23:59h), incluindo os feriados nacionais, pontos facultativos e/ou outras datas festivas.

4.12. Requisitos de Experiência Profissional

4.12.1. A CONTRATADA deverá manter equipe especializada com experiência, formação, certificados pelo fabricante da solução e conhecimento técnico, necessários ao pleno desempenho

dos serviços contratados e deverá dimensionar a equipe necessária para o pleno desempenho dos serviços contratados.

4.12.2. Os serviços de assistência técnica, suporte e garantia deverão ser prestados por profissionais devidamente capacitados e habilitados para o objeto especificado neste TERMO DE REFERÊNCIA, bem como com todos os recursos ferramentais necessários para a prestação dos serviços, impondo-lhes rigoroso padrão de qualidade, segurança e eficiência.

4.13. **Requisitos de Formação da Equipe**

4.13.1. A execução do suporte técnico de garantia e de instalação da solução deve ser realizada pela CONTRATADA por meio de profissional certificado pelo fabricante da solução sem custos adicionais para a AGU, durante o período de garantia, sendo indispensável a apresentação de documentação original do fabricante que comprove a validade da certificação enquanto durar o vínculo contratual, podendo ser solicitada a qualquer momento.

4.14. **Requisitos de Metodologia de Trabalho**

4.14.1. Será realizada reunião Inicial entre a CONTRATANTE e CONTRATADA após assinatura de contrato e previamente a emissão de Ordem de Serviço (OS) ou Ordem de fornecimento de Bens (OFB). Serão realizadas quantas reuniões forem necessárias para discussão de assuntos referentes a execução do contrato.

4.14.2. O fornecimento dos produtos ou a execução dos serviços estão condicionados ao recebimento pelo Contratado de Ordem de Serviço (OS) ou Ordem de fornecimento de Bens (OFB) emitida pela Contratante. A OS/OFB indicará o tipo de serviço ou o tipo de equipamento, a quantidade e a localidade na qual os equipamentos deverão ser entregues.

4.14.3. O andamento do fornecimento dos produtos/serviços deve ser acompanhado pelo Contratado, que dará ciência de eventuais acontecimentos à Contratante.

4.14.4. A AGU realizará a gestão e fiscalização do contrato, bem como o aceite/rejeição das OS/OFB.

4.14.5. O suporte técnico ocorrerá sem nenhum ônus, mesmo quando for necessária a atualização, o traslado e a estada de técnicos da CONTRATADA ou qualquer outro tipo de serviço necessário para garantir o cumprimento dos serviços contratados e demandados.

4.14.6. O atendimento técnico na forma presencial será requerido sempre que necessário e/ou quando ocorrerem falhas ou problemas de funcionamento dos Serviços de responsabilidade da CONTRATADA.

4.14.7. A contratação deverá contemplar o fornecimento padronizado de toda a solução de rede com vistas a estabelecer um padrão de qualidade, compatibilidade, e desonerar o Órgão na instrução e realização de processos licitatórios em separado.

4.14.8. A modernização pretendida deve permitir a AGU agregar disponibilidade, desempenho, gestão, monitoramento, visibilidade e qualidade de serviços a todos os usuários, sendo um salto qualitativo na adoção de soluções que visam atender de forma eficiente e racional à demanda da sociedade.

4.14.9. A empresa contratada deve manter central de atendimento para abertura de chamados em regime 24x7 (24h por dia x 7 dias da semana), de segunda a domingo (00h às 23:59h), incluindo feriados.

4.14.10. Formalizar a AGU, por escrito, quaisquer anormalidades, que ponham em risco o êxito e o cumprimento dos prazos de execução dos serviços, propondo as ações corretivas necessárias.

4.14.11. Informar a AGU quando da necessidade de visita de seus técnicos que precisarem permanecer nas dependências da AGU, para execução da instalação, configuração e testes de equipamentos, bem como para serviço de manutenção, reestruturação, devendo esses serem supervisionados por pessoal técnico indicado pela AGU.

4.14.12. Respeitar as normas e procedimentos de controle de acesso às dependências da AGU.

4.14.13. Cumprir fielmente as obrigações assumidas em contrato, observando todas as especificações técnicas exigidas para a execução dos serviços.

4.14.14. Assegurar à AGU o direito de fiscalizar, sustentar, recusar ou mandar refazer qualquer serviço que não esteja de acordo com a boa técnica, normas, projetos ou especificações, ou que atente contra a segurança de terceiros, ficando acordado que, em nenhuma hipótese, a falta de fiscalização do AGU eximirá o CONTRATADO das suas responsabilidades provenientes do contrato.

4.14.15. Comunicar à AGU qualquer interrupção programada com, no mínimo, 7 (sete) dias de antecedência. A comunicação não importa em suspensão de glosa pela não prestação do serviço.

4.14.16. Será considerado para efeitos do nível de serviço exigido, prazo de solução definitiva, como o tempo decorrido entre a abertura do chamado técnico efetuada pela equipe técnica à CONTRATADA e a efetiva recolocação dos serviços em seu pleno estado de funcionamento.

4.14.17. A contagem do prazo de solução definitiva de cada chamado será a partir da abertura do chamado na Central de Atendimento disponibilizada pela CONTRATADA, até o momento da comunicação da solução definitiva do problema e aceite pela equipe técnica.

4.14.18. Após concluído o chamado, a CONTRATADA comunicará o fato à equipe técnica e solicitará autorização para o fechamento dele.

4.14.19. Os chamados deverão estar disponíveis por meio de relatórios encaminhados mensalmente atendendo aos seguintes tópicos:

- a) Chamados Abertos no Período: Relatório com todas as Ocorrências abertas no mês e o status;
- b) Chamados em Andamento: Relatório onde constam as ocorrências que estão sendo tratadas e qual o status;
- c) Chamados Fechados no Período: Relatório com todos os chamados que foram fechados no mês.

4.14.20. No caso de defeito em equipamento e/ou componentes da solução, **faculta-se à CONTRATADA substituir temporariamente** tais itens por outros de mesmas características técnicas, quando então, a partir de seu pleno estado de funcionamento, ficará suspensa a contagem do prazo de solução definitiva.

4.14.21. O **prazo máximo** para a **substituição temporária** descrita no subitem anterior será de 30 (trinta) dias, sendo que neste prazo o equipamento e/ou componente deverá ser devolvido em perfeito estado de funcionamento.

4.14.22. No caso de **inviabilidade da solução definitiva** do problema apresentado no equipamento e/ou componente, **faculta-se à CONTRATADA promover a substituição em caráter definitivo** por outro equipamento de iguais características técnicas ou superior sem qualquer ônus à AGU.

4.14.23. **A substituição definitiva será admitida com anuência**, após prévia avaliação técnica quanto às condições de uso e compatibilidade do equipamento e/ou componente ofertado, em relação àquele que está sendo substituído.

4.15. Requisitos de Segurança da Informação e Privacidade

4.15.1. As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.

4.15.2. Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do art. 6º da LGPD.

4.15.3. É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.

4.15.4. A Administração deverá ser informada no prazo de 5 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pelo Contratado.

4.15.5. Terminado o tratamento dos dados nos termos do art. 15 da LGPD, é dever do contratado eliminá-los, com exceção das hipóteses do art. 16 da LGPD, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

4.15.6. É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.

4.15.7. O Contratado deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

4.15.8. O Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.

4.15.9. O Contratado deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

4.15.10. Bancos de dados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro individual rastreável de tratamentos realizados (LGPD, art. 37), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.

4.15.11. Os referidos bancos de dados devem ser desenvolvidos em formato interoperável, a fim de garantir a reutilização desses dados pela Administração nas hipóteses previstas na LGPD.

4.15.12. O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

4.15.13. Os contratos e convênios de que trata o § 1º do art. 26 da LGPD deverão ser comunicados à autoridade nacional.

4.16. **Vistoria**

4.16.1. A avaliação prévia do local de execução dos serviços é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, sendo assegurado ao interessado o direito de realização de vistoria prévia, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 8h às 18h, devendo o agendamento ser efetuado previamente pelo endereço eletrônico dti@agu.gov.br, na Advocacia Geral da União - Departamento de Tecnologia da Informação - Setor de Indústrias Gráficas SIG, Quadra 06, Lote 800 – Brasília - DF, CEP: 70610-460, telefones: (61) 2026-7709 e 2026-7807.

4.16.2. Serão disponibilizados data e horário diferentes aos interessados em realizar a vistoria prévia.

4.16.3. O prazo para vistoria iniciar-se-á no dia útil seguinte ao da publicação do Edital, estendendo-se até 24 (vinte e quatro) horas, em dias úteis, antes da data prevista para a abertura da sessão pública.

4.16.4. Para a vistoria, o licitante, ou o seu representante legal, deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.

4.16.5. A **Declaração de Vistoria** integrante deste TERMO DE REFERÊNCIA, nos termos do APÊNDICE “K”, deverá ser assinada pelos representantes da AGU e da Licitante, ou o seu representante legal, comprovando que a empresa realizou a vistoria técnica para conhecimento dos serviços necessários, do ambiente tecnológico da AGU e das condições técnicas para sua realização.

4.16.6. A Licitante deverá apresentar a Declaração de Vistoria impressa em papel timbrado da empresa, em duas vias, em papel A4 e com seus dados e de seu representante legal, devidamente preenchidos.

4.16.7. A Licitante poderá optar pela não realização da vistoria, para tanto deverá apresentar, junto com sua proposta de preços, caso seja a vencedora da etapa de lances, a **Declaração de Recusa de Vistoria**, conforme modelo fornecido, nos termos do APÊNDICE “L”, devidamente assinada por seus representantes legais.

4.16.8. A não realização da vistoria, quando facultativa, não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo o contratado assumir os ônus dos serviços decorrentes.

4.16.9. O prazo para VISTORIA iniciar-se-á no dia útil seguinte ao da publicação do Edital, estendendo-se até o 4º dia útil anterior à data prevista para a abertura da sessão pública. Para a realização da VISTORIA, o licitante e/ou o seu representante, deverão estar devidamente identificados.

4.17. **Outros Requisitos Aplicáveis**

4.17.1. Não se aplica

4.18. **Sustentabilidade**

4.18.1. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis:

a) Só será admitida a oferta que cumpra os critérios de segurança, compatibilidade eletromagnética e eficiência energética, previstos na Portaria nº 170, de 2012 do INMETRO. Só será admitida a oferta de bens de informática e/ou automação que não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr (V1)), cádmio (Cd), bifenil polibromados (PBBs), éteres difenil-polibromados (PBDEs);

b) O conceito de TI verde é definido como um conjunto de práticas que torna mais sustentável e menos prejudicial o uso da tecnologia e está ligado aos processos de fabricação dos componentes, a administração e a utilização dos ativos de TI, bem como o descarte do “lixo eletrônico”. Dentro desse contexto, poderá ser priorizada a utilização de tecnologias de virtualização, as quais podem ser definidas como soluções computacionais que permitem a execução de vários sistemas operacionais e seus respectivos softwares a partir de uma única máquina física. Como benefícios da virtualização podem ser citados o melhor aproveitamento da infraestrutura existente, a redução no consumo de energia elétrica, diminuição na geração

de lixo eletrônico e menor emissão de carbono.

c) Outro critério a ser priorizado nas especificações é a adoção de um plano de descarte ou reuso dos ativos de TI a serem contratados, haja vista que na sua fabricação são usadas substâncias que lhes conferem durabilidade, desempenho e proteção, contudo, quando chegam ao final do seu ciclo de vida esses elementos, tais como mercúrio, chumbo, fósforo e cádmio, podem representar riscos à saúde da natureza e do homem se não forem descartados adequadamente. Também poderá ser priorizada a adoção de processos administrativos na sua forma eletrônica, utilizando softwares aplicativos.

d) Os documentos deverão ser gerados e mantidos em sua forma digital e, com o objetivo de garantir a integridade dos mesmos, nestes poderão ser utilizados recursos tecnológicos de segurança da informação. O objetivo da referida adoção é reduzir o número de cópias e impressões em papel. Portanto, recomenda-se inserir critérios de sustentabilidade ambiental nas especificações técnicas para aquisição de ativos de TI, os quais deverão atender aos requisitos técnicos que propiciam maior eficiência energética, maior vida útil e menor custo de manutenção.

e) Os critérios de sustentabilidade deverão ser fundamentados no desenvolvimento econômico, social e na conservação do meio ambiente, além de serem baseados nas diretrizes de sustentabilidade como menor impacto sobre recursos naturais, preferência para materiais, tecnologias e matérias-primas de origem local e maior eficiência na utilização de recursos naturais como água e energia.

4.19. Indicação de marcas ou modelos (Art. 41, inciso I, da Lei nº 14.133, de 2021)

4.19.1. Não se aplica.

4.20. Da vedação de utilização de marca/produto na execução do serviço

4.20.1. Não se aplica

4.21. Da exigência de carta de solidariedade

4.21.1. Não se aplica.

4.22. Subcontratação

4.22.1. É vedada a subcontratação total ou parcial do objeto, exceto quanto ao fornecimento de materiais, peças e componentes de reposição que poderão ser adquiridas junto a terceiros. Tal ação não exime a CONTRATADA de qualquer responsabilidade por ela assumida no Termo Contratual

4.22.2. É vedada a participação de empresas em consórcio na licitação.

4.22.3. Não se vislumbra necessidade de permissão da participação em consórcio, tendo em vista as características técnicas do objeto.

4.22.4. A vedação de empresas em consórcio não acarretará restrição à competitividade, pois há no mercado diversas empresas prestadoras dos serviços objeto desta contratação, que se encontram aptas a atender as exigências de habilitação previstas neste TERMO DE REFERÊNCIA.

4.23. Da verificação de amostra do objeto

4.23.1. Não se aplica.

4.24. Garantia da Contratação

4.24.1. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, no percentual de 5% (cinco por cento) do valor total do contrato, conforme regras previstas no Contrato.

4.24.2. Em caso de opção pelo seguro-garantia, a parte adjudicatária deverá apresentá-la, no máximo, até a data de assinatura do contrato.

4.24.3. A garantia, nas modalidades caução e fiança bancária, deverá ser prestada em até 10 (dez) dias úteis após a assinatura do contrato.

4.24.4. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

4.25. Informações relevantes para o dimensionamento e apresentação da proposta

4.25.1. A proposta da licitante deverá conter a especificação clara e completa do objeto, obedecida a mesma ordem constante deste TERMO DE REFERÊNCIA, sem conter alternativas de preços, ou de qualquer outra condição que induza o julgamento a ter mais de um resultado, conforme Modelo de Proposta de Preços constante no APÊNDICE "C", deste TERMO DE REFERÊNCIA.

4.25.2. Entende-se por especificação clara e completa do objeto, o detalhamento do objeto, os quantitativos de equipamentos a serem entregues, marcas/modelos de aparelhos/equipamentos a

serem fornecidos, o detalhamento da arquitetura da plataforma, além das características técnicas do objeto, em conformidade com os requisitos técnicos exigidos e demais condições gerais de prestação dos serviços que deverão constar da proposta da licitante.

4.25.3. Não serão aceitas propostas contendo cópia das exigências deste TERMO DE REFERÊNCIA no lugar da especificação clara e inequívoca dos equipamentos a serem adquiridos.

4.25.4. A licitante vencedora deverá apresentar planilha de preços, discriminando os valores total e unitário de cada item.

4.25.5. A proposta da licitante deverá estar integralmente preenchida, discriminando os valores unitários e totais de cada item objeto deste TERMO DE REFERÊNCIA, em conformidade com o modelo constante deste TERMO DE REFERÊNCIA.

4.25.6. A proposta deverá conter declaração da licitante de que se encontra apta a entregar o objeto pertinentes ao ofertado e às regras de negócio envolvidas.

4.25.7. A demanda do órgão tem como base ainda as seguintes características:

4.25.8. Switches Datacenter Spine-Leaf: A necessidade contempla 2 (dois) elementos SPINE em cada um dos 2 (dois) datacenters da AGU em Brasília (Sedes I e II) totalizando 4 (quatro) equipamentos tipo 1 SPINE;

4.25.9. Switches Datacenter Spine-Leaf: A necessidade contempla 10 (dez) Switches LEAF Tipo 2 no Datacenter Sede II. No Datacenter Sede I totalizam 4 (quatro) Switches tipo 2 LEAF;

4.25.10. Switches Acesso/Borda: A necessidade contempla 230 (duzentos e trinta) elementos Tipo 3 para atendimento das necessidades das unidades da AGU;

4.25.11. Switches Acesso/Borda: A necessidade contempla 100 (cem) elementos Tipo 4 para atendimento das necessidades das unidades da AGU;

4.25.12. Access Point 4x4: A necessidade contempla 160 (cento e sessenta) elementos Tipo 1 para atendimento das necessidades das unidades da AGU;

4.25.13. Access Point 2x2: A necessidade contempla 550 (quinhentos e cinquenta) elementos Tipo 2 para atendimento das necessidades das unidades da AGU;

4.25.14. A solução deverá ser gerida por uma solução redundante de gerência, do mesmo fabricante, com todas as funcionalidades elencadas nas especificações técnicas disponíveis;

4.25.15. A solução de segurança que provê o controle de acesso à rede (NAC) deverá estar licenciada por usuários simultâneos e ser do mesmo fabricante.

5. PAPÉIS E RESPONSABILIDADES

5.1. São obrigações da CONTRATANTE:

5.1.1. Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

5.1.2. 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;

5.1.3. Receber o objeto fornecido pelo contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

5.1.4. Aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

5.1.5. Liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

5.1.6. Comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

5.1.7. Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do contratado, com base em pesquisas de mercado, quando aplicável;

5.1.8. Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer;

5.2. São obrigações da CONTRATADA

5.2.1. Indicar formalmente preposto apto a representá-la junto à contratante, que deverá responder pela fiel execução do contrato;

5.2.2. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

5.2.3. 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;

5.2.4. 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, desde que motivadas as causas e justificativas desta decisão;

5.2.5. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

5.2.6. Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

5.2.7. Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

5.2.8. 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;

5.2.9. Fazer a transição contratual, quando for o caso;

5.3. **São obrigações do órgão gerenciador do registro de preços**

5.3.1. efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços;

5.3.2. conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;

5.3.3. definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:

5.3.3.1. as formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível; e

5.3.3.2. definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável;

5.3.4. definir mecanismos de controle de fornecimento da solução de TIC, observando, dentre outros:

- 5.3.4.1. a definição da produtividade ou da capacidade mínima de fornecimento da solução de TIC;
- 5.3.4.2. as regras para gerenciamento da fila de fornecimento da solução de TIC aos órgãos participantes e não participantes, contendo prazos e formas de negociação e redistribuição da demanda, quando esta ultrapassar a produtividade definida ou a capacidade mínima de fornecimento e for requerida pelo contratado; e
- 5.3.4.3. as regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a verificação de Amostra do Objeto, observado o disposto no inciso III, alínea "c", item 2 do art. 17 da Instrução Normativa SGS/ME nº 94, de 2022, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica.
- 5.3.4.4. Caberá à AGU, como órgão gerenciador da Ata de Registro de Preços, as responsabilidades elencadas no Decreto nº 11.462/23, que regulamenta o Sistema de Registro de Preços.
- 5.3.4.5. Dentre as competências da AGU, destaca-se o procedimento de Intenção de Registro de Preços, antes de iniciar o procedimento licitatório, consultar a IRP em andamento e deliberar a respeito da conveniência de sua participação.
- 5.3.5. A dispensa da divulgação da intenção de registro de preços encontra amparo no Decreto 11.462, de 31 de março de 2023, art. 9º, parágrafo 2º, conforme transcrito a seguir:

Art. 9º Para fins de registro de preços, o órgão ou a entidade gerenciadora deverá, na fase preparatória do processo licitatório ou da contratação direta, realizar procedimento público de IRP para possibilitar, pelo prazo mínimo de oito dias úteis, a participação de outros órgãos ou outras entidades da Administração Pública na ata de registro de preços e determinar a estimativa total de quantidades da contratação, observado, em especial, o disposto nos incisos III e IV do caput do art. 7º e nos incisos I, III e IV do caput do art. 8º.

(...)

§ 2º O procedimento previsto no caput poderá ser dispensado quando o órgão ou a entidade gerenciadora for o único contratante.

- 5.3.5.1. O Sistema de Registro de Preços visa atender a necessidade de contratação de solução de rede unificada incluindo instalação, configuração, suporte técnico e garantia para a AGU, cujo o projeto foi construído exclusivamente para atender demandas específicas da infraestrutura tecnológica da AGU, conforme suas características e complexidade, para diagnóstico situacional do ambiente de infraestrutura e de sistemas de TI, visando identificar riscos e conformidades, dentre outras atividades,

possibilitando a melhoria na Gestão/Governança de TIC da AGU, verifica-se a necessidade de dispensa da divulgação da intenção de registro de preços.

5.3.6. Desta forma, considerando as características da contratação, não será admitida a adesão à ata de registro de preços decorrente da licitação.

6. MODELO DE EXECUÇÃO DO CONTRATO

6.1. Condições de execução

6.1.1. Do encaminhamento Formal de Demandas

6.1.1.1. O gestor do contrato emitirá a Ordem de fornecimento de bens (OFB)/ Ordem de Serviço (OS) para a entrega dos bens desejados.

6.1.1.2. O Contratado deverá fornecer equipamentos com as mesmas configurações e quantidades definidas na OFB.

6.1.1.3. Os bens serão recebidos provisoriamente, quando da entrega integral do objeto (incluindo todas as parcelas), pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste TERMO DE REFERÊNCIA e na proposta.

6.1.1.4. Os bens serão recebidos definitivamente no prazo de 15 dias úteis, contados do recebimento provisório, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo circunstanciado, desde que estejam de acordo com os critérios de aceitação constante no subitem 7.10 deste TERMO DE REFERÊNCIA.

6.1.2. O objeto do contrato será prestado nos endereços da AGU dispostos no APÊNDICE 'B' deste TERMO DE REFERÊNCIA.

6.2. Forma de execução e acompanhamento do contrato

6.2.1. Condições de entrega

6.2.1.1. O prazo de entrega dos bens é de 90 (noventa) dias corridos contados da data de emissão da Ordem de Fornecimento de Bens (OFB).

6.2.1.2. Caso não seja possível a entrega na data assinalada, a empresa deverá comunicar as razões respectivas com pelo menos 30 (trinta) dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

6.2.1.3. Disponibilização formal, pela contratada, dos canais para suporte (no mínimo e-mail, sistema de chamados e telefone): em até 2 (dois) dias, contados da data da ativação do serviço de conectividade; e

6.2.1.4. Cumprimento dos prazos relativos aos níveis mínimos de serviços deste documento.

6.3. Local e horário da entrega dos bens e da prestação dos serviços

6.3.1. Os bens deverão ser entregues nos endereços constantes no APÊNDICE “B” deste TERMO DE REFERÊNCIA.

6.3.2. Os bens deverão ser entregues no horário constante no APÊNDICE “A” deste TERMO DE REFERÊNCIA.

6.4. Materiais a serem disponibilizados

6.4.1. Não se aplica.

6.5. Informações relevantes para o dimensionamento da proposta

6.5.1. A CONTRATADA deverá assegurar, durante a vigência do CONTRATO, assistência técnica on-site (no local quando necessário) ou remota, preventiva e corretiva total dos equipamentos, da solução de gerenciamento, incluindo-se todas as ações, sejam de manutenção, reposição de peças, instalação, configuração, remanejamento e alteração da localização de equipamentos, ou outras necessárias, com vistas a garantir o correto funcionamento dos mesmos, assim como o atendimento às necessidades da AGU, de acordo com os requisitos da contratação e os seguintes níveis mínimos de serviço exigidos.

6.5.2. Demais aspectos relevantes para o correto dimensionamento e cotejo da proposta de preços constam no APÊNDICE “A” – Especificações Técnicas da Solução.

6.6. Especificação da garantia do serviço (art. 40, §1º, inciso III, da Lei nº 14.133, de 2021)

6.6.1. O prazo de garantia contratual dos serviços é aquele estabelecido na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor).

6.7. Do preposto da contratada

6.7.1. A CONTRATADA deverá indicar preposto (*account manager*), que será responsável por acompanhar a execução do CONTRATO e atuar como interlocutor administrativo principal junto ao CONTRATANTE incumbido de receber, diligenciar, encaminhar e responder às questões legais e administrativas referentes à execução contratual.

6.7.2. A demanda da AGU tem como base as seguintes características técnicas:

- a) Redução no tempo de indisponibilidade dos serviços, através do tempo para recuperação de falhas nos equipamentos;
- b) Redução nos riscos de interrupção dos serviços, com a identificação prévia de potenciais problemas e adoção de ações preventivas em tempo hábil;
- c) Acesso irrestrito e conexão direta com a equipe de suporte do contratado para abertura e controle de chamados;
- d) Atualização de componentes físicos e lógicos para versões mais recentes, permitindo a manutenção da compatibilidade com os diversos produtos existentes ou que vierem a existir no ambiente computacional da AGU e o aumento da vida útil da solução.

6.8. Formas de transferência de conhecimento

6.8.1. A transferência do conhecimento deverá ser realizada observando-se o que segue:

6.8.1.1. Toda e qualquer informação produzida no âmbito da execução do objeto do contrato pela empresa prestadora dos serviços será de propriedade da AGU e fica a CONTRATADA obrigada a documentar e registrar os produtos, serviços e eventos.

6.8.1.2. Será de inteira responsabilidade da CONTRATADA garantir o repasse bem-sucedido de todas as informações necessárias para a continuidade dos serviços pela AGU ou empresa por ela designada.

6.9. Procedimentos de transição e finalização do contrato

6.9.1. Os procedimentos de transição e finalização do contrato constituem-se das seguintes etapas:

6.9.1.1. A TRANSIÇÃO CONTRATUAL inicial, a fim de preparar o CONTRATADO a assumir integralmente as obrigações advindas com o CONTRATO, deverá ser viabilizada sem ônus adicional a AGU, e será baseada em reuniões técnicas e repasse de documentos e/ou manuais específicos das soluções desenvolvidas.

6.9.1.2. O processo de TRANSIÇÃO CONTRATUAL se inicia a partir do momento em que o CONTRATADO assume as responsabilidades, de forma gradual, pelos serviços prestados, preparando-se para o início efetivo da operação. A execução dessa etapa de repasse dos serviços deverá ser finalizada em no máximo 30 (trinta) dias corridos a partir do início da prestação dos serviços.

EVENTOS DE TRANSIÇÃO CONTRATUAL			
EVENTO	PRAZO DE REFERÊNCIA	DESCRIÇÃO	RESPONSABILIDADE
E ₁	-	Assinatura do CONTRATO	AGU / CONTRATADO
E ₂	E ₁ + 10 dias	Apresentação da GARANTIA CONTRATUAL	CONTRATADO
E ₃	E ₁ + 5 dias	REUNIÃO INICIAL	AGU / CONTRATADO
E ₄	E ₁ + 10 dias	Apresentação do PLANO DE IMPLANTAÇÃO	CONTRATADO
E ₅	E ₃ + 10 dias	Início da execução do CONTRATO e implantação da solução	CONTRATADO
E ₆	E ₄ + 30 dias	Encerramento da TRANSIÇÃO CONTRATUAL	CONTRATADO

6.9.1.3. No caso da finalização do contrato, a CONTRATADA deverá prestar à AGU toda a assistência necessária à continuidade dos serviços prestados.

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

6.10.1. Não se aplica

6.11. Mecanismos formais de comunicação

6.11.1. São definidos como mecanismos formais de comunicação, entre a Contratante e o Contratado, os seguintes:

- Ordem de Fornecimento de Bens (OFB);
- Termos de Recebimento;
- Ofício;
- Relatórios e Atas de Reunião;
- E-mail institucional/corporativo;
- Ferramenta Microsoft Teams ou similar em uso pela AGU;
- SUPER SAPIENS - (<https://supersapiens.agu.gov.br/auth/login>);
- Sistema de abertura de chamados;
- Demais Termos previstos no instrumento convocatório.

6.12. Formas de Pagamento

6.12.1. Os critérios de medição e pagamento dos serviços prestados serão tratados no item 8. deste TERMO DE REFERÊNCIA.

6.13. Manutenção de Sigilo e Normas de Segurança

6.13.1. O Contratado 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.

6.13.2. O Termo de Compromisso e Manutenção de Sigilo, APÊNDICE "H", contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal do Contratado, e o Termo de Ciência, APÊNDICE "I", bem como a Declaração de Ciência e Consentimento da LGPD, APÊNDICE "J", deverão ser assinados por todos os empregados da Contratada diretamente envolvidos na contratação.

7. MODELO DE GESTÃO DO CONTRATO

7.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

7.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

7.3. As comunicações entre o órgão ou entidade e o contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

7.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

7.5. Reunião Inicial

7.5.1. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.

7.5.2. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em até 15 (quinze) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.

7.5.3. A pauta desta reunião observará, pelo menos:

- a) Presença do representante legal da contratada, que apresentará o seu preposto;
- b) Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;
- c) esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;
- d) A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à Contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;
- e) Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste TERMO DE REFERÊNCIA.

7.6. **Fiscalização**

7.6.1. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput) , nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

7.7. **Fiscalização Técnica**

7.7.1. O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

7.7.1.1. O fiscal técnico do contrato anotar no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º, e Decreto nº 11.246, de 2022, art. 22, II);

7.7.1.2. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);

7.7.1.3. O fiscal técnico do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV).

7.7.1.4. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. (Decreto nº 11.246, de 2022, art. 22, V).

7.7.1.5. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

7.8. Fiscalização Administrativa

7.8.1. O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação do contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

7.8.2. Caso ocorram descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; (Decreto nº 11.246, de 2022, art. 23, IV).

7.9. Gestor do Contrato

7.9.1. O gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022, coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. (Decreto nº 11.246, de 2022, art. 21, IV).

7.9.2. O gestor do contrato acompanhará a manutenção das condições de habilitação do contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

7.9.3. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (Decreto nº 11.246, de 2022, art. 21, II).

7.9.4. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Decreto nº 11.246, de 2022, art. 21, VIII).

7.9.5. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).

7.9.6. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou prorrogação contratual. (Decreto nº 11.246, de 2022, art. 22, VII).

7.9.7. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Decreto nº 11.246, de 2022, art. 21, VI).

7.9.8. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

7.10. Critérios de Aceitação

7.10.1. A avaliação da qualidade dos produtos entregues, para fins de aceitação, consiste na verificação dos critérios relacionados a seguir:

7.10.1.1. Todos os equipamentos fornecidos deverão ser novos (incluindo todas as peças e componentes presentes nos produtos), de primeiro uso (sem sinais de utilização anterior), não reconicionados e em fase de comercialização normal através dos canais de venda do fabricante no Brasil (não serão aceitos produtos end-of-life).

7.10.1.2. Todos os componentes do(s) equipamento(s) e respectivas funcionalidades deverão ser compatíveis entre si, sem a utilização de adaptadores, frisagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos não previstos nas especificações técnicas ou, ainda, com emprego de materiais inadequados ou que visem adaptar forçadamente o produto ou suas partes que sejam fisicamente ou logicamente incompatíveis.

7.10.1.3. Todos os componentes internos do(s) equipamento(s) deverá(ão) estar instalado(s) de forma organizada e livres de pressões ocasionados por outros componentes ou cabos, que possam causar desconexões, instabilidade, ou funcionamento inadequado.

7.10.1.4. O número de série de cada equipamento deve ser obrigatório e único, afixado em local visível, na parte externa do gabinete e na embalagem que o contém. Esse número deverá ser identificado pelo fabricante, como válido para o produto entregue e para as condições do mercado brasileiro no que se refere à garantia e assistência técnica no Brasil.

7.10.1.5. Serão recusados os produtos que possuam componentes ou acessórios com sinais claros de oxidação, danos físicos, sujeira, riscos ou outro sinal de desgaste, mesmo sendo o componente ou acessório considerado como novos pelo fornecedor dos produtos.

7.10.1.6. Os produtos, considerando a marca e modelo apresentados na licitação, não poderão estar fora de linha comercial, considerando a data de LICITAÇÃO (abertura das propostas). Os produtos devem ser fornecidos completos e prontos para a utilização, com todos os acessórios, componentes, cabos etc.

7.10.1.7. Todas as licenças, referentes aos softwares e drivers solicitados, devem estar registrados para utilização do Contratante, em modo definitivo (licenças perpétuas), legalizado, não sendo admitidas versões “shareware” ou “trial”. O modelo do produto ofertado pelo licitante deverá estar em fase de produção pelo fabricante (no Brasil ou no exterior), sem previsão de encerramento de produção, até a data de entrega da proposta.

7.10.1.8. A Contratante poderá optar por avaliar a qualidade de todos os equipamentos fornecidos ou uma amostra dos equipamentos, atentando para a inclusão nos autos do processo administrativo de todos os documentos que evidenciem a realização dos testes de aceitação em cada equipamento selecionado, para posterior rastreabilidade.

7.10.1.9. Só haverá o recebimento definitivo, após a análise da qualidade dos bens e/ou serviços, em face da aplicação dos critérios de aceitação, resguardando-se ao Contratante o direito de não

receber o OBJETO cuja qualidade seja comprovadamente baixa ou em desacordo com as especificações definidas neste TERMO DE REFERÊNCIA – situação em que poderão ser aplicadas à Contratada as penalidades previstas em lei, neste TERMO DE REFERÊNCIA e no Contrato. Quando for o caso, a empresa será convocada a refazer todos os serviços rejeitados, sem custo adicional.

7.11. Procedimentos de Teste e Inspeção

7.11.1. A AGU poderá, se julgar necessário, realizar inspeções e diligências a fim de garantir que a licitante vencedora esteja em condições de fornecer os equipamentos pretendidos de acordo com a qualidade exigida.

7.12. Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

7.12.1. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela contratante, conforme a tabela abaixo:

Id	Ocorrência	Glosa / Sanção
1	Não prestar os esclarecimentos imediatamente, referente à execução dos serviços, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de (24) horas úteis.	Multa de 1 % sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela contratante, até o limite de 10 dias úteis. Após o limite de 10 dias úteis, aplicar-se-á multa de 3 % do valor total do Contrato.
2	Descumprimento de prazos estabelecidos neste TERMO DE REFERÊNCIA.	Para atrasos de até 10 (dez) dias corridos → multa de 0,1% (um décimo por cento) ao dia do valor total do respectivo Contrato. Para atrasos superiores a 10 (dez) dias corridos → a multa descrita na alínea “a” será substituída por multa de 0,25% (vinte e cinco centésimos por cento) ao dia, até o limite máximo de 5% (cinco por cento) do valor total do respectivo Contrato.
3	Descumprimento de prazos na entrega dos produtos adquiridos.	Para atrasos de até 15 (quinze) dias corridos → multa de 0,2% (dois décimos por cento) ao dia do valor total dos produtos adquiridos. Para atrasos superiores a 15 (quinze) dias corridos → a multa descrita na alínea “a” será substituída por multa de 0,5% (cinco décimos por cento) ao dia, até o limite máximo de 10% (dez por cento) do valor total dos produtos adquiridos.
4	Descumprimento de prazos na entrega dos serviços de instalação.	Para atrasos de até 10 (dez) dias corridos → multa de 0,2% (dois décimos por cento) ao dia do valor total do item Instalação;

		Para atrasos superiores a 10 (dez) dias corridos → a multa descrita na alínea “a” será substituída por multa de 0,5% (cinco décimos por cento) ao dia, até o limite máximo de 10% (dez por cento) do valor total do item Instalação.
5	Dar causa à inexecução parcial do contrato.	Advertência. Em caso de reincidência, aplicar-se-á multa de 2% sobre o valor total do Contrato.
6	Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo.	A Contratada será impedida de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
7	Dar causa à inexecução total do contrato.	A Contratada será impedida de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
8	Deixar de entregar a documentação exigida para o certame.	A Contratada será impedida de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
9	Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado.	A Contratada será impedida de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
10	Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta.	A Contratada será impedida de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
11	Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado.	A Contratada será impedida de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
12	Apresentar declaração ou documentação falsa exigida para o certame ou prestar	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, pelo prazo mínimo de 3 (três) anos e máximo de 6

	declaração falsa durante a licitação ou a execução do contrato.	(seis) anos, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021. Após o limite de 7 dias úteis, aplicar-se-á multa de 10% do valor total do Contrato.
13	Fraudar a licitação ou praticar ato fraudulento na execução do contrato.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
14	Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
15	Praticar atos ilícitos com vistas a frustrar os objetivos da licitação.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
16	Praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
17	Não atender ao indicador de nível de serviço IAE (Indicador de Atraso de Entrega de OS)	Glosa de 0,5% sobre o valor da OS para valores do indicador IAE de 0,11 a 0,20. Glosa de 0,75% sobre o valor da OS para valores do indicador IAE de 0,21 a 0,30. Glosa de 1% sobre o valor da OS para valores do indicador IAE de 0,31 a 0,50. Glosa de 1,5% sobre o valor da OS para valores do indicador IAE de 0,51 a 1,00. Multa de 10% sobre o valor do Contrato e Glosa de 3% sobre o valor da OS, para valores do indicador IAE maiores que 1,00.
18	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	Advertência. Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de 3% do valor total do Contrato.

7.12.2. Nos termos do art. 19, inciso III da Instrução Normativa SGD/ME nº 94, de 2022, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, nos casos em que p contratado:

7.12.2.1. não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou

7.12.2.2. deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada;

7.12.3. Advertência

7.12.3.1. A sanção de advertência consiste em uma comunicação formal à CONTRATADA, após a instauração do processo administrativo sancionador, sendo aplicada quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves – assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado.

7.12.4. A advertência deve conter o apontamento do fato gerador, determinando que seja sanada a impropriedade e notificando que, em caso de reincidência, sanção mais elevada poderá ser aplicada.

8. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

8.1. A avaliação da execução do objeto utilizará o Instrumento de Medição de Resultado (IMR), conforme disposto neste item.

8.2. Níveis mínimos de serviço exigidos:

8.2.1. Deverão ser considerados os seguintes prazos e níveis de severidade para os chamados de Suporte Técnico:

PRAZOS PARA SOLUÇÃO DAS OCORRÊNCIAS REGISTRADAS (a partir do registro da ocorrência)	
SEVERIDADE INFORMADA	TEMPO PARA SOLUÇÃO
1	4 Horas úteis
2	24 Horas úteis
3	72 Horas úteis
4	48 Horas úteis

8.2.2. **Severidade 1** – quando ocorre a perda ou paralisação de serviços relevantes prestados pela AGU ou atividades exercidas pela mesma, configurando-se como situação de emergência. Uma solicitação de serviço de Severidade 1 pode possuir uma ou mais das seguintes características:

8.2.2.1. Dados corrompidos;

8.2.2.2. Sem conectividade;

8.2.2.3. Uma função crítica não está disponível;

8.2.2.4. O sistema se desliga repentinamente causando demoras excessivas e intermitências para utilização de recursos;

8.2.2.5. O sistema falha repetidamente após tentativas de reinicialização;

8.2.2.6. O sistema continua em execução permanente (congelado) necessitando ser reiniciado.

8.2.2.7. Falha crítica de componente de hardware.

8.2.3. **Severidade 2** – quando se verifica uma grave perda de funcionalidade, no entanto, sem interromper os serviços prestados pela AGU ou atividades exercidas pela mesma.

8.2.4. **Severidade 3** – quando se verifica uma perda de menor relevância de funcionalidades, causando apenas inconveniências para a devida prestação dos serviços pela AGU ou a realização de atividades exercidas pela mesma.

8.2.5. **Severidade 4** – quando se verifica como necessária a prestação de informações, aperfeiçoamentos ou esclarecimentos sobre documentação ou funcionalidades, porém sem prejudicar diretamente a devida prestação dos serviços pela AGU ou a realização de atividades exercidas pela mesma.

8.2.6. O nível de severidade será atribuído pela AGU no momento da abertura do chamado. Considerando que as soluções das ocorrências de software, pela sua natureza, podem envolver atividades relacionadas ao desenvolvimento de patches específicos, admite-se, para todos os casos, a adoção de solução de contorno (workaround), respeitados os prazos definidos para cada severidade informada, sem prejuízo da disponibilização da solução definitiva cabível. Neste caso, a partir do encerramento do chamado original, com a disponibilização da solução de contorno, a CONTRATADA deverá abrir uma nova ocorrência para provimento da solução definitiva imediatamente, na qual deverá constar, obrigatoriamente, um novo campo contendo o número do chamado original (encerrado com a solução de contorno). O prazo máximo para disponibilização da solução definitiva será:

PRAZOS PARA SOLUÇÃO DEFINITIVA
(a partir do encerramento do chamado original, com a disponibilização da solução de contorno)

SEVERIDADE INFORMADA	TEMPO PARA SOLUÇÃO
1	15 dias corridos
2	30 dias corridos
3	45 dias corridos

8.2.7. Considerando solução de ocorrências de hardware: caso se esgote o prazo de solução da ocorrência, sem que seja sanado o defeito reclamado, a CONTRATADA deverá providenciar a substituição do equipamento ou módulo defeituoso por outro, em caráter definitivo dentro do prazo máximo de 12 (doze) horas corridas, contadas a partir da expiração do prazo de solução.

8.2.8. Considerando a solução de ocorrências de hardware, a substituição dos módulos ou equipamentos defeituosos deverá utilizar módulos ou equipamentos novos e originais, recomendados pelo fabricante. Após a substituição, a CONTRATADA deverá entregar um documento onde constem as descrições e os números de série dos módulos ou equipamentos defeituosos e dos novos (de substituição).

8.2.9. Para fins de cálculo do período decorrido para solução da ocorrência de software, será contabilizado o prazo entre a formalização e o fechamento efetivo da ocorrência – seja essa solução de caráter definitivo ou provisório com a disponibilização de solução de contorno (workaround).

8.2.10. Para fins de cálculo do período decorrido para solução da ocorrência de hardware, será contabilizado o prazo entre a formalização e o fechamento efetivo da ocorrência. Nos casos em que houver a substituição do módulo ou equipamento defeituoso para a solução da ocorrência, o seu fechamento efetivo se dará somente após a entrada em operação do novo módulo ou equipamento (de substituição).

8.2.11. Entende-se como substituição do módulo ou equipamento defeituoso, a desativação e remoção física do módulo ou equipamento defeituoso, seguida da ativação física e lógica do módulo ou equipamento novo (de substituição), reestabelecendo completamente o serviço que o mesmo atendia antes da ocorrência.

8.2.12. Em caso de impossibilidade da disponibilização de solução de contorno ou definitiva das ocorrências de software, dentro dos prazos estabelecidos, a CONTRATADA deverá, ainda dentro

destes prazos, emitir um parecer com previsão de novo prazo, contendo o histórico de maior abrangência possível das atividades desenvolvidas desde a abertura do respectivo chamado.

8.2.13. Após avaliação deste parecer inicial, a AGU decidirá sobre a periodicidade da emissão de pareceres ou laudos posteriores, até o fechamento do atendimento, sem prejuízo da aplicação das penalidades previstas pelo descumprimento dos prazos estabelecidos neste TERMO DE REFERÊNCIA.

8.3. Recebimento do Objeto

8.3.1. Os serviços serão recebidos provisoriamente, no prazo de 15 (quinze) dias, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. (Art. 140, I, a, da Lei nº 14.133 e Arts. 22, X e 23, X do Decreto nº 11.246, de 2022).

8.3.2. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda do contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.

8.3.3. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico. (Art. 22, X, Decreto nº 11.246, de 2022).

8.3.4. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo. (Art. 23, X, Decreto nº 11.246, de 2022)

8.3.5. O fiscal setorial do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo.

8.3.6. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato.

8.3.7. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou

única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

8.3.8. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório. (Art. 119 c/c art. 140 da Lei nº 14133, de 2021)

8.3.9. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

8.3.10. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste TERMO DE REFERÊNCIA e na proposta, sem prejuízo da aplicação das penalidades.

8.3.11. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

8.3.12. Os serviços serão recebidos definitivamente no prazo de 15 (quinze) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

8.3.13. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento (art. 21, VIII, Decreto nº 11.246, de 2022).

8.3.14. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à Contratada, por escrito, as respectivas correções;

8.3.15. Emitir Termo Circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e

8.3.16. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

8.3.17. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

8.3.18. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que concerne à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

8.3.19. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

8.3.20. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

8.4. Procedimentos de Teste e Inspeção

8.4.1. Os equipamentos serão recebidos após a avaliação e realização dos testes necessários e a verificação do seu funcionamento, conforme exigências deste documento.

8.5. Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

8.5.1. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela contratante, conforme a tabela abaixo:

Id	Ocorrência	Glosa / Sanção
1	Dar causa à inexecução parcial do contrato.	Advertência. Em caso de reincidência, aplicar-se-á multa de 2% sobre o valor total do Contrato.
2	Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo.	A Contratada será impedida de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
3	Dar causa à inexecução total do contrato.	A Contratada será impedida de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.

4	Deixar de entregar a documentação exigida para o certame.	A Contratada será impedida de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
5	Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado.	A Contratada será impedida de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
6	Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta.	A Contratada será impedida de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
7	Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado.	A Contratada será impedida de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
8	Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021. Após o limite de 7 dias úteis, aplicar-se-á multa de 10% do valor total do Contrato.
9	Fraudar a licitação ou praticar ato fraudulento na execução do contrato.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
10	Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
11	Praticar atos ilícitos com vistas a frustrar os objetivos da licitação.	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, sem prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
12	Praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013 .	A Contratada será declarada inidônea para licitar ou contratar com a Administração Pública, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, sem

		prejuízo das demais penalidades previstas na Lei nº 14.133, de 2021.
13	Não atender ao indicador de nível de serviço IAE (Indicador de Atraso de Entrega de OS)	Glosa de 0,5% sobre o valor da OS para valores do indicador IAE de 0,11 a 0,20. Glosa de 0,75% sobre o valor da OS para valores do indicador IAE de 0,21 a 0,30. Glosa de 1% sobre o valor da OS para valores do indicador IAE de 0,31 a 0,50. Glosa de 1,5% sobre o valor da OS para valores do indicador IAE de 0,51 a 1,00. Multa de 10% sobre o valor do Contrato e Glosa de 3% sobre o valor da OS, para valores do indicador IAE maiores que 1,00.
N	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	Advertência. Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de 3% do valor total do Contrato.

8.5.2. Nos termos do art. 19, inciso III da Instrução Normativa SGD/ME nº 94, de 2022, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, nos casos em que o contratado:

8.5.2.1. não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou

8.5.2.2. deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada.

8.6. Liquidação

8.6.1. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de 30 (trinta) dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022.

8.6.2. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

8.6.3. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

- a) o prazo de validade;
- b) a data da emissão;
- c) os dados do contrato e do órgão contratante;
- d) o período respectivo de execução do contrato;
- e) o valor a pagar; e
- f) eventual destaque do valor de retenções tributárias cabíveis.

8.6.4. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao contratante;

8.6.5. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado 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. 68 da Lei nº 14.133, de 2021.

8.6.6. A Administração deverá realizar consulta ao SICAF para:

- a) verificar a manutenção das condições de habilitação exigidas no edital;
- b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

8.6.7. Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, 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 do contratante.

8.6.8. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, 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.

8.6.9. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

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

8.7. Prazo de pagamento

8.7.1. O pagamento será efetuado no prazo de até 20 (vinte) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

8.7.2. No caso de atraso pelo Contratante, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice de Custo de Tecnologia da Informação (ICTI), de correção monetária.

8.8. Forma de pagamento

8.8.1. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

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

8.8.3. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

8.8.4. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

8.8.5. O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

8.9. Antecipação de pagamento

8.9.1. Não será admitida antecipação de pagamento.

8.10. Cessão de crédito

8.10.1. É admitida a cessão fiduciária de direitos creditícios com instituição financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de Julho de 2020, conforme as regras deste tópico.

8.10.2. As cessões de crédito não fiduciárias dependerão de prévia aprovação do contratante.

8.10.3. A eficácia da cessão de crédito, de qualquer natureza, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.

8.10.4. Sem prejuízo do regular atendimento da obrigação contratual de cumprimento de todas as condições de habilitação por parte do contratado (cedente), a celebração do aditamento de cessão de crédito e a realização dos pagamentos respectivos também se condicionam à regularidade fiscal e trabalhista do cessionário, bem como à certificação de que o cessionário não se encontra impedido de licitar e contratar com o Poder Público, conforme a legislação em vigor, ou de receber benefícios ou incentivos fiscais ou creditícios, direta ou indiretamente, conforme o art. 12 da Lei nº 8.429, de 1992, tudo nos termos do Parecer JL-01, de 18 de maio de 2020.

8.10.5. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração.

8.10.6. A cessão de crédito não afetará a execução do objeto contratado, que continuará sob a integral responsabilidade do contratado.

9. FORMA E CRITÉRIO DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

9.1. Forma de seleção e critério de julgamento da proposta

9.1.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO ELETRÔNICO, com adoção do critério de julgamento pelo menor preço, para registro de preços, em observância às hipóteses previstas no art. 3º, II, do Decreto nº 11.462/2023.

9.2. Da Motivação para o Registro de Preços

9.2.1. A adoção do Sistema de Registro de Preços é justificada com base no art. 3º, II, do Decreto nº 11.462/2023 que menciona o cabimento de registro de preços quando for conveniente a aquisição

de bens com previsão de entregas parceladas. Dessa forma, considerando a quantidade e tipos de itens que compõem a solução, entende-se haver compatibilidade com as hipóteses previstas no Decreto nº 11.462/2023.

9.2.2. As características e o vulto da aquisição ora proposta requerem medidas técnico-administrativas eficientes na garantia de que a Administração não venha prescindir dos serviços devido à falta de soluções de necessidade básica, assim como ocorra o uso racional, proativo e menos onerosa dos escassos recursos e da infraestrutura existente. Por esta razão, o Sistema de Registro de Preços (SRP) torna-se o sistema de contratação pública mais eficiente à pretensão.

9.2.3. Desta forma, deverá ser adotada a opção pelo Sistema de Registro de Preços, regulamentado pelo Decreto nº 11.462, e instituído pelo art. 82 a 86 da Lei nº 14.133/21, dispõe sobre o sistema de registro de preços para a contratação de bens e serviços, inclusive obras e serviços de engenharia, no âmbito da Administração Pública federal direta, autárquica e fundacional.

Art. 40. O planejamento de compras deverá considerar a expectativa de consumo anual e observar o seguinte:

- I - Condições de aquisição e pagamento semelhantes às do setor privado;
- II - Processamento por meio de sistema de registro de preços, quando pertinente;

9.2.4. A adoção do Sistema de Registro de Preços é justificada com base no art. 3º do Decreto nº 11.462/23, em seus incisos I e IV. A parte final do inciso I alude ao cabimento de Registro de Preços quando, houver necessidade de contratações frequentes. Já o inciso IV trata da hipótese de cabimento do Registro de Preço quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.

9.2.5. Considerando-se que o objeto da contratação se trata de recurso de contratação de solução de rede unificada incluindo instalação, configuração, suporte técnico e garantia para a AGU por meio da inserção de novas tecnologias no ambiente organizacional da AGU, essencial à garantia da sustentação, e atendimento das necessidades da AGU, de forma a atender aos objetivos institucionais, que visa a implantação de uma solução de solução de rede unificada incluindo instalação, configuração, suporte técnico e garantia para a AGU, que por trata-se de uma demanda de difícil quantificação, pois o crescimento dos serviços em nuvem, não ocorre de forma linear, impede que seja possível definir previamente o volume de trabalho a ser desenvolvido na AGU e o quantidade de licenças serem demandados, para suprir as necessidades das áreas, e, desta forma, entende-se haver plena compatibilidade entre tais fatos e as hipóteses previstas no art. 3º do Decreto nº 11.462/23, que regulamenta o Sistema de Registro de Preços, previsto no art. 82 a 86 da Lei nº 14.133/21.

Art. 3º O SRP poderá ser adotado quando a Administração julgar pertinente, em especial:

- I - Quando, pelas características do objeto, houver necessidade de contratações permanentes ou frequentes;
- II - Quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida, como quantidade de horas de serviço, postos de trabalho ou em regime de tarefa;
- III - quando for conveniente para atendimento a mais de um órgão ou a mais de uma entidade, inclusive nas compras centralizadas;
- IV - Quando for atender a execução descentralizada de programa ou projeto federal, por meio de compra nacional ou da adesão de que trata o § 2º do art. 32; ou
- V - Quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.

9.3. Adicionalmente vê-se um conjunto de benefícios aqui elencados:

- a) Propicia a redução do volume de fornecimento: O Registro de Preços propicia a redução de volume de fornecimento a serem executados, pois a Administração deve requisitar o objeto cujo preço foi registrado somente quando houver demanda.
- b) Propicia transparência: O Registro de Preços, como é um procedimento que pode envolver vários órgãos, proporciona maior transparência já que todos os seus procedimentos são monitorados por todos os agentes envolvidos e devem ser publicados para que todos tenham conhecimento. A Lei nº 14.133/21, por exemplo, exige que sejam feitas publicações trimestrais dos preços registrados, ampliando a transparência do procedimento e proporcionando o acompanhamento dos preços por todos os cidadãos.
- c) Adequado à imprevisibilidade do consumo: Como não há a obrigatoriedade da contratação imediata, a Administração poderá registrar os preços e, somente quando houver a necessidade, efetivar a contratação, considerando-se este um dos principais motivos da contratação por meio de Registro de Preços, em virtude da imprevisibilidade de crescimento da Instituição e abertura de novas áreas de negócio e frentes de trabalho, bem como do possível aumento no volume de trabalhos a ser desenvolvido, corroborando às hipóteses previstas para a utilização do sistema de registro de preços. Em se confirmando o crescimento da AGU e o aumento no volume de serviços, haverá aumento na infraestrutura computacional, e consequentemente haverá a necessidade de equipamentos de informático, como novos hardwares e softwares associados, que permitam garantir a continuidade das atividades de gestão e de negócios, bem como nas de controle e fiscalização dos servidores do órgão, motivo pelo qual, diante desta imprevisibilidade, reforça-se a adoção do sistema de registro de preços para a contratação pretendida.
- d) Agiliza as aquisições: Com o Registro de Preços as aquisições ficarão mais ágeis, pois a licitação já estará realizada, as condições de fornecimento estarão ajustadas, os preços e os

respectivos fornecedores já estarão definidos. Sendo assim, a partir da necessidade a AGU somente solicitará prestação do serviço e o fornecedor deverá realizar o fornecimento conforme condições anteriormente ajustadas.

e) Proporciona a redução do número de licitações: O Registro de Preços ainda proporciona a redução do número de licitações, pois projetos de mesma natureza podem ser demandados por outras organizações públicas.

9.4. Regime de execução

9.4.1. O regime de execução indireta do contrato será por empreitada por preço unitário.

9.5. Da Aplicação da Margem de Preferência

9.5.1. Nos termos da legislação vigente, quando aplicável, conforme previsão em EDITAL, nas aquisições de bens e serviços de informática e automação definidos pela Lei nº 8.248, de 1991, será assegurado o direito de preferência conforme procedimento estabelecido pelo Decreto nº 11.890, de 22 de janeiro de 2024, e nos art. 44 e 45 da Lei Complementar nº 123, de 14 de dezembro de 2006.

9.5.2. As licitantes qualificadas como microempresas ou empresas de pequeno porte que fizerem jus ao direito de preferência terão prioridade no exercício desse benefício em relação às médias e às grandes empresas na mesma situação.

9.5.3. Destacando-se que a aplicação desse critério e direito ocorre de forma automática no sistema compras governamentais.

9.6. Exigências de habilitação

9.3.1. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

9.6.1.1. Habilitação jurídica

9.6.1.1.1. **Pessoa física:** cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

9.6.1.1.2. **Empresário individual:** inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

9.6.1.1.3. **Microempreendedor Individual - MEI:** Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio <https://www.gov.br/empresas-e-negocios/pt-br/empreendedor>;

9.6.1.1.4. **Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada**

como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

9.6.1.1.5. **Sociedade empresária estrangeira:** portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020;

9.6.1.1.6. **Sociedade simples:** inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

9.6.1.1.7. **Filial, sucursal ou agência de sociedade simples ou empresária:** inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

9.6.1.1.8. **Sociedade cooperativa:** ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

9.6.1.1.9. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

9.6.1.2. Habilitação fiscal, social e trabalhista

9.6.1.2.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

9.6.1.2.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

9.6.1.2.3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

9.6.1.2.4. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a

apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

9.6.1.2.5. Prova de inscrição no cadastro de contribuintes Municipal/Estadual relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

9.6.1.2.6. Prova de regularidade com a Fazenda Municipal/Estadual do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

9.6.1.2.7. Caso o fornecedor seja considerado isento dos tributos Municipais/Estaduais relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

9.6.1.2.8. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

9.6.1.3. Qualificação Econômico-Financeira

9.6.1.3.1. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art. 5º, inciso II, alínea “c”, da Instrução Normativa Seges/ME nº 116, de 2021), ou de sociedade simples;

9.6.1.3.2. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

9.6.1.3.3. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando:

- a) Índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um);
- b) As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura; e
- c) Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos.
- d) Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.

9.6.1.3.4. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos

índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação a comprovação de patrimônio líquido de 10% (dez por cento) do valor total estimado da contratação.

9.6.1.3.5. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).

9.6.1.3.6. O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

9.6.1.4. Qualificação Técnica

9.6.1.4.1. Comprovação de aptidão para execução de serviço de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.

9.6.1.4.2. Apresentar carta ou declaração emitida pelo fabricante da solução, em papel timbrado e assinada pelo representante legal da fabricante, atestando que a licitante participante é autorizada a revender a solução ofertada.

9.6.1.4.3. Os modelos de equipamentos ofertados devem possuir, na data da entrega da proposta, homologação junto à ANATEL.

9.6.1.4.4. Apresentar, no mínimo, 01 (um) Atestado de Capacidade Técnica, expedido por pessoa jurídica de direito público ou privado, em documento timbrado, e que comprove aptidão para execução do objeto da contratação, em quantidades e características, no mínimo, 50% (cinquenta por cento), nos itens de maior relevância (Itens 1, 2, 3, 4, 9, 10, 11 e 12) contendo as seguintes informações:

- a) Identificação do órgão ou empresa emitente com nome ou razão social, CNPJ, endereço completo, nome da pessoa responsável e função no órgão ou empresa, telefone e fax para contato;
- b) Indicação do CONTRATANTE de que foram atendidos os requisitos de qualidade e prazos requeridos (descrição, duração e avaliação dos resultados);

- c) Descrição das principais características dos serviços, comprovando que a CONTRATADA executa ou executou o objeto da contratação, considerando;
- d) Data de emissão do atestado ou da certidão;
- e) Assinatura e identificação do signatário (nome, telefone, cargo e função que exerce junto ao órgão ou empresa emitente).

9.6.1.4.5. Os atestados deverão ser válidos e conter informações sobre a venda, instalação e configuração de equipamentos iguais ou similares aos listados nos itens 1, 2, 3, 4, 9, 10, 11 e 12.

9.6.1.4.6. Ficará a cargo da AGU, caso julgue necessário, realizar diligências para averiguação das informações constantes dos atestados de capacidade técnica apresentados solicitando, por exemplo, cópia do contrato de compra, Ordem de Fornecimento, Termo de Recebimento dentre outros.

9.6.1.4.7. No caso de atestados emitidos por pessoas jurídicas de direito privado, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa CONTRATADA.

9.6.1.4.8. Serão considerados como pertencentes ao mesmo grupo empresarial da empresa licitante empresas controladas ou controladoras da empresa licitante ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da empresa licitante.

9.6.1.4.9. Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

9.6.1.4.10. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

9.6.1.4.11. Poderá ser admitida, para fins de comprovação de quantitativo mínimo do serviço, a apresentação de diferentes atestados de serviços executados de forma concomitante, pois essa situação se equivale, para fins de comprovação de capacidade técnico-operacional, a uma única contratação, nos termos do item 10.9 do Anexo VII-A da IN SEGES/MPDG n. 5/2017.

9.6.1.4.12. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior, conforme item 10.8 do Anexo VII-A da IN SEGES/MPDG n. 5, de 2017.

9.6.1.4.13. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato

que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.

9.6.1.4.14. O fornecedor deverá apresentar Declaração 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 14.133, de 2021.

9.6.1.4.15. Caso admitida a participação de cooperativas, será exigida a seguinte documentação complementar:

- a) A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764, de 1971;
- b) A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;
- c) A comprovação do capital social proporcional ao número de cooperados necessários à prestação do serviço;
- d) O registro previsto na Lei n. 5.764, de 1971, art. 107;
- e) A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato; e

9.6.1.4.16. Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa:

- a) ata de fundação;
- b) estatuto social com a ata da assembleia que o aprovou;
- c) regimento dos fundos instituídos pelos cooperados, com a ata da assembleia;
- d) editais de convocação das três últimas assembleias gerais extraordinárias;
- e) três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais; e
- f) ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da licitação;

9.6.1.4.17. A última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764, de 1971, ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.

10. ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO

10.1. O custo estimado total da contratação é de R\$ 19.876.855,56 (dezenove milhões, oitocentos e setenta e seis mil, oitocentos e cinquenta e cinco reais e cinquenta e seis centavos), conforme tabela descrita no subitem 1.1. deste TERMO DE REFERÊNCIA.

11. ADEQUAÇÃO ORÇAMENTÁRIA

11.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União, e será formalizado conforme preconizado no Decreto nº 11.462/2023, que regulamenta os art. 82 a art. 86 da Lei nº 14.133/2021, para dispor sobre o Sistema de Registro de Preços.

11.2. A contratação será atendida pela seguinte dotação:

Gestão/Unidade	Fonte de Recursos	Programa de Trabalho	Elemento de Despesa
110792/00001	0100000000	03092213026740001	339040

11.3. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

11.4. Cronograma Físico Financeiro

11.4.1. Os pagamentos serão efetuados obedecendo aos seguintes critérios:

Itens	Periodicidade	Condições de Pagamento
Itens de 1 a 20	Parcela única	Até 30 (trinta) dias mediante a apresentação da Ordem de Fornecimento de Bens (OFB)/Ordem de Serviço (OS) emitida, contendo o detalhamento do objeto, apresentação do Termo de Recebimento Definitivo e a apresentação da NF.

12. DA VIGÊNCIA DO CONTRATO

12.1. O prazo de vigência da contratação é de 12 (doze) meses, contados da data de sua assinatura, na forma do artigo 105 da Lei nº 14.133, de 2021.

13. DA VIGÊNCIA DA ATA DE REGISTRO DE PREÇOS

13.1. O prazo de vigência da Ata de Registro de Preços será de 12 (doze) meses e poderá ser prorrogado, por igual período, desde que comprovado o preço vantajoso, na forma do artigo 84 da Lei nº 14.133, de 2021.

13.2. Demais regras sobre o procedimento de Sistema de Registro de Preços - SRP, serão detalhados no Edital.

14. DO REAJUSTE DE PREÇOS

14.1. Os preços serão fixos e irrevogáveis.

15. DA MATRIZ DE RISCOS

15.1. Em observância ao disposto no inciso XXVII do art. 6º da Lei nº 14.133/2021, as PARTES, declaram que a presente contratação não apresenta eventos supervenientes impactantes no equilíbrio econômico-financeiro que justifiquem ou fundamentem a elaboração de Matriz de Riscos para o contrato.

16. DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO

16.1. A Equipe de Planejamento da Contratação foi instituída pela PORTARIA DLOG/SGA/AGU n. 00099 de 20 de junho de 2023 (Seq. 4).

16.2. Conforme o §6º do art. 12 da IN SGD/ME nº 94/2022, o TERMO DE REFERÊNCIA será assinado pela Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC, e aprovado pela autoridade competente.

INTEGRANTE REQUISITANTE	INTEGRANTE TÉCNICO	INTEGRANTE ADMINISTRATIVO
(assinado eletronicamente) UENDEL DA SILVA TAVARES	(assinado eletronicamente) THIAGO DE SOUZA MARTINS	(assinado eletronicamente) LEONARDO COSTA DA SILVA

Aprovo,

AUTORIDADE MÁXIMA DA ÁREA DE TIC (OU AUTORIDADE SUPERIOR, SE APLICÁVEL – § 3º do art. 11)
(assinado eletronicamente) ÁLVARO DA COSTA RONDON NETO Diretor de Tecnologia da Informação

17. INTEGRAM ESTE TERMO DE REFERÊNCIA OS SEGUINTE APÊNDICES:

- APÊNDICE “A”** - Requisitos e Especificações Técnicas da solução
- APÊNDICE “B”** - Relação das unidades da AGU e a demanda
- APÊNDICE “C”** - Modelo de Proposta de Preços
- APÊNDICE “D”** - Modelo de Ordem de Fornecimento de Bens/Ordem de Serviço
- APÊNDICE “E”** - Modelo de Declaração de Sustentabilidade Ambiental
- APÊNDICE “F”** - Termo de Recebimento Provisório - Compras TIC
- APÊNDICE “G”** - Termo de Recebimento Definitivo
- APÊNDICE “H”** - Termo de Compromisso de Manutenção de Sigilo
- APÊNDICE “I”** - Termo de Ciência
- APÊNDICE “J”** - Declaração de cumprimento da lei geral de proteção de dados
- APÊNDICE “K”** - Declaração de vistoria
- APÊNDICE “L”** - Declaração de recusa de vistoria
- APÊNDICE “M”** - Termo de Confidencialidade e Sigilo - Vistoriador
- APÊNDICE “N”** – Modelo de comprovação Ponto-a-Ponto

APÊNDICE “A”

REQUISITOS E ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
REQUISITOS GERAIS PARA OS ITENS 1 e 2 (SPINE & LEAF)	
A-1	Os equipamentos deverão ser completamente instalados no prazo máximo de 90 (noventa) dias corridos, contados a partir da data de aceite de entrega;
A-2	Todas as configurações serão realizadas em conformidade com a recomendação do fabricante dos equipamentos e softwares da solução, boas práticas de implementação recomendada pelo fabricante e os requisitos fornecidos pela AGU para o ambiente em questão. Sendo vedada a subcontratação para tais serviços
A-3	Os serviços de instalação física e as configurações dos equipamentos poderão ocorrer, a critério da AGU, em dias não úteis (sábado e domingo e feriados), no horário acordado com a AGU, podendo ocorrer fora do horário comercial;
A-4	A CONTRATADA deverá prover serviços profissionais do fabricante ou técnicos certificados pelo fabricante para efetuar a execução dos serviços de implantação;
A-5	A CONTRATADA deverá fornecer com antecedência mínima de 10 (dias) dias corridos, anteriores a instalação, os dados e a documentação dos profissionais que atuarão na instalação;
A-6	A CONTRATADA deverá providenciar todos os materiais necessários à instalação física dos equipamentos;
A-7	A CONTRATADA deve garantir que todos os equipamentos, componentes, acessórios e cabos de conexão para interligar fisicamente todos os componentes da solução sejam entregues;
A-8	Toda e qualquer despesa relacionada ao transporte, alimentação e hospedagem dos profissionais envolvidos deverá ocorrer por conta da CONTRATADA, sem quaisquer ônus para a AGU;
A-9	Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;
A-10	Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;
A-11	Deve possuir interface dedicada para gerenciamento local do tipo "out-of-band". Esta interface de gerenciamento deverá possuir porta 1000Base-T com conector RJ-45;
A-12	Deve suportar Q-in-Q, recurso também conhecido como <i>Stacked VLAN</i> ou VLAN sobre VLAN em que é possível configurar duas TAGs de VLAN no mesmo frame conforme padrão IEEE 802.1ad;
A-13	Deve implementar Flow Control baseado no padrão IEEE 802.3X;
A-14	Deve suportar o padrão IEEE 802.1Qbb (<i>Priority-based Flow Control</i>);

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
A-15	Deve permitir a configuração de links agrupados virtualmente (<i>link aggregation</i>) de acordo com o padrão IEEE 802.3ad (<i>Link Aggregation Control Protocol – LACP</i>);
A-16	Deve suportar <i>Multi-Chassis Link Agregation</i> (MCLAG) ou mecanismo similar para agrupar suas interfaces com interfaces de outro switch de mesmo modelo de tal forma que equipamentos terceiros reconheçam as interfaces de ambos os switches como uma única interface lógica;
A-17	Deve suportar a comutação de Jumbo Frames;
A-18	Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;
A-19	Deve suportar a criação de rotas estáticas em IPv4 e IPv6;
A-20	Deve possuir hardware capaz de suportar roteamento dinâmico através dos protocolos RIP, BGP, OSPF em IPv4 e OSPF em IPv6. É obrigatória a entrega de licenças caso o software exija licenciamento adicional para ativação dos protocolos;
A-21	Deve possuir hardware capaz de suportar roteamento <i>multicast</i> através do protocolo PIM-SSM (<i>Protocol Independent Multicast – Source-Specific Multicast</i>). É obrigatória a entrega de licenças caso o software exija licenciamento adicional para ativação dos protocolos;
A-22	Deve possuir hardware capaz de suportar o protocolo VRRP ou mecanismo similar de redundância de gateway. É obrigatória a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo;
A-23	Deve suportar <i>Bidirectional Forwarding Detection</i> (BFD). É obrigatória a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo;
A-24	Deve ser capaz de criar múltiplas tabelas de roteamento através de VRF (<i>Virtual Routing and Forwarding</i>). É obrigatória a entrega de licenças caso o software exija licenciamento adicional para ativação deste recurso;
A-25	Deve permitir configurar determinadas portas físicas do switch como interfaces de camada 3 que tenha suporte às funções de roteamento sem requerer a configuração de uma VLAN;
A-26	Deve implementar serviço de DHCP Server e DHCP Relay;
A-27	Deve suportar o protocolo <i>Virtual Extensible LAN</i> (VXLAN) para permitir que o tráfego de camada 2 seja encaminhado para outros locais da rede via roteamento;
A-28	Deve suportar IGMP <i>Snooping</i> para controle de tráfego de <i>multicast</i> , permitindo a criação de pelo menos 500 (quinhentos) grupos;
A-29	Deve suportar o protocolo <i>Multicast Listener Discovery</i> (MLD) <i>Snooping</i> para otimizar as comunicações multicast em IPv6;
A-30	Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch e outro switch da rede (port mirroring / SPAN);

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
A-31	Deve permitir o espelhamento de uma porta ou de um grupo de portas para uma porta especificada em outro equipamento através de RSPAN e ERSPAN;
A-32	Deve implementar <i>Spanning Tree</i> conforme os padrões IEEE 802.1w (<i>Rapid Spanning Tree</i>) e IEEE 802.1s (<i>Multiple Spanning Tree</i>). Deve implementar pelo menos 30 (trinta) instâncias de <i>Multiple Spanning Tree</i> ;
A-33	Deve implementar recurso conhecido como <i>PortFast</i> ou <i>Edge Port</i> para que uma porta de acesso seja colocada imediatamente no status " <i>Forwarding</i> " do <i>Spanning Tree</i> após sua conexão física;
A-34	Deve implementar mecanismo de proteção da " <i>root bridge</i> " do algoritmo <i>Spanning Tree</i> para prover defesa contra-ataques do tipo " <i>Denial of Service</i> " no ambiente nível 2;
A-35	Deve permitir a suspensão de recebimento de BPDUs (<i>Bridge Protocol Data Units</i>) caso a porta esteja colocada no modo " <i>fast forwarding</i> " (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;
A-36	Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;
A-37	Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (<i>flapping</i>) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;
A-38	Deverá possuir controle de <i>broadcast</i> , <i>multicast</i> e <i>unicast</i> nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;
A-39	Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;
A-40	Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;
A-41	Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);
A-42	Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores do campo " <i>Differentiated Services Code Point</i> " (DSCP) do cabeçalho IP, conforme definições do IETF;
A-43	Deverá implementar ao menos 1 (um) dos seguintes mecanismos de prevenção contra congestão de tráfego: Weighted Round Robin (WRR), WRED (<i>Weighted Random Early Detection</i>) ou <i>Weighted Fair Queuing</i> (WFQ);
A-44	Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;
A-45	Deve suportar o mecanismo <i>Explicit Congestion Notification</i> (ECN) para notificar o emissor que há uma congestão ocorrendo e com isso evitar que os pacotes sejam descartados;
A-46	Deve implementar mecanismo de proteção contra ataques do tipo <i>IPspoofing</i> para mensagens de IPv6 <i>Router Advertisement</i> . A licitante deverá comprovar que esse recurso opera em camada 3 (L3);

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
A-47	Deverá implementar mecanismo de proteção contra ataques que utilizam o protocolo ARP. Devendo, no mínimo, proteger contra os seguintes tipos de ataques: man-in-the-middle (IPv4), ARP Spoofing, ARP Storm e ARP Flood Attack;
A-48	Deve implementar DHCP <i>Snooping</i> em IPv4 e IPv6 para mitigar problemas com servidores DHCP que não estejam autorizados na rede;
A-49	Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;
A-50	Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;
A-51	Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;
A-52	Deve suportar MAC <i>Authentication Bypass</i> (MAB);
A-53	Deve implementar RADIUS CoA (Change of Authorization);
A-54	Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;
A-55	Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;
A-56	Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;
A-57	Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;
A-58	Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;
A-59	Deve suportar RADIUS <i>Authentication</i> e RADIUS <i>Accounting</i> através de IPv6;
A-60	Deve suportar o protocolo PTP (<i>Precision Time Protocol</i>);
A-61	Deve implementar <i>Netflow</i> , <i>sFlow</i> ou similar;
A-62	Deve suportar o envio de mensagens de log para servidores externos através de syslog;
A-63	Deve suportar o protocolo SNMP (<i>Simple Network Management Protocol</i>) nas versões v1, v2c e v3;
A-64	Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (<i>Command Line Interface</i>);

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
A-65	Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;
A-66	Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);
A-67	Deve permitir ser gerenciado através de IPv6;
A-68	Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;
A-69	Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;
A-70	Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;
A-71	Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;
A-72	Deverá suportar protocolo <i>OpenFlow</i> v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;
A-73	Deverá suportar ser configurado e monitorado através de REST API;
A-74	Deve possuir ferramenta para captura de pacotes que auxiliarão na identificação de problemas na rede. Deve permitir a utilização de filtros para selecionar o tráfego que deverá ser capturado e permitir a exportação dos pacotes através de arquivo. pcap para análise em software <i>Wireshark</i> ;
A-75	Deve ser capaz de armazenar no mínimo duas versões de firmware simultaneamente em sua memória flash;
A-76	Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
A-77	Deve suportar temperatura de operação de até 40º Celsius;
A-78	Deve possuir MTBF (<i>Mean Time Between Failures</i>) igual ou superior a 10 (dez) anos;
ID	ITEM 1 - SWITCH DATACENTER TIPO 1 - SPINE
B-1	Camada na arquitetura " <i>Spine-and-Leaf</i> " que deve ser suportada.
B-2	Deve possuir 32 (trinta e duas) slots QSFP28 para conexão de fibras ópticas do tipo 100GBase-X operando em 40GbE e 100GbE, para interconexão com os servidores, sistemas de armazenamento, firewalls, balanceadores de carga, dentre outros equipamentos de rede.
B-3	Deve possuir capacidade de comutação de pelo menos 6400 Gbps Duplex;
B-4	Deve possuir capacidade de encaminhar, no mínimo, 4300 Mpps (Milhões de pacotes por segundo);
B-5	Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
B-6	Deve suportar 1000 (um mil) ACLs de entrada;
B-7	Latência < 1 us.
B-8	16 MB Memória mínima de Buffer (<i>Packet Buffer</i>).
B-9	Capacidade mínima de 72.000 endereços na tabela MAC (<i>MAC address table size</i>).
B-10	Direção do fluxo de ar <i>Front to back</i> .
B-11	Deve ser fornecido com fontes de alimentação redundantes do tipo <i>hotswap</i> , com capacidade para operar em tensões de 110V e 220V;
B-12	Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;
ID	ITEM 2 - SWITCH DATACENTER TIPO 2 - LEAF
C-1	Camada na arquitetura " <i>Spine-and-Leaf</i> " que deve ser suportada.
C-2	Deve possuir 48 (quarenta e oito) slots para conexão de fibras ópticas do tipo 1GE/10GE/25GE SFP28, para interconexão com os servidores, sistemas de armazenamento, firewalls, balanceadores de carga, dentre outros equipamentos de rede.
C-3	Adicionalmente, deve possuir ao menos 8 (oito) slots 40GE/100GE QSFP28 para conexão de fibras ópticas operando com velocidades de 40 e 100 Gigabit Ethernet;
C-4	Deve possuir capacidade de comutação de pelo menos 4 Tbps Duplex;
C-5	Deve possuir capacidade de encaminhar no mínimo 2.4 Mbps (Milhões de pacotes por segundo);
C-6	Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;
C-7	Deve suportar 3000 (três mil) ACLs de entrada;
C-8	Latência < 1us.
C-9	12 MB Memória mínima de Buffer (<i>Packet Buffer</i>).
C-10	Capacidade mínima de 96.000 endereços na tabela MAC (<i>MAC address table size</i>).
C-11	Direção do fluxo de ar <i>Front to back</i> .
C-12	Tipo de rack a ser instalado.
C-13	Deve ser fornecido com fontes de alimentação redundantes do tipo hot-swap, com capacidade para operar em tensões de 110V e 220V;
C-14	Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
ID	ITEM 3 - SWITCH DE ACESSO 24 PORTAS TIPO 3 (PoE BASE T)
D-1	Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;
D-2	Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a autonegociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);
D-3	Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;
D-4	Deverá implementar os padrões IEEE 802.3af (<i>Power over Ethernet – PoE</i>) e IEEE 802.3at (<i>Power over Ethernet Plus – PoE+</i>) com PoE <i>budget</i> de 370W a serem alocados em qualquer uma das portas 1000Base-T;
D-5	Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;
D-6	Deve possuir 1 (uma) interface USB;
D-7	Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 180 Mpps (milhões de pacotes por segundo);
D-8	Deve suportar 4000 (quatro mil) VLANs ativas de acordo com o padrão IEEE 802.1Q;
D-9	Deve possuir tabela MAC com suporte a 32.000 endereços;
D-10	Deve operar com latência igual ou inferior à 1us (microsegundo);
D-11	Deve implementar Flow Control baseado no padrão IEEE 802.3X;
D-12	Deve permitir a configuração de links agrupados virtualmente (<i>link aggregation</i>) de acordo com o padrão IEEE 802.3ad (<i>Link Aggregation Control Protocol – LACP</i>);
D-13	Deve suportar a comutação de Jumbo Frames;
D-14	Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;
D-15	Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;
D-16	Deve suportar a criação de rotas estáticas em IPv4 e IPv6;
D-17	Deve implementar serviço de DHCP Relay;
D-18	Deve suportar IGMP <i>snooping</i> para controle de tráfego de <i>multicast</i> , permitindo a criação de pelo menos 1000 (mil) entradas na tabela;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
D-19	Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);
D-20	Deve implementar <i>Spanning Tree</i> conforme os padrões IEEE 802.1w (<i>Rapid Spanning Tree</i>) e IEEE 802.1s (<i>Multiple Spanning Tree</i>). Deve implementar pelo menos 15 (quinze) instâncias de <i>Multiple Spanning Tree</i> ;
D-21	Deve implementar recurso conhecido como <i>PortFast</i> ou <i>Edge Port</i> para que uma porta de acesso seja colocada imediatamente no status " <i>Forwarding</i> " do <i>Spanning Tree</i> após sua conexão física;
D-22	Deve implementar mecanismo de proteção da "root bridge" do algoritmo <i>Spanning Tree</i> para prover defesa contra-ataques do tipo " <i>Denial of Service</i> " no ambiente nível 2;
D-23	Deve permitir a suspensão de recebimento de BPDUs (<i>Bridge Protocol Data Units</i>) caso a porta esteja colocada no modo " <i>fast forwarding</i> " (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;
D-24	Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;
D-25	Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;
D-26	Deverá possuir controle de <i>broadcast</i> , <i>multicast</i> e <i>unicast</i> nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar <i>rate limit</i> ;
D-27	Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;
D-28	Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;
D-29	Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);
D-30	Deverá implementar priorização de tráfego baseada nos valores do campo " <i>Differentiated Services Code Point</i> " (DSCP) do cabeçalho IP, conforme definições do IETF;
D-31	Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;
D-32	Deverá implementar mecanismo de proteção contra ataques do tipo <i>man-in-the-middle</i> que utilizam o protocolo ARP;
D-33	Deve implementar DHCP <i>Snooping</i> para mitigar problemas com servidores DHCP que não estejam autorizados na rede;
D-34	Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
D-35	Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;
D-36	Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;
D-37	Deve suportar <i>MAC Authentication Bypass (MAB)</i> ;
D-38	Deve implementar <i>RADIUS CoA (Change of Authorization)</i> ;
D-39	Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;
D-40	Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;
D-41	Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;
D-42	Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;
D-43	Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;
D-44	Deve suportar <i>RADIUS Authentication</i> e <i>RADIUS Accounting</i> através de IPv6;
D-45	Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;
D-46	Deve permitir a customização do tempo em segundos em que um determinado <i>MAC Address</i> aprendido dinamicamente ficará armazenado na tabela de endereços MAC (<i>MAC Table</i>);
D-47	Deve ser capaz de gerar log de eventos quando um novo endereço <i>MAC Address</i> for aprendido dinamicamente nas interfaces, quando o <i>MAC Address</i> mover entre interfaces do mesmo switch e quando o <i>MAC Address</i> for removido da interface;
D-48	Deve suportar o protocolo NTP (<i>Network Time Protocol</i>) ou SNTP (<i>Simple Network Time Protocol</i>) para a sincronização do relógio;
D-49	Deve suportar o envio de mensagens de log para servidores externos através de syslog;
D-50	Deve suportar o protocolo SNMP (<i>Simple Network Management Protocol</i>) nas versões v1, v2c e v3;
D-51	Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (<i>Command Line Interface</i>);

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
D-52	Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;
D-53	Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);
D-54	Deve permitir ser gerenciado através de IPv6;
D-55	Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;
D-56	Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;
D-57	Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;
D-58	Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;
D-59	Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;
D-60	Deverá suportar protocolo <i>OpenFlow</i> v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;
D-61	Deverá suportar ser configurado e monitorado através de REST API;
D-62	Deve suportar o padrão IEEE 802.3az (<i>Energy Efficient Ethernet</i> - EEE);
D-63	Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
D-64	Deve suportar temperatura de operação de até 45º Celsius;
D-65	Deve possuir MTBF (<i>Mean Time Between Failures</i>) igual ou superior a 10 (dez) anos;
D-66	Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;
D-67	Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;
ID	ITEM 4 - SWITCH DE ACESSO 48 PORTAS TIPO 4 (PoE BASE T)
D-68	Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;
D-69	Deve possuir 48 (quarenta e oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a autonegociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
D-70	Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;
D-71	Deverá implementar os padrões IEEE 802.3af (<i>Power over Ethernet – PoE</i>) e IEEE 802.3at (<i>Power over Ethernet Plus – PoE+</i>) com PoE <i>budget</i> de 740W a serem alocados em qualquer uma das portas 1000Base-T;
D-72	Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;
D-73	Deve possuir 1 (uma) interface USB;
D-74	Deve possuir capacidade de comutação de pelo menos 176 Gbps e ser capaz de encaminhar até 250 Mpps (milhões de pacotes por segundo);
D-75	Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;
D-76	Deve possuir tabela MAC com suporte a 32.000 endereços;
D-77	Deve operar com latência igual ou inferior à 1us (microsegundo);
D-78	Deve implementar Flow Control baseado no padrão IEEE 802.3X;
D-79	Deve permitir a configuração de links agrupados virtualmente (<i>link aggregation</i>) de acordo com o padrão IEEE 802.3ad (<i>Link Aggregation Control Protocol – LACP</i>);
D-80	Deve suportar a comutação de Jumbo Frames;
D-81	Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;
D-82	Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;
D-83	Deve suportar a criação de rotas estáticas em IPv4 e IPv6;
D-84	Deve implementar serviço de DHCP Relay;
D-85	Deve suportar IGMP <i>snooping</i> para controle de tráfego de <i>multicast</i> , permitindo a criação de pelo menos 1000 (mil) entradas na tabela;
D-86	Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (<i>port mirroring / SPAN</i>);
D-87	Deve implementar <i>Spanning Tree</i> conforme os padrões IEEE 802.1w (<i>Rapid Spanning Tree</i>) e IEEE 802.1s (<i>Multiple Spanning Tree</i>). Deve implementar pelo menos 15 (quinze) instâncias de <i>Multiple Spanning Tree</i> ;
D-88	Deve implementar recurso conhecido como <i>PortFast</i> ou <i>Edge Port</i> para que uma porta de acesso seja colocada imediatamente no status " <i>Forwarding</i> " do <i>Spanning Tree</i> após sua conexão física;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
D-89	Deve implementar mecanismo de proteção da “root bridge” do algoritmo <i>Spanning Tree</i> para prover defesa contra-ataques do tipo “ <i>Denial of Service</i> ” no ambiente nível 2;
D-90	Deve permitir a suspensão de recebimento de BPDUs (<i>Bridge Protocol Data Units</i>) caso a porta esteja colocada no modo “ <i>fast forwarding</i> ” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;
D-91	Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;
D-92	Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (<i>flapping</i>) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;
D-93	Deverá possuir controle de <i>broadcast</i> , <i>multicast</i> e <i>unicast</i> nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;
D-94	Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;
D-95	Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;
D-96	Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);
D-97	Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF;
D-98	Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;
D-99	Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;
D-100	Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;
D-101	Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;
D-102	Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;
D-103	Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;
D-104	Deve suportar MAC Authentication Bypass (MAB);
D-105	Deve implementar RADIUS CoA (Change of Authorization);

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
D-106	Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;
D-107	Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;
D-108	Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;
D-109	Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;
D-110	Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;
D-111	Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;
D-112	Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;
D-113	Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);
D-114	Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;
D-115	Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;
D-116	Deve suportar o envio de mensagens de log para servidores externos através de syslog;
D-117	Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;
D-118	Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);
D-119	Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;
D-120	Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);
D-121	Deve permitir ser gerenciado através de IPv6;
D-122	Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
D-123	Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;
D-124	Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;
D-125	Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;
D-126	Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;
D-127	Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;
D-128	Deverá suportar ser configurado e monitorado através de REST API;
D-129	Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);
D-130	Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
D-131	Deve suportar temperatura de operação de até 45º Celsius;
D-132	Deve possuir MTBF (<i>Mean Time Between Failures</i>) igual ou superior a 10 (dez) anos;
D-133	Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;
D-134	Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;
ID	ITEM 5 - PONTO DE ACESSO TIPO 1 – 2X2
E-1	Ponto de acesso (AP) que permita acesso dos dispositivos à rede através do wireless e que possua todas as suas configurações centralizadas em controlador/gerenciador wireless;
E-2	Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;
E-3	Deve identificar automaticamente o controlador/gerenciador wireless ao qual se conectará;
E-4	Deve permitir ser gerenciado remotamente através de links WAN;
E-5	Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
E-6	Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;
E-7	O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (wIDS/wIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação;
E-8	Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;
E-9	Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente;
E-10	Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN;
E-11	Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;
E-12	Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;
E-13	Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at.
E-14	O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless;
E-15	Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;
E-16	Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;
E-17	Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;
E-18	Deve permitir operação em modo Mesh;
E-19	Deve possuir potência de irradiação mínima de 21dBm em ambas as frequências;
E-20	Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio;
E-21	Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
E-22	Deve suportar OFDMA;
E-23	Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax;
E-24	Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;
E-25	Deve suportar BSS Coloring;
E-26	Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;
E-27	Deve possuir sensibilidade mínima de -94dBm quando operando em 5GHz com MCS0 (HT20);
E-28	Deve possuir antenas internas ao equipamento com ganho mínimo de 2.6dBi em 2.4GHz e 3.75 dBi em 5GHz;
E-29	Em conjunto com o controlador/gerenciador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;
E-30	Em conjunto com o controlador/gerenciador wireless, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
E-31	Em conjunto com o controlador/gerenciador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz;
E-32	Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;
E-33	Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS);
E-34	Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 14 (quatorze) SSIDs com operação simultânea;
E-35	Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
E-36	Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3;
E-37	Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
E-38	Deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAPMSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST;
E-39	Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
E-40	Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
E-41	Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
E-42	Deve implementar o padrão IEEE 802.11e;
E-43	Deve implementar o padrão IEEE 802.11h;
E-44	Deve implementar o padrão IEEE 802.3az;
E-45	Deve suportar ser gerenciado via SNMP;
E-46	Deve suportar consultas via REST API;
E-47	Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação;
E-48	Deve ser capaz de operar em ambientes com temperaturas entre 0 e 40° C;
E-49	Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar;
E-50	Deve possuir indicadores luminosos (LED) para indicação de status;
E-51	O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores/gerenciador wireless deste processo;
E-52	Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste TERMO DE REFERÊNCIA deverão ser fornecidos;
E-53	Deve possuir certificado emitido pela Wi-Fi Alliance;
ID	ITEM 6 - PONTO DE ACESSO TIPO 2 – 4X4
F-1	Ponto de acesso (AP) que permita acesso dos dispositivos à rede através do wireless e que possua todas as suas configurações centralizadas em controlador/gerenciador wireless;
F-2	Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador/gerenciador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;
F-3	Deve identificar automaticamente o controlador/gerenciador wireless ao qual se conectará;
F-4	Deve permitir ser gerenciado remotamente através de links WAN;
F-5	Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
F-6	Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;
F-7	O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (WIDS/WIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação;
F-8	Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;
F-9	Deve permitir a conexão de 500 (quinhentos) clientes wireless simultaneamente;
F-10	Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN;
F-11	Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;
F-12	Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;
F-13	Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at.
F-14	O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless;
F-15	Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;
F-16	Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;
F-17	Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;
F-18	Deve permitir operação em modo Mesh;
F-19	Deve possuir potência de irradiação mínima de 23dBm em ambas as frequências;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
F-20	Deve suportar, no mínimo, operação MIMO 4x4 com 4 fluxos espaciais permitindo data rates de até 2400 Mbps em um único rádio;
F-21	Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);
F-22	Deve suportar OFDMA;
F-23	Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax;
F-24	Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;
F-25	Deve suportar BSS Coloring;
F-26	Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;
F-27	Deve possuir sensibilidade mínima de -94dBm quando operando em 5GHz com MCS0 (HT20);
F-28	Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz e 5GHz;
F-29	Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;
F-30	Em conjunto com o controlador wireless, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
F-31	Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz;
F-32	Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;
F-33	Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS);
F-34	Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 14 (quatorze) SSIDs com operação simultânea;
F-35	Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES) com 802.1x ou Chave pré-compartilhada, WEP, Captive Portal, lista de bloqueio e lista de permissões MAC;
F-36	Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3;
F-37	Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
F-38	Deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAPMSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST;
F-39	Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
F-40	Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
F-41	Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
F-42	Deve implementar o padrão IEEE 802.11e;
F-43	Deve implementar o padrão IEEE 802.11h;
F-44	Deve implementar o padrão IEEE 802.3az;
F-45	Deve suportar ser gerenciado via SNMP;
F-46	Deve suportar consultas via REST API;
F-47	Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação;
F-48	Deve ser capaz de operar em ambientes com temperaturas entre 0 e 40° C;
F-49	Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar;
F-50	Deve possuir indicadores luminosos (LED) para indicação de status;
F-51	O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;
F-52	Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste TERMO DE REFERÊNCIA deverão ser fornecidos;
F-53	Deve possuir certificado emitido pela Wi-Fi Alliance;
ID	ITEM 7 – SOLUÇÃO DE GERENCIAMENTO E CONTROLADORA
G-1	A solução deve ser baseada em máquina virtual ou appliance físico do mesmo fabricante da solução ofertada objeto deste certame que vão do item 1 a 6, e ter como objetivo gerenciar de modo centralizado todos os equipamentos a partir de uma única console de administração;
G-2	Caso a solução seja fornecida em Appliance Virtual compatível com as plataformas a seguir. Será de responsabilidade da contratada o fornecimento do servidor/hardware com todos os licenciamentos necessários para a plena funcionalidade da solução.

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
G-3	Caso seja necessário complemento de outras soluções para atendimento dos itens descritos ele deverá ser do mesmo fabricante.
G-4	Deverá estar devidamente licenciada de maneira perpétua;
G-5	Gerenciar, no mínimo, 2000 (duas mil) unidades dos equipamentos da solução do Item 1 a 6 de forma simultânea;
G-6	Caso a solução seja entregue como appliance virtual, este deve suportar:
G-7	Deve ser compatível com pelo menos 1(um) dos hypervisors VMWare 6.5 e superiores, Hyper-V 2016 e superiores e KVM;
G-8	A Solução deverá ser fornecida com o número de vCPU necessário para atendimento do item.
G-9	Deve suportar vMotion com o intuito de possibilitar alta disponibilidade da máquina virtual a nível de servidor físico. Caso esta funcionalidade não seja suportada, a solução deve ser entregue em alta disponibilidade;
G-10	Caso a solução seja entregue como appliance físico, este deve suportar:
G-11	Pelo menos 2x RJ45 10GE ports, 2x SFP+ ports;
G-12	Suportar a configuração de RAID 0/1,1s/5,5s/6,6s/10/50/60 para os discos internos;
G-13	Possuir fonte de alimentação interna, redundante e hot-swap;
G-14	Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;
G-15	Deve suportar o conceito de multi-tenancy visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução.
G-16	A solução deve permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança;
G-17	Solução que permita administrar de maneira centralizada todos os elementos responsáveis pelo gerenciamento da segurança e infraestrutura de rede e que garanta suporte a processos relativos à LGPD;
G-18	A solução deverá estar devidamente licenciada para administrar todos os pontos de acesso, switches e elementos responsáveis pelo gerenciamento da segurança e infraestrutura de rede deste processo pelo período do contrato;
G-19	Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste TERMO DE REFERÊNCIA deverão ser fornecidos;
G-20	A solução deve possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem/conflitem com outras (shadowing) ou ainda garantir que esta exigência seja plenamente atendida por meio diverso;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
G-21	A solução deve permitir agendamento para a execução de configurações nos elementos administrados;
G-22	A solução deve permitir a criação e execução de scripts em elementos administrados de maneira programada;
G-23	A solução deverá permitir uma configuração simplificada do painel de controle, que permita ao gerenciador da rede obter rapidamente uma visão da saúde de sua rede, incluindo Wi-Fi, Ethernet, e verificar se há algo que requer atenção.
G-24	A solução deverá permitir utilizar informações de tendência e SLAs configurados para determinar a saúde boa ou ruim da sua rede.
G-25	A solução deverá permitir rapidamente obter sugestões de remediação para problemas de rede detectados.
G-26	A solução deverá permitir que a solução de gerenciamento entregue diretamente às informações de seu interesse e permita que o gerenciador da rede aprofunde o quanto desejar nas informações registradas sobre o dispositivo.
G-27	A solução deverá permitir prever problemas potenciais antes que ocorram, receber ações recomendadas e automatizarem tarefas, como correções, através de Aprendizado de Máquina (Machine Learning).
G-28	A solução deve permitir a criação de templates de configuração a serem aplicados de maneira centralizada e padronizada em elementos da rede sem fio e switches;
G-29	As seguintes características do SSID devem ser configuradas nos pontos de acesso através dos templates: nome do SSID, endereçamento DHCP a ser entregue aos clientes wireless, métodos de autenticação e agendamento da disponibilidade do SSID;
G-30	As seguintes características devem ser configuradas nos pontos de acesso através dos templates: potência de transmissão Wi-Fi, escolha do canal, tamanho do canal, configuração do algoritmo de seleção automática de potência e canal, configuração de short guard interval, modo de operação e acesso administrativo ao ponto de acesso;
G-31	As seguintes características de segurança devem ser configuradas na rede sem fio através dos templates: configuração da detecção de Rogue Aps e configuração de assinaturas de wIDS ou wIPS;
G-32	A solução deve listar os elementos administrados e seu status de operação;
G-33	A solução deve listar todos os clientes conectados na rede sem fio, o nome do ponto de acesso ao qual o cliente está conectado, qualidade do sinal da conexão de cada cliente, tipo de dispositivo utilizado na conexão e nome do SSID;
G-34	A solução deve listar todos os rogue APs na rede sem fio, nome do SSID do propagado, canal impactado, nível de sinal detectado e nome do ponto de acesso que detectou o Rogue AP;
G-35	A solução deve garantir visão centralizada do status e estatísticas de uso das interfaces dos switches;
G-36	A solução deve permitir o agrupamento dos elementos administrados para aplicação de políticas ou templates de configuração;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
G-37	A solução deverá realizar o backup automático das configurações dos elementos e permitir o retorno (rollback) de uma versão de configuração salva previamente;
G-38	A solução deverá possibilitar que o administrador visualize e compare diferentes versões de configurações dos elementos, sejam elas configurações vigentes, configurações anteriores e configurações antigas;
G-39	A solução deverá possuir sistema de backup e restauração de todas as configurações da própria ferramenta de administração centralizada;
G-40	A solução deverá identificar a versão de firmware em execução nos elementos administrados e garantir que quando houver novas versões de software para eles, que seja realizada a distribuição e instalação remota de maneira centralizada;
G-41	A solução deve permitir criar políticas/templates que definam a versão de firmware a ser distribuída e instalada em elementos administrados.
G-42	A solução deve garantir visão centralizada das estatísticas de uso da rede sem fio;
G-43	A solução deve garantir visão centralizada das aplicações mais acessadas na rede, com informações sobre o volume total de dados trafegados para cada aplicação e a identificação dos usuários que fizeram os acessos;
G-44	A solução deve garantir visão centralizada das categorias de websites mais acessados na rede, com informações sobre o volume total de dados trafegados para cada categoria e a identificação dos usuários que fizeram os acessos;
G-45	A solução deve garantir visão centralizada dos usuários que mais trafegaram dados na rede, com informações sobre os hosts aos quais o usuário estava conectado, volume de dados trafegados e os endereços de destino que foram acessados;
G-46	Deverá garantir a integridade do item de configuração, através de bloqueio de alterações, em caso de acesso simultâneo de dois ou mais administradores no mesmo ativo;
G-47	Permitir acesso concorrente de administradores, permitindo ainda que seja definida uma cadeia de aprovação das alterações realizadas;
G-48	Como parte da visibilidade dos dispositivos gerenciados centralmente, a solução deve ter visibilidade das verificações de saúde do link, desempenho da aplicação, utilização da largura de banda e conformidade com o nível de serviço definido;
G-49	Deve ter a capacidade de permitir o provisionamento de comunidades VPN e monitorar as conexões VPN de todos os dispositivos gerenciados a partir de uma única console, além de exibir sua localização geográfica em um mapa;
G-50	Permitir usar palavras chaves ou cores para facilitar identificação de regras;
G-51	Permitir localizar em quais regras um objeto (ex. computador, serviço etc.) está sendo utilizado;
G-52	Permitir criação de regras que fiquem ativas em horário definido;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
G-53	Realizar o backup das configurações para permitir o retorno de uma configuração salva;
G-54	Possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras, ou garantir que esta exigência seja plenamente atendida por meio diverso.
G-55	Possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;
G-56	Possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;
G-57	Garantir que quando houver novas versões de software dos equipamentos, seja realizada a distribuição e instalação remota de maneira centralizada;
G-58	Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;
G-59	Deve suportar a definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
G-60	Deve suportar autenticação de administradores em base local e de modo remoto por meio de RADIUS, LDAP, TACACS+ e PKI.
G-61	Permitir criar na solução de gerência templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração;
G-62	Permitir criar scripts personalizados, que sejam executados de forma centralizada em um ou mais dispositivos gerenciados com comandos de CLI dos mesmos;
G-63	Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;
G-64	A gerência centralizada deve vir acompanhada com solução de visualização de logs e geração de relatórios. Esta solução pode ser disponibilizada no mesmo equipamento de gerenciamento centralizado, ou fornecido em equipamento externo do mesmo fabricante;
G-65	Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;
G-66	A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica;
G-67	Solução que deverá administrar e controlar de maneira centralizada os switches do mesmo fabricante da solução ofertada;
G-68	A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso;
G-69	A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
G-70	A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados;
G-71	A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de, no mínimo, 11.312 (onze mil e trezentos e doze) portas de switch ou um total de 352 (trezentos e cinquenta e dois) switches (Spine 4 switches = 128 portas, Leafs 18 switches = 864 portas, Acesso 24 portas 230 switches = 5.520 portas, Acesso 48 portas 100 switches = 4.800 portas que compõe esse projeto);
G-72	A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas;
G-73	A solução deve permitir, através da interface gráfica, configurar VLANs e distribuí-las automaticamente nos switches e pontos de acesso por ela gerenciados;
G-74	A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;
G-75	A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;
G-76	A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;
G-77	A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;
G-78	A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;
G-79	A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;
G-80	A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;
G-81	A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;
G-82	Solução que deverá administrar e controlar de maneira centralizada os pontos de acesso wireless do mesmo fabricante da solução ofertada;
G-83	Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste TERMO DE REFERÊNCIA deverão ser fornecidos;
G-84	A solução deve estar pronta e licenciada para garantir o gerenciamento de até 710 (setecentos e dez) pontos de acesso wireless simultaneamente em um único appliance;
G-85	Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;
G-86	Deve permitir a conexão de dispositivos wireless que transmitam tráfego IPv4 e IPv6;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
G-87	A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor;
G-88	A solução deverá ser capaz de gerenciar pontos de acesso que estejam conectados remotamente através de links WAN e Internet;
G-89	O controlador wireless deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;
G-90	A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;
G-91	Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;
G-92	O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional para suportar a conexão dos túneis originados dos pontos de acesso;
G-93	Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;
G-94	Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso de Split-Tunneling por SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;
G-95	Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;
G-96	Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre controladora e ponto de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X;
G-97	A solução deve permitir definir quais redes serão tuneladas até o controlador e quais redes serão comutadas diretamente pela interface do ponto de acesso;
G-98	A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
G-99	A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;
G-100	A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;
G-101	A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;
G-102	A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;
G-103	A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;
G-104	A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de off-channel/Background scanning. Quando realizada através de off-channel/Background scanning, a solução deve ser capaz de mensurar a utilização do ponto de acesso para caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;
G-105	A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;
G-106	A solução deve permitir a adição de controlador redundante que deve monitorar a disponibilidade e sincronizar as configurações do controlador principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;
G-107	A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;
G-108	A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;
G-109	A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;
G-110	Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;
G-111	A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
G-112	A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
G-113	A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
G-114	A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;
G-115	A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;
G-116	A solução deve implementar técnicas de <i>Call Admission Control</i> para limitar o número de chamadas simultâneas;
G-117	A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;
G-118	Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;
G-119	A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados;
G-120	A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de <i>Airtime</i> ;
G-121	A solução deve suportar a configuração do BLE (<i>Bluetooth Low Energy</i>) nos pontos de acesso que tenham este recurso;
G-122	A solução deve suportar recurso que ignore <i>Probe Requests</i> de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os <i>Probe Requests</i> sejam ignorados;
G-123	A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;
G-124	A solução deve permitir a configuração de <i>Short Guard Interval</i> para o rádio 5GHz;
G-125	A solução deve implementar recurso conhecido como <i>Airtime Fairness</i> (ATF) para controlar o uso de airtime nos SSIDs;
G-126	A solução deve ser capaz de reconfigurar automaticamente os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
G-127	A solução deve implementar recurso para controle de URLs acessadas na rede wireless através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários e SSID;
G-128	A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede wireless;
G-129	O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria;
G-130	A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas;
G-131	A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução;
G-132	A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento;
G-133	A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e para websites/domínios específicos;
G-134	A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS;
G-135	A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede wireless com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig;
G-136	O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6;
G-137	A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução;
G-138	A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede wireless;
G-139	A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução;
G-140	A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações;
G-141	A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
G-142	A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada SSID;
G-143	A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS;
G-144	A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes wireless;
G-145	A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: - Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); - Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; - ASLEAP; - Null Probe Response or Null SSID Probe Response; - Long Duration; - Ataques contra Wireless Bridges; - Weak WEP; - Invalid MAC OUI.
G-146	A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication;
G-147	A solução deve implementar mecanismos de proteção contra ataques do tipo ARP <i>Poisoning</i> na rede wireless;
G-148	Permitir configurar o bloqueio na comunicação entre os clientes wireless conectados a um determinado SSID;
G-149	Deve implementar autenticação administrativa através dos protocolos RADIUS ou TACACS;
G-150	Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA, WPA2, and WPA3;
G-151	Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;
G-152	A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;
G-153	Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;
G-154	A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
G-155	A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (<i>Change of Authorization</i>) para autenticações 802.1X;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
G-156	Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
G-157	A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informar as credenciais válidas para acesso à rede;
G-158	A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;
G-159	A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;
G-160	A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;
G-161	A solução deve permitir que a página de autenticação seja hospedada em servidor externo;
G-162	A solução deve permitir a configuração do captive portal com endereço IPv6;
G-163	A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;
G-164	A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;
G-165	Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;
G-166	A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários;
G-167	A solução deverá suportar <i>Single Sign-On</i> (SSO);
G-168	A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada;
G-169	A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede;
G-170	A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;
G-171	A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;
G-172	A solução deve permitir a configuração do captive portal com endereço IPv6;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
G-173	A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;
G-174	A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;
G-175	Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;
G-176	A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários;
G-177	A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários;
G-178	O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria;
G-179	A solução deverá permitir a customização de página de bloqueio apresentada aos usuários;
G-180	Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo continuar;
G-181	A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados;
G-182	A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas;
G-183	A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução;
G-184	A solução deve implementar recurso de DHCP Server (em IPv4 e IPv6) para facilitar a configuração de redes visitantes;
G-185	A solução deve suportar o protocolo OSPF em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura de rede LAN e WLAN;
G-186	A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;
G-187	A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;
G-188	A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;
G-189	A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
G-190	A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no equipamento ao qual os APs estejam fisicamente conectados;
G-191	A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;
G-192	A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;
G-193	A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps;
G-194	A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;
G-195	A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);
G-196	A solução deve permitir a captura de pacotes na rede wireless e exportá-los em arquivos no formato. pcap;
G-197	A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;
G-198	A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;
G-199	A solução deve permitir o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;
G-200	A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;
G-201	A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;
G-202	A solução deve permitir a atualização de firmware individualmente nos pontos de acesso, garantindo a gestão e operação simultânea de pontos de acesso com firmwares diferentes;
G-203	A solução deve possuir ferramentas de diagnósticos e debug;
G-204	A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de um ponto de acesso;
G-205	A solução deve suportar comunicação com elementos externos através de REST API;
G-206	A solução deverá ser compatível e gerenciar os pontos de acesso deste processo;
G-207	Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;
ID	ITEM 7 – SOLUÇÃO DE GERENCIAMENTO E CONTROLADORA – Solução de Identificação e Autenticação Centralizada
H-1	Características E Funcionalidades Gerais

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
H-2	Poderá ser entregue em equipamento único ou com composição de equipamentos. para atender as funcionalidades exigidas.
H-3	Deverá ser compatível e integrável com itens deste termo.
H-4	Deverá possuir licenciamento para, no mínimo, 15.000 usuários locais ou remotos;
H-5	Deverá possuir licenciamento para até 800 grupos de usuários,
H-6	Deverá possuir licenciamento para até 50 certificados de usuários.
H-7	Deverá possuir licenciamento para até 15.000 tokens para dispositivos móveis, compatíveis com sistemas Android e iOS.
H-8	Requisitos gerais:
H-9	Suportar administração em interface gráfica (GUI) por HTTP e/ou HTTPS;
H-10	Suporta administração em interface baseada em linhas de comando (CLI) por TELNET e/ou SSH;
H-11	Permitir definir perfis de administradores para a solução, de modo que possa segmentar a responsabilidade dos administradores por tarefas operativas;
H-12	Possuir Indicador visual, centralizado, de informações críticas (estado da licença, versão de firmware, consumo de CPU/Memória/Disco, quantidade de usuários criados e licenciados);
H-13	Suportar a atualização do firmware via interface gráfica, por processo simplificado e intuitivo;
H-14	Suportar customização de mensagens padrão da solução como páginas de erro, portais de autenticação, auto registro, reset de senha e outros. Suportar também a inclusão, alteração e remoção de imagens nas mensagens/páginas sem a necessidade de recursos ou conectividade externa;
H-15	Suportar configuração de Alta Disponibilidade (HA), reduzindo ao máximo os períodos de interrupção;
H-16	Suportar implementações de HA como "Ativo-Passivo" ou sincronizando configurações entre duas caixas ativas;
H-17	Permitir sincronismo automático de configurações entre todos os equipamentos que componham a solução em HA;
H-18	Suportar implementação de HA sincronizando configurações com appliances em localidades geograficamente separadas;
H-19	Suportar a opção de backup criptografado;
H-20	Suportar backup automatizado (agendados por critérios pré-definidos), não somente sob demanda;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
H-21	Suportar o backup completo da configuração, incluindo base de usuários, grupos, tokens, certificados, configurações de single-sign-on e etc. A solução deve também permitir a restauração de toda configuração diretamente da interface gráfica;
H-22	Suportar NTP (Network Time Protocol), visando o sincronismo de hora/data;
H-23	Suportar SNMP v1, v2 e v3 permitindo consultar MIB própria e envio de Traps;
H-24	Suportar nativamente Trap SNMP indicando mudança de status de HÁ;
H-25	Suportar captura de pacotes através da interface gráfica para Troubleshoot avançado em ferramentas de análise de pacotes (ex.: Wireshark);
H-26	O equipamento deve permitir o envio de e-mails relacionados a reset de senha, aprovação de novos usuários, auto-registro de usuários e autenticação de segundo fator (token);
H-27	Deve suportar o envio de mensagens SMS para os usuários através de gateways SMS de terceiros ou seu próprio serviço de envio de SMS, sendo este segundo licenciado ou não;
H-28	Deve suportar o registro de todos os eventos que os usuários de sua base de dados local realizem com suas contas, tais como criação de um usuário, troca de senha de um usuário e alteração de informação gerais;
H-29	Autenticação:
H-30	A solução deve efetuar autenticação para a gerência de identidade dos usuários da rede, ajudando a simplificar a administração dos mesmos sendo um ponto central de controle de autenticação, onde múltiplos métodos de autenticação possam ser consolidados;
H-31	Deve suportar autenticação em dois fatores (two-factor authentication);
H-32	Deve possuir suporte a autenticação de dois fatores em pelo menos dois tipos diferentes de tokens, sendo o primeiro físico (token), e o segundo lógico como software para dispositivos móveis, e-mail ou SMS, permitindo que seja dada a escolha de qual dos tipos utilizar para cada usuário;
H-33	A solução deve permitir que se defina um perfil de complexidade mínimo para as senhas de todos os usuários cadastrados na base de dados local, possibilitando a definição de número mínimo de letras minúsculas, letras maiúsculas, caracteres numéricos, caracteres especiais e etc;
H-34	A solução deve permitir a criação de política de bloqueio automático de usuários após uma quantidade de falhas de autenticação, assim evitando ataques de força bruta;
H-35	A solução deve suportar a criação de usuários em base local, que poderão ser utilizados na autenticação dos dispositivos conforme necessidade;
H-36	A solução deve permitir a criação em massa de usuários na base de dados local através da importação de lista de usuários a serem criados contida em arquivos externos;
H-37	A solução deve permitir a criação de novos usuários na base de dados local e que o criador/administrador possa definir uma senha no momento de criação;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
H-38	A solução deve permitir a criação de novos usuários na base de dados local de forma que o equipamento gere uma senha aleatória e envie automaticamente ao usuário;
H-39	A solução deve permitir a criação de novos usuários na base de dados local sem a definição de senha, exigindo que o mesmo utilize o token como único fator de autenticação;
H-40	Deve permitir associar os tokens aos usuários criados localmente na base de dados;
H-41	Deve permitir que os próprios usuários façam o registro dos seus tokens e relatem a perda de um token automaticamente, sem necessidade de envolver um administrador;
H-42	Remoção automática em massa de usuários desabilitados, baseado em critérios definidos;
H-43	A solução deve possuir formas que permitam que os usuários locais possam fazer o reset de suas senhas de forma segura sem a intervenção de administradores, através de correio eletrônico ou pergunta de segurança;
H-44	Deve suportar a criação de grupos de usuários, que poderão ser utilizados na autenticação dos dispositivos conforme necessidade;
H-45	Os tokens deverão gerar códigos com no mínimo 6 dígitos e intervalos não superiores à 60 segundos
H-46	Suportar autenticação em dois fatores por hardware dedicado (Token);
H-47	Suportar autenticação em dois fatores por aplicativo mobile (iOS e Android);
H-48	Suportar autenticação em dois fatores por envio de mensagem SMS;
H-49	Suportar autenticação em dois fatores por envio de e-mail;
H-50	Suportar a sincronização com dispositivo em hardware de geração de OTP (One Time Password);
H-51	Deve permitir sincronizar os tokens com o equipamento para o correto funcionamento dos mesmos
H-52	Deve permitir desabilitar um token quando este seja roubado ou extraviado, permitindo sua reativação posterior quando/se for recuperado;
H-53	Deve permitir a desassociação de um token a um usuário e associá-lo à outro usuário quando necessário, permitindo assim que sejam reaproveitados;
H-54	Deve continuar permitindo a autenticação de dois fatores em clientes windows mesmo com a máquina offline;
H-55	Deve prover um portal web para o auto-registro dos usuários, de forma que o mesmo acesse, preencha os seus dados e submeta o registro. Após o usuário efetuar o registro, o administrador deverá ser notificado automaticamente para aprovar ou negar o cadastro do mesmo antes de que ele seja ativado;
H-56	A solução deve funcionar como servidor RADIUS (Remote Authentication Dial-In User Server), proporcionando autenticação aos dispositivos compatíveis com tal protocolo;
H-57	A solução deve suportar a integração com servidor RADIUS remoto;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
H-58	A solução pode funcionar como servidor LDAP (Lightweight Directory Access Protocol), proporcionando autenticação aos dispositivos compatíveis com tal protocolo;
H-59	A solução deve suportar a integração com servidor LDAP remoto (como Microsoft Active Directory);
H-60	A solução deve suportar autenticação de usuários com credenciais de mídias sociais de terceiros como Facebook, Twitter, LinkedIn e Google+;
H-61	A solução deve permitir que usuários que não possuam uma conta local ou em mídias sociais se autenticuem através de um rápido cadastro, que garanta o mínimo de rastreabilidade, através da validação de endereços de e-mail ou número de telefone;
H-62	A solução deve permitir o login automático de usuários visitantes depois de se registrarem com sucesso;
H-63	A solução deve permitir configurar os parâmetros de rede (como as configurações de WiFi) em um endpoint baixando um script ou um executável através do portal de visitantes;
H-64	Deve suportar Security Assertion Markup Language (SAML), agindo como um Provedor de Identidade (Identity Provider - IDP) estabelecendo um relacionamento de confiança para autenticação segura de usuários tentando acessar um Provedor de Serviços (Service Provider - SP);
H-65	Deve permitir integração com bases do Azure Directory e GSuite;
H-66	Por meio do SAML, deve permitir integrações com SPs variados, tais como Office 365;
H-67	Deve suportar FIDO;
H-68	A solução deve apontar a última vez (data) em que um token foi utilizado;
H-69	A solução deve suportar OpenID Connect (OIDC);
H-70	Deve suportar autenticação adaptativa;
H-71	Deve suportar regras granulares no processo de autenticação. Ex: usuários se autenticando na VPN precisam utilizar MFA, mas, o mesmo usuário, em portal web, não precise informar o token;
H-72	Deve suportar push notification;
H-73	Controle baseado em porta:
H-74	A solução deve suportar nativamente (sem redirecionamentos) a integração e autenticação de switches e outros dispositivos compatíveis com o padrão 802.1X
H-75	Suportar os seguintes métodos 802.1X EAP: PEAP (MSCHAPv2), EAP-TTLS, EAP-TLS e EAP-GTC
H-76	Suportar interoperabilidade com equipamentos de acesso (switches) de outros fabricantes, para autenticação de portas junto a solução, através dos padrões 802.1X

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
H-77	Deve suportar bypass de autenticação 802.1X para dispositivos conhecidos que não suportem 802.1X, a liberação deverá ser feita baseada no endereço MAC dos equipamentos previamente cadastrados, estes terão acesso a rede sem necessidade de autenticação ou ação do usuário ou dispositivo
H-78	Certificados:
H-79	A solução deve atuar como Autoridade Certificadora (CA)
H-80	Deve permitir a administração de certificados digitais, com emissão e revogação
H-81	Deve permitir o uso de CA's confiáveis para validação de certificados emitidos por CA's externas
H-82	Deve suportar OCSP para que se possa fornecer uma lista de certificados revogados (CRL)
H-83	Deve prover repositório para autenticação de VPN Site-to-Site através de Certificados
H-84	Deve suportar SCEP Server (Simple Certificate Enrollment Protocol), permitindo a assinatura de requisições de certificados digitais (CSR) automaticamente ou com interação do administrador
H-85	Deve ser capaz de importar outros certificados de CA's assim como a lista de certificados revogados
H-86	Deve ser capaz de permitir ao administrador do sistema gerar, assinar e revogar certificados digitais para os usuários
H-87	Suportar ao protocolo ACME para geração de certificados
H-88	Serviço De Autenticação Única (Single Sign-On)
H-89	A solução deve prover capacidade de serviço SSO (Single Sign-On), com autenticação transparente (passiva) de usuários em sistemas compatíveis
H-90	Deve ser capaz de integrar-se a um diretório ativo (Windows AD) e poder oferecer a funcionalidade de SSO, onde a autenticação automática/transparente via SSO para os serviços necessários é baseada na autenticação prévia feita pelo usuário no domínio
H-91	Deve permitir definir uma lista de usuários de SSO que serão ignorados, evitando assim interferência de contas de serviços tais como antivírus ou scripts via GPO
H-92	Deve suportar análise de arquivos syslog enviados de fonte remota, para uso pelo serviço de SSO
H-93	Deve suportar Security Assertion Markup Language (SAML), agindo como autenticador de um Provedor de Serviços (Service Provider - SP) solicitando informações de identidade de usuários a Provedores de Identidade (Identity Providers - IDP's) de terceiros
H-94	Deve suportar SSO baseado em Radius (RSSO - RADIUS Single Sign-On)
H-95	Deve suportar RSSO Accounting Proxy permitindo a recepção de pacotes radius de accounting, a modificação destes pacotes e o encaminhamento dos mesmos para vários outros pontos

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
H-96	Segundo Fator De Autenticação Para Redes Privadas Virtuais
H-97	Deve ser do mesmo fabricante dos itens 1, 2, 3, 4, 9 e 10 que compõe a presente solução.
H-98	Possuir licenciamento perpétuo de token e sem limites de transferência para outros dispositivos.
H-99	Permitir o download gratuito do seu provisionamento.
H-100	Suportar exclusão e adição de novos tokens.
H-101	Instalado no dispositivo móvel sem que haja a necessidade de alteração de sua configuração, ou mesmo a capacidade de formatar o dispositivo móvel de forma remota.
H-102	Garantir a privacidade do dispositivo móvel.
H-103	Deve requerer a permissão do proprietário para envio de notificações ou qualquer tipo de alteração nas configurações.
H-104	Deve suportar, no mínimo, as principais plataformas de mobile do mercado: iOS, Android e Windows
H-105	Suportar a geração dinâmica das sementes de token, minimizando a exposição online.
H-106	Suportar ativação através da utilização de QR Codes e manual.
H-107	Criptografar o armazenamento de sementes utilizadas na geração do token.
H-108	Ter a capacidade de gerar senhas de uso único (One Time Programmable - OTP) baseado em tempo (TOTP) ou evento (HTOP) compatível com OATH.
H-109	Suportar a ocultação do token para tokens baseados em tempo (TOTP).
H-110	Ter a capacidade de proteger abertura do aplicativo através de PIN, Impressão Digital e Face Security.
H-111	Exibir o intervalo de tempo OTP.
H-112	Exibir do número de série do token.
H-113	Ser compatível com o relógio da Apple ou relógios Smart watch.
H-114	Suportar que a senha gerada possa ser copiada para a área de transferência.
H-115	Suportar detalhes de login enviados ao telefone para aprovação com um toque.
H-116	Ter um serviço de provisionamento dinâmico, onde apenas na atribuição de um token a um usuário a semente é criada e é removida durante o download ou após um tempo limite configurável.
H-117	Homologado para as especificações OTP RFC6238 e RFC4226.
H-118	Ter a capacidade de realizar vinculação com o dispositivo móvel;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
H-119	Suportar à sua utilização como segundo fator de autenticação para acesso VPN via SSL ou IPSEC, sem a necessidade de utilização de um servidor RADIUS.
ID	ITEM 7 – SOLUÇÃO DE GERENCIAMENTO E CONTROLADORA – Gerencia centralizada para coleta, armazenamento e análise automatizada de registros
I-1	A solução deve ser baseada em máquina virtual ou appliance físico do mesmo fabricante da solução do 1 à 6 e ter como objetivo a coleta, armazenamento e análise automatizada de registros em modo centralizado de todos os equipamentos a partir de uma única console de administração;
I-2	Poderá ser entregue em formato de appliance físico ou appliance virtual;
I-3	Deverá estar devidamente licenciada para:
I-4	Suportar a coleta de, no mínimo, 150 GB de logs diários;
I-5	Permitir espaço de armazenamento de, no mínimo, 24 TB;
I-6	Deve possuir solução de retenção de logs com capacidade mínima para armazenar os logs da solução por 6 (seis) meses. (Marco Civil Art.13 – 1 ano)
I-7	A solução dedicada de logs, deve suportar relatórios listando os endpoints por localidade e fabricante, usuários associados, além de relatórios de inventário, devices registrados e rogues.
I-8	Caso a solução seja entregue como appliance virtual, este deve suportar:
I-9	Deve ser compatível com pelo menos 1 (um) dos hypervisors VMWare 6.5 e superiores, Hyper-V 2016 e superiores, e KVM;
I-10	A Solução deverá ser fornecida com o número de vCPU necessário para atendimento do item.
I-11	Não deverá existir limite para a expansão da memória RAM no appliance virtual;
I-12	Deve suportar vMotion com o intuito de possibilitar alta disponibilidade da máquina virtual a nível de servidor físico. Caso esta funcionalidade não seja suportada, a solução deve ser entregue em alta disponibilidade;
I-13	Caso a solução seja entregue como appliance físico, este deve suportar:
I-14	Pelo menos 4 x RJ45 GE e 2 x SFP;
I-15	Suportar a configuração de RAID 0/1,1s/5,5s/10 para os discos internos;
I-16	Possuir fonte de alimentação interna, redundante e hot-swap;
I-17	Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;
I-18	Realizar o backup das configurações para permitir o retorno de uma configuração salva;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
I-19	Possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;
I-20	Deve suportar a definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
I-21	Deve suportar o conceito de multi-tenancy visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução.
I-22	A solução deve permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança;
I-23	Através da análise de tráfego de rede, web e DNS, deve suportar a verificação de máquinas potencialmente comprometidas ou usuários com uso de rede suspeito;
I-24	Realizar agregação via pontuação, para geração de um veredito sobre máquinas comprometidas na rede e atividades suspeitas;
I-25	Utilizar técnicas de machine learning para a captura de índices de comprometimento, através de URLs, domínios e endereços IPs maliciosos;
I-26	Deve possuir um painel com as informações de máquinas comprometidas indicando informações de endereço IP dos usuários, veredito, número de incidentes etc.;
I-27	Deve oferecer um portal do cliente fácil de usar permitindo acesso às capacidades seguras como: monitoramento e políticas e objetos, painéis analíticos, visualizações e relatórios, auditoria e recursos adicionais, como documentação;
I-28	Suporte a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;
I-29	Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;
I-30	Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;
I-31	Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;
I-32	Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;
I-33	Deve possuir mecanismos de remoção automática para logs antigos;
I-34	Permitir importação e exportação de relatórios
I-35	Deve ter a capacidade de criar relatórios no formato HTML, PDF, XML e CSV;
I-36	Deve permitir exportar os logs no formato CSV;
I-37	Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
I-38	Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;
I-39	A solução deve ter relatórios predefinidos;
I-40	Deve permitir o envio automático dos logs para um servidor FTP externo a solução;
I-41	Deve ter a capacidade de personalizar a capa dos relatórios obtidos;
I-42	Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;
I-43	Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;
I-44	Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;
I-45	Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;
I-46	Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;
I-47	Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;
I-48	Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;
I-49	Permitir o envio por e-mail relatórios automaticamente;
I-50	Deve permitir que o relatório seja enviado por e-mail para o destinatário específico;
I-51	Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;
I-52	Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;
I-53	Deve permitir o uso de filtros nos relatórios;
I-54	Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;
I-55	Permitir especificar o idioma dos relatórios criados;
I-56	Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;
I-57	Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;
I-58	Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
I-59	Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;
I-60	Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;
I-61	Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;
I-62	Deve permitir visualizar em tempo real os logs recebidos;
I-63	Deve permitir o encaminhamento de log no formato syslog;
I-64	Deve permitir o encaminhamento de log no formato CEF (Common Event Format);
I-65	Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;
I-66	Deve ser capaz de visualizar alertas de surtos e baixar automaticamente manipuladores de eventos e relatórios relacionados;
I-67	Deve permitir o time de resposta a incidentes identificar se um artefato malicioso de "Zero Day" encontrado na rede faz parte de alguma campanha específica de malware, se foi visto até o momento somente na rede da instituição;
I-68	Caso o malware faça parte de alguma campanha, deve ser detalhado qual o objetivo dela, tipos de indústria que já foram alvo do malware, comportamento malicioso conhecido sobre o malware e quais são os autores;
I-69	Deve permitir gerar alertas de eventos a partir de logs recebidos;
I-70	A solução deve possuir garantia, suporte e atualizações ao software durante a vigência do contrato;
ID	ITEM 8 – SOLUÇÃO DE NAC
J-1	Solução de controle de acesso à rede
J-2	Solução de controle de acesso à rede, a ser ofertado em formato de appliance físico ou virtual, este que deverá estar disponível para as plataformas Vmware ESXi, AWS e Microsoft Azure;
J-3	Deve ser uma solução multi-vendor capaz de suportar os switches e concentrador VPN da AGU;
J-4	A solução deve suportar capacidade de expansão para até 25.000 endpoints simultâneos, sem demandar do cliente a troca do hardware/VM;
J-5	A solução deve estar licenciada para operação com, pelo menos, 5000 endpoints conectados simultaneamente;
J-6	A solução deve ser entregue em alta disponibilidade;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
J-7	A solução deve ser capaz de inspecionar tanto IoT quanto estações/notebooks, sem depender de recursos como 802.1X e Mac-address bypass (MAB);
J-8	Para estações de trabalho, deve suportar verificação de compliance em VPN IPsec e SSL;
J-9	A licença contemplada deverá suportar todas as características exigidas neste TERMO DE REFERÊNCIA;
J-10	A solução deve permitir diferentes perfis de administração, com a capacidade de limitar e controlar a quantidade de acesso permitido às funcionalidades disponíveis, dependendo do grupo administrativo da organização ao qual o usuário pertence;
J-11	Deve detectar e classificar automaticamente o tipo dos dispositivos conectados na rede sem a necessidade de softwares instalados nos dispositivos;
J-12	Deve permitir determinar o perfil dos dispositivos descobertos por meio de métodos que não exigem a instalação de agentes, incluindo pelo menos os seguintes:
J-13	Consultas em DHCP Fingerprint;
J-14	Consultas via protocolos HTTP/HTTPS;
J-15	Consultas via protocolo SNMP;
J-16	Consultas via protocolo SSH;
J-17	Consultas via protocolo Telnet;
J-18	Consultas de portas TCP;
J-19	Consultas de portas UDP;
J-20	MAC OUI;
J-21	Consultas via protocolo WMI;
J-22	Protocolo ONVIF;
J-23	Base assinaturas pré-definidas;
J-24	A solução deve ser capaz de reconhecer as seguintes informações sobre os dispositivos conectados à rede:
J-25	Endereço MAC;
J-26	Endereço IP;
J-27	Sistema operacional;
J-28	Nome do host;
J-29	Horário de conexão;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
J-30	Usuário conectado;
J-31	Localização.
J-32	A solução deve ser capaz de reconhecer os seguintes sistemas operacionais em execução nos dispositivos conectados à rede:
J-33	Android;
J-34	Apple iOS para iPhone, iPod e iPad;
J-35	Chrome OS;
J-36	Linux;
J-37	MacOS X;
J-38	Windows 10 ou superior;
J-39	Deve lembrar o perfil atribuído a cada dispositivo e verificar sua validade a cada conexão;
J-40	Deve permitir a designação de um sponsor para autorizar a categorização dos dispositivos;
J-41	Deve permitir a recategorização periódica de dispositivos;
J-42	Deve permitir a importação de um arquivo CSV contendo informações sobre os dispositivos a serem registrados;
J-43	A solução deve incluir a detecção de dispositivos desconhecidos conectados à rede e adotar medidas de controle para limitar o acesso;
J-44	A solução deve suportar autenticação através de EAP-PEAP e EAP-TLS;
J-45	A solução deve suportar RADIUS Change of Authorization;
J-46	A solução deve suportar MAC Address Bypass;
J-47	A solução deve consultar bases LDAP e Active Directory para a identificação de usuários e grupos de usuários;
J-48	A solução deve permitir a criação de políticas de controle que combinem informações sobre a identidade do usuário e tipo de dispositivo com objetivo de autorizar dinamicamente o acesso à rede;
J-49	Deve permitir a definição dos horários em que os dispositivos serão autorizados a conectar na rede;
J-50	Deve garantir a segmentação dinâmica da rede e aplicação de políticas de segurança, tendo como base variadas combinações, como login do AD e atributos (departamento, cidade, e-mail, telefone), características da máquina (asset tag, hostname), localidade e horário;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
J-51	A solução deve incluir recursos de gerenciamento de visitantes, permitindo a criação de diferentes perfis de utilização e autorização a serem associados aos usuários, distinguindo por exemplo prestadores de serviços dos visitantes;
J-52	A solução deve permitir o cadastro dos usuários visitantes na base interna da ferramenta para que não seja necessário realizar consultas em bases externas;
J-53	A solução deve possuir ferramenta que permita a geração automática de credenciais para usuários visitantes com login e respectivas senhas;
J-54	A solução deve possuir ferramenta que permita a criação de credenciais para eventos;
J-55	Deve permitir a definição de complexidade da senha dos usuários visitantes;
J-56	Deve ser possível definir um período de validade para as contas de usuários visitantes;
J-57	Deve ser possível definir data e horário para início e encerramento das contas de usuários visitantes;
J-58	A autenticação e autorização dos usuários visitantes deve ocorrer através de portal captivo acessível via browser web;
J-59	Os visitantes em hipótese alguma deverão ter acesso à Internet e rede interna antes que a autenticação seja concluída e o usuário seja autorizado;
J-60	A solução deve vincular o login do visitante à máquina utilizada no acesso;
J-61	Deve suportar a validação de credenciais:
J-62	Em base local interna à ferramenta;
J-63	Em servidores RADIUS;
J-64	Em servidores LDAP.
J-65	A solução deve autenticar usuários visitantes através das seguintes redes sociais: Facebook, LinkedIn e Twitter;
J-66	A ferramenta deve permitir que os usuários visitantes possam realizar auto registro através do preenchimento de cadastro disponível em portal web;
J-67	Deve permitir a customização dos campos obrigatórios e opcionais para o cadastro de auto registro;
J-68	A solução deve suportar o envio da senha de acesso aos visitantes através de SMS e e-mail;
J-69	Deve ser possível definir um período para que os usuários visitantes sejam obrigados a se reautenticar;
J-70	Deve permitir a designação de grupos de usuários com função de sponsor que ficarão responsáveis por autorizar o acesso dos usuários visitantes e prestadores de serviços;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
J-71	Os usuários do tipo sponsor poderão cadastrar previamente um usuário visitante. O portal de cadastro e gerenciamento de usuários visitantes não deve permitir gerência administrativa dos demais recursos da solução;
J-72	A solução deve permitir a customização da aparência do captive portal, permitindo editar textos e inserir imagens;
J-73	Os usuários do tipo sponsor podem ser cadastrados na base local da ferramenta ou fazer parte de grupo de usuários em base LDAP/Active Directory;
J-74	A solução deve incluir recursos de conformidade de endpoint. Antes de permitir que os dispositivos acessem a rede, a solução deve garantir que estes cumpram requisitos de segurança, integridade e conformidade;
J-75	Deve permitir o uso de software agente instalado no dispositivo e agentes evanescentes que não precisam ser instalados;
J-76	Tanto para IoTs quanto para estações de trabalho, se configurado, não devem ter qualquer acesso à rede de produção enquanto não forem inspecionados e identificados;
J-77	Se um dispositivo não passar os testes de conformidade, deve ser possível:
J-78	Não forçar a remediação;
J-79	Forçar a remediação imediatamente enviando o dispositivo à rede de quarentena;
J-80	Permitir a remediação retardada, ou seja, dando um período de tolerância para que o usuário corrija o problema. Caso os problemas persistam, o dispositivo deve ser colocado em quarentena;
J-81	A solução deve permitir verificações de conformidade em endpoint que façam uso do sistema operacional:
J-82	Windows 10 ou superior;
J-83	MacOS;
J-84	Linux.
J-85	Para garantir a conformidade com as políticas de segurança, a solução deve permitir que sejam verificados os seguintes itens antes de autorizar o acesso de um endpoint na rede:
J-86	Presença de software de antivírus instalado e em execução;
J-87	Versão do sistema operacional;
J-88	Nome de domínio do Active Directory ao qual a estação Windows pertença;
J-89	Serviços em execução para estações Windows;
J-90	Informações sobre um determinado certificado digital em estações Windows;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
J-91	Registros ou chaves de registro para estações Windows;
J-92	Processos em execução para estações Windows, Linux e MacOS;
J-93	Arquivo armazenado em um determinado diretório para estações Windows, Linux e MacOS;
J-94	Pacotes instalados em estações Linux e MacOS.
J-95	A solução deve ser capaz de monitorar quando um serviço requerido for desabilitado ou interrompido em computadores. Além disso deve enviar a estação para quarentena de forma a garantir a conformidade com a política de segurança;
J-96	Deve possuir serviço RADIUS interno, além de permitir o uso de RADIUS externos;
J-97	Deve permitir a distribuição de agentes através de, pelo menos, os seguintes métodos: a) Programas de gerenciamento e distribuição de software; b) GPO do Active Directory; c) Captive Portal
J-98	Deve permitir a atualização automática ou programada dos agentes instalados nas máquinas;
J-99	O agente instalado nos computadores deve notificar os usuários com mensagens informativas em casos de eventos;
J-100	Quando em quarentena, um portal web deve ser apresentado aos usuários com informações sobre as razões pelas quais estes foram movidos para o isolamento;
J-101	A solução deve compartilhar a identificação dos usuários e/ou dispositivos autenticados para a plataforma de segurança da rede via SSO, de forma que sejam vinculadas aos acessos de Internet, provendo rastreabilidade futura;
J-102	No que tange compliance, quando houver sucesso, falha ou alerta, a solução deve permitir as seguintes ações: alerta, envio de e-mail e SMS, desabilitar o host, envio de mensagem direta para o host envolvido e executar políticas adicionais de compliance;
J-103	A solução deve integrar com plataformas de MDM, suportando pelo menos: Air Watch, Google GSuite, JAMF, MaaS360, Microsoft Intune, Mobile Iron, Nozomi, Citrix Endpoint Management;
J-104	Deve suportar integração com soluções de patching;
J-105	Deve suportar integração com soluções de análise de vulnerabilidades;
J-106	A solução deve possuir dashboard que apresente informações e estatísticas relevantes de forma resumida;
J-107	A solução deve permitir a customização do dashboard para apresentar as informações que o administrador considera relevante;
J-108	A solução deve permitir a consulta de informações e alteração de parâmetros de configuração via REST API;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
J-109	A solução deve armazenar os eventos internamente e permitir que sejam exportados;
J-110	A solução deve permitir a exportação dos eventos através de syslog;
J-111	Deve suportar alta disponibilidade, suportando todos os registros e autenticações caso um nó da solução esteja indisponível;
J-112	A solução deve ser capaz de isolar hosts na quarentena mesmo quando estes estão conectados em redes de localidades remotas, tais como filiais. Não deve ser necessário estender a VLAN para isso;
J-113	Deve possuir registro dos eventos ocorridos na solução, bem como auditoria das configurações efetuadas;
J-114	Deve possibilitar o rastreo de dispositivos, notificando a localização deles quando se conectarem à rede;
J-115	Instalação e configuração:
J-116	A solução de NAC deverá ser do mesmo fabricante dos equipamentos itens 1 a 6.
J-117	Deve possuir solução de retenção de logs com capacidade mínima para armazenar os logs da solução por <u>6 (seis) meses</u> . (Marco Civil Art.13 – 1 ano)
J-118	Dentre os relatórios disponibilizados pela solução dedicada de logs, deve suportar relatórios listando os <i>endpoints</i> por localidade e fabricante, usuários associados, além de relatórios de inventário, devices registrados e roques;
ID	ITEM 9 – CABO DAC PARA EMPILHAMENTO (SWITCHES TIPO 3 E TIPO 4) ou AOC com CONECTORES
K-1	Ser do tipo <i>Direct Attached</i> . Será aceito conexão passiva (<i>passive cooper cable</i>) ou ativa (<i>active optical</i> - AOC) com os conectores;
K-2	Não serão aceitos cabos do tipo <i>Breakout</i> ;
K-3	Ser utilizado para empilhamento dos switches tipo 3 e tipo 4;
K-4	Suportar a velocidade de 10Gbps full-duplex;
K-5	Deve ser do tipo <i>hot swappable</i> , permitindo sua instalação/remoção com o equipamento em operação;
K-6	Deve possuir, no mínimo, 1 (um) metro de comprimento;
K-7	Deve ser compatível com os switches ofertados
K-8	Deve ser do mesmo fabricante dos switches ofertados.
ID	ITEM 10 – INTERFACE ÓTICA (TRANSCIVER) 100GBE QSFP28 100GBASE-SR4 MPO
L-1	Ser do tipo QSFP28 de 100GBASE-SR4
L-2	Suportar a velocidade de 100Gbps full-duplex

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
L-3	Conector MPO
L-4	Deve ser do tipo <i>hot swappable</i> , permitindo sua instalação/remoção com o equipamento em operação
ID	ITEM 11 – TRANSCEIVER 40G QSFP28 40GBASE-SR MPO
M-1	Ser do tipo QSFP28+ de 40GBASE-SR
M-2	Suportar a velocidade de 40Gbps full-duplex
M-3	Conector MPO
M-4	Deve ser do tipo <i>hot swappable</i> , permitindo sua instalação/remoção com o equipamento em operação
ID	ITEM 12 – INTERFACE ÓTICA (TRANSCEIVER) 25GBE SFP28 25GBASE-SR
N-1	Ser do tipo SFP28 de 25GBase-SR
N-2	Suportar a velocidade de 25Gbps full-duplex
N-3	Conector Duplex LC
N-4	Deve ser do tipo <i>hot swappable</i> , permitindo sua instalação/remoção com o equipamento em operação
ID	ITEM 13 – INTERFACE ÓTICA (TRANSCEIVER) 10GBE SFP+ 10GBASE-SR
O-1	Ser do tipo SFP+ de 10GBase-SR
O-2	Suportar a velocidade de 10Gbps full-duplex
O-3	Conector Duplex LC
O-4	Deve ser do tipo <i>hot swappable</i> , permitindo sua instalação/remoção com o equipamento em operação
ID	ITEM 14 – CABO ÓTICO 100G QSFP28 100GBASE-SR MMF
P-1	O cordão óptico deverá possuir, no mínimo, 15 (quinze metros) de comprimento, constituído por fibras ópticas do tipo multimodo (MM) duplex, com conectores tipo MPO/MPO, compatível com o transceiver item 1 dessa cotação.
P-2	Suportar a velocidade de 100Gbps full-duplex.
ID	ITEM 15 – CABO ÓTICO 40G QSFP+ 40GBASE-SR MMF
Q-1	O cordão óptico deverá possuir, no mínimo, 10 (dez metros) de comprimento, constituído por fibras ópticas do tipo multimodo (MM) duplex, com conectores tipo MPO/MPO, compatível com o transceiver item 2 desse pedido de cotação.
Q-2	Suportar a velocidade de 40Gbps full-duplex

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
ID	ITEM 16 – CABO ÓTICO 25 GBE SFP28 10 MTS
R-1	O cordão óptico deverá possuir, no mínimo, 10 (dez metros) de comprimento, constituído por fibras ópticas do tipo multimodo (MM) duplex, com conectores tipo LC/LC, compatível com o transceiver item 3 desse pedido de contratação.
R-2	Suportar a velocidade de 25Gbps full-duplex
ID	ITEM 17 – CABO ÓTICO 10G SFP+ 10GBASE-SR MMF LC
S-1	O cordão óptico deverá possuir, no mínimo, 10 (dez metros) de comprimento, constituído por fibras ópticas do tipo multimodo (MM) duplex, com conectores tipo LC/LC, compatível com o transceiver item 4 desse pedido de contratação.
S-2	Suportar a velocidade de 10Gbps full-duplex
ID	ITEM 18 – SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DOS SWITCHES DE DATACENTER TIPOS 1 E 2, SOLUÇÃO DE GERENCIAMENTO E SOLUÇÃO DE NAC.
T-1	Deverá apresentado cronograma de atividades para aprovação, bem como a realização de alinhamento técnico dos requisitos e premissas do projeto.
T-2	Após a avaliação, o especialista da Contratada designado desenvolverá o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos.
T-3	O plano será modificado de acordo com os requisitos da AGU, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente.
ID	PRÉ-INSTALAÇÃO
T-4	Deverá a contratada realizar a avaliação das necessidades de rede e design personalizado de topologia <i>spine-and-leaf</i> .
T-5	Planejamento da Topologia de Rede.
T-6	Verificação dos Requisitos de Energia e Refrigeração.
T-7	Preparação de Cabos e Conectores.
T-8	Configuração de Endereços IP e DHCP.
T-9	Testes de funcionamento.
T-10	Segurança da Rede
T-11	Neste prazo está incluída a elaboração e entrega do cronograma de atividades definitivo para desenvolvimento dos serviços, consoante os requerimentos constantes ao longo do edital de licitação e seus anexos.

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
EXECUÇÃO DO PROJETO	
T-12	A Contratada deverá desenvolver as ações estabelecidas no projeto aprovado e finalizar as atividades discriminadas, atendendo rigorosamente todos os quesitos constantes ao longo deste documento.
T-13	Deverá a contratada realizar alguns dos seguintes serviços:
T-14	Instalação Física
T-15	Configuração Lógica
T-16	Configuração de Alta Disponibilidade e Redundância
T-17	Implementação de Segurança e Monitoramento
T-18	Testes e Validação
T-19	Passagem de Conhecimento e Documentação
T-20	Os serviços de entrega, instalação, configuração e testes do ambiente poderão ser realizados em horários extraordinários (período noturno, finais de semana e/ou feriados), a critério da Contratante, com entendimentos prévios junto à Contratada, de sorte a minimizar eventuais intervenções no ambiente de produção das entidades.
T-21	A instalação e configuração da solução serão acompanhadas e supervisionadas pela equipe técnica da AGU.
T-22	A configuração deverá ser realizada de acordo com as recomendações do fabricante (<i>recommended settings</i>).
T-23	Depois de concluída a instalação e configuração da solução, a Contratada deverá fornecer a documentação detalhada de todo esse processo de instalação e configuração.
CONCLUSÃO DA IMPLANTAÇÃO	
T-24	A formalização do fim da implantação, concluídas todas as etapas do projeto pela Contratada, se processará após análise e validação da AGU. Posteriormente, a Contratada, por meio de documento de sua própria emissão, formalizará a finalização dessa fase do projeto.
SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO DE GERENCIAMENTO	
T-25	Deverá apresentado cronograma de atividades para aprovação, bem como a realização de alinhamento técnico dos requisitos e premissas do projeto.
T-26	Após a avaliação, o especialista da Contratada designado desenvolverá o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos.
T-27	O plano será modificado de acordo com os requisitos da AGU, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente.

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
	PRÉ-INSTALAÇÃO
T-28	Deverá a contratada realizar a avaliação das necessidades de rede e design personalizado de topologia de Rede da AGU.
T-29	Planejamento da Topologia de Rede.
T-30	Verificação dos Requisitos de Energia e Refrigeração.
T-31	Preparação de Cabos e Conectores.
T-32	Configuração de Endereços IP e DHCP.
T-33	Testes de funcionamento.
T-34	Segurança da Rede
T-35	Neste prazo está incluída a elaboração e entrega do cronograma de atividades definitivo para desenvolvimento dos serviços, consoante os requerimentos constantes ao longo do edital de licitação e seus anexos.
	EXECUÇÃO DO PROJETO
T-36	A Contratada deverá desenvolver as ações estabelecidas no projeto aprovado e finalizar as atividades discriminadas, atendendo rigorosamente todos os quesitos constantes ao longo deste documento.
T-37	Deverá a contratada realizar alguns dos seguintes serviços:
T-38	Instalação Física
T-39	Configuração Lógica
T-40	Implementação gerenciamento dos equipamentos dos itens 1 a 6.
T-41	Criação de Dashboard para Gerenciamento
T-42	Provisionamento e Configuração
T-43	Configurar políticas de segurança.
T-44	Definir regras e implementar políticas de VPN através da solução de Gerenciamento.
T-45	Criação de Dashboard para Monitoramento
T-46	Geração de Relatórios periódicos a ser encaminhado a contratada.
T-47	Configuração da solução de Autenticação

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
T-48	Configurar o Gerenciamento de Logs a fim de armazenar logs de eventos de segurança e tráfego para fins de auditoria e investigação de incidentes.
T-49	Configuração de Automação para tomada de ação em caso de problemas ocasionados na rede.
T-50	Configuração do MFA e Token.
T-51	Configurar o controle de acesso segregando por grupos a ser definido pela AGU.
T-52	Inclusão de dispositivos a serem monitorados;
T-53	Ajuste de filtros de segurança para acesso de conteúdo;
T-54	Configuração de backup de dispositivos de rede;
T-55	Configuração de relatórios do ambiente de redes;
T-56	Criação de SSIDs, com autenticação, integração na rede e requisitos básicos de segurança;
T-57	Configuração das APs em cluster;
T-58	Configuração de <i>Captive Portal</i> ;
T-59	Implementação de Segurança e Monitoramento
T-60	Testes e Validação
T-61	Passagem de Conhecimento e Documentação
T-62	Os serviços de entrega, instalação, configuração e testes do ambiente poderão ser realizados em horários extraordinários (período noturno, finais de semana e/ou feriados), a critério da Contratante, com entendimentos prévios junto à Contratada, de sorte a minimizar eventuais intervenções no ambiente de produção das entidades.
T-63	A instalação e configuração da solução serão acompanhadas e supervisionadas pela equipe técnica da AGU.
T-64	A configuração deverá ser realizada de acordo com as recomendações do fabricante (<i>recommended settings</i>).
T-65	Depois de concluída a instalação e configuração da solução, a Contratada deverá fornecer a documentação detalhada de todo esse processo de instalação e configuração.
CONCLUSÃO DA IMPLANTAÇÃO	
T-66	A formalização do fim da implantação, concluídas todas as etapas do projeto pela Contratada, se processará após análise e validação da AGU. Posteriormente, a Contratada, por meio de documento de sua própria emissão, formalizará a finalização dessa fase do projeto.
SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO NAC	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
T-67	Deverá apresentado cronograma de atividades para aprovação, bem como a realização de alinhamento técnico dos requisitos e premissas do projeto.
T-68	Após a avaliação, o especialista da Contratada designado desenvolverá o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos.
T-69	O plano será modificado de acordo com os requisitos da AGU, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente.
PRÉ-INSTALAÇÃO	
T-70	Deverá a contratada realizar a avaliação das necessidades de rede e design personalizado de topologia de switches de acesso LAN.
T-71	Planejamento da Topologia de Rede.
T-72	Verificação dos Requisitos de Energia e Refrigeração.
T-73	Preparação de Cabos e Conectores.
T-74	Configuração de Endereços IP e DHCP.
T-75	Testes de funcionamento.
T-76	Segurança da Rede
T-77	Neste prazo está incluída a elaboração e entrega do cronograma de atividades definitivo para desenvolvimento dos serviços, consoante os requerimentos constantes ao longo do edital de licitação e seus anexos.
EXECUÇÃO DO PROJETO	
T-78	A Contratada deverá desenvolver as ações estabelecidas no projeto aprovado e finalizar as atividades discriminadas, atendendo rigorosamente todos os quesitos constantes ao longo deste documento.
T-79	Deverá a contratada realizar alguns dos seguintes serviços:
T-80	Instalação Física
T-81	Configuração Logica
T-82	Configuração Perfil de dispositivo
T-83	Configuração com a solução de Autenticação e Registro.
T-84	Configuração do gerenciamento de usuários visitantes e posturas
T-85	Configuração de perfis de host/usuários

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
T-86	Configuração da Network Access Policies
T-87	Configuração de Políticas de compliance para dispositivos de usuários da AGU e Visitantes.
T-88	Criação de Dashboard para Gerenciamento
T-89	Provisionamento e Configuração
T-90	Configurar políticas de segurança.
T-91	Definir regras e implementar políticas de VPN através da solução de Gerenciamento.
T-92	Criação de Dashboard para Monitoramento
T-93	Geração de Relatórios periódicos a ser encaminhado a contratada.
T-94	Configuração de Automação para tomada de ação em caso de problemas ocasionados na rede.
T-95	Configurar o controle de acesso segregando por grupos a ser definido pela AGU.
T-96	Inclusão de dispositivos a serem monitorados;
T-97	Ajuste de filtros de segurança para acesso de conteúdo;
T-98	Configuração de backup de dispositivos de rede;
T-99	Configuração de relatórios do ambiente de redes;
T-100	Configuração de <i>Captive Portal</i> ;
T-101	Implementação de Segurança e Monitoramento
T-102	Testes e Validação
T-103	Passagem de Conhecimento e Documentação
T-104	Os serviços de entrega, instalação, configuração e testes do ambiente poderão ser realizados em horários extraordinários (período noturno, finais de semana e/ou feriados), a critério da Contratante, com entendimentos prévios junto à Contratada, de sorte a minimizar eventuais intervenções no ambiente de produção das entidades.
T-105	A instalação e configuração da solução serão acompanhadas e supervisionadas pela equipe técnica da AGU.
T-106	A configuração deverá ser realizada de acordo com as recomendações do fabricante (<i>recommended settings</i>).
T-107	Depois de concluída a instalação e configuração da solução, a Contratada deverá fornecer a documentação detalhada de todo esse processo de instalação e configuração.

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
	CONCLUSÃO DA IMPLANTAÇÃO
T-108	A formalização do fim da implantação, concluídas todas as etapas do projeto pela Contratada, se processará após análise e validação da AGU. Posteriormente, a Contratada, por meio de documento de sua própria emissão, formalizará a finalização dessa fase do projeto.
ID	ITEM 19 – SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DOS SWITCHES DE ACESSO TIPOS 3 E 4
U-1	Deverá apresentado cronograma de atividades para aprovação, bem como a realização de alinhamento técnico dos requisitos e premissas do projeto.
U-2	Após a avaliação, o especialista da Contratada designado desenvolverá o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos.
U-3	O plano será modificado de acordo com os requisitos da AGU, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente.
	PRÉ-INSTALAÇÃO
U-4	Deverá a contratada realizar a avaliação das necessidades de rede e design personalizado de topologia de switches de acesso LAN.
U-5	Planejamento da Topologia de Rede.
U-6	Verificação dos Requisitos de Energia e Refrigeração.
U-7	Preparação de Cabos e Conectores.
U-8	Configuração de Endereços IP e DHCP.
U-9	Testes de funcionamento.
U-10	Segurança da Rede
U-11	Neste prazo está incluída a elaboração e entrega do cronograma de atividades definitivo para desenvolvimento dos serviços, consoante os requerimentos constantes ao longo do edital de licitação e seus anexos.
	EXECUÇÃO DO PROJETO
U-12	A Contratada deverá desenvolver as ações estabelecidas no projeto aprovado e finalizar as atividades discriminadas, atendendo rigorosamente todos os quesitos constantes ao longo deste documento.
U-13	Deverá a contratada realizar alguns dos seguintes serviços:
U-14	Instalação Física
U-15	Configuração Lógica

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
U-16	Configuração de Alta Disponibilidade e Redundância
U-17	Implementação lógica de software de gerenciamento
U-18	Implementação de Segurança e Monitoramento
U-19	Testes e Validação
U-20	Passagem de Conhecimento e Documentação
U-21	Os serviços de entrega, instalação, configuração e testes do ambiente poderão ser realizados em horários extraordinários (período noturno, finais de semana e/ou feriados), a critério da Contratante, com entendimentos prévios junto à Contratada, de sorte a minimizar eventuais intervenções no ambiente de produção das entidades.
U-22	A instalação e configuração da solução serão acompanhadas e supervisionadas pela equipe técnica da AGU.
U-23	A configuração deverá ser realizada de acordo com as recomendações do fabricante (<i>recommended settings</i>).
U-24	Depois de concluída a instalação e configuração da solução, a Contratada deverá fornecer a documentação detalhada de todo esse processo de instalação e configuração.
CONCLUSÃO DA IMPLANTAÇÃO	
U-25	A formalização do fim da implantação, concluídas todas as etapas do projeto pela Contratada, se processará após análise e validação da AGU. Posteriormente, a Contratada, por meio de documento de sua própria emissão, formalizará a finalização dessa fase do projeto.
ID	ITEM 20 – SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DOS ACCESS POINT TIPOS 1 E 2
V-1	Deverá apresentado cronograma de atividades para aprovação, bem como a realização de alinhamento técnico dos requisitos e premissas do projeto.
V-2	Após a avaliação, o especialista da Contratada designado desenvolverá o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos.
V-3	O plano será modificado de acordo com os requisitos da AGU, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente.
PRÉ-INSTALAÇÃO	
V-4	Deverá a contratada realizar a avaliação das necessidades de rede e design personalizado de topologia de switches de acesso WLAN.
V-5	Planejamento da Topologia de Rede.
V-6	Verificação dos Requisitos de Energia e Refrigeração.

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
V-7	Preparação de Cabos e Conectores.
V-8	Configuração de Endereços IP e DHCP.
V-9	Testes de funcionamento.
V-10	Segurança da Rede
V-11	Neste prazo está incluída a elaboração e entrega do cronograma de atividades definitivo para desenvolvimento dos serviços, consoante os requerimentos constantes ao longo do edital de licitação e seus anexos.
EXECUÇÃO DO PROJETO	
V-12	A Contratada deverá desenvolver as ações estabelecidas no projeto aprovado e finalizar as atividades discriminadas, atendendo rigorosamente todos os quesitos constantes ao longo deste documento.
V-13	Deverá a contratada realizar alguns dos seguintes serviços:
V-14	Instalação Física
V-15	Configuração Logica
V-16	Implementação logica do equipamento com a controladora.
V-17	Instalação de licenças na plataforma;
V-18	Inclusão de dispositivos a serem monitorados;
V-19	Ajuste de filtros de segurança para acesso de conteúdo;
V-20	Configuração de backup de dispositivos de rede;
V-21	Configuração de relatórios do ambiente de redes;
V-22	Criação de SSIDs, com autenticação, integração na rede e requisitos básicos de segurança;
V-23	Configuração das APs em cluster;
V-24	Configuração de Captive Portal;
V-25	Implementação de Segurança e Monitoramento
V-26	Testes e Validação
V-27	Passagem de Conhecimento e Documentação
V-28	Os serviços de entrega, instalação, configuração e testes do ambiente poderão ser realizados em horários extraordinários (período noturno, finais de semana e/ou feriados), a critério da Contratante, com

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
	entendimentos prévios junto à Contratada, de sorte a minimizar eventuais intervenções no ambiente de produção das entidades.
V-29	A instalação e configuração da solução serão acompanhadas e supervisionadas pela equipe técnica da AGU.
V-30	A configuração deverá ser realizada de acordo com as recomendações do fabricante (recommended settings).
V-31	Depois de concluída a instalação e configuração da solução, a Contratada deverá fornecer a documentação detalhada de todo esse processo de instalação e configuração.
CONCLUSÃO DA IMPLANTAÇÃO	
V-32	A formalização do fim da implantação, concluídas todas as etapas do projeto pela Contratada, se processará após análise e validação da AGU. Posteriormente, a Contratada, por meio de documento de sua própria emissão, formalizará a finalização dessa fase do projeto.

APÊNDICE “B”

RELAÇÃO DAS UNIDADES DA AGU E A DEMANDA INICIAL

Item	UF	Endereço	CEP	Equipamentos
1	AC	Rua Rui Barbosa nº 142 - Prédio - 2º andar - Centro - Rio Branco - AC - Cep. 69900-084	69900-084	1 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
2	AL	Av. Comend. Gustavo Paiva, 2789, salas 1301/1305 - Edf. Norcon Empresarial - Mangabeiras - Maceió - AL - Cep. 57030-800	57030-800	1 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 3 – AP Tipo 2
3	AL	Avenida Moreira e Silva, Nº 863 - - Farol - Maceió - AL - Cep. 57051-500	57051-500	1 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
4	AL	Av. Dep. José Lages, 555 - 10º andar - Ponta Verde - Maceió - AL - Cep. 57035-330	57035-330	1 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
5	AM	RUA SALVADOR, 440, EDIFÍCIO SOBERANE LIVE + WORK, 16 e 17º ANDAR, BAIRRO ADRIANÓPOLIS, MANAUS - AM, CEP 69057-040	69057-040	1 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
6	AP	Av. FAB, nº 1374 - Esquina com a Rua Leopoldo Machado - Centro - Cep, 68900-908	68900-908	1 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
7	BA	Av. Benedita Silveira, 118 - Centro Empresarial Portinari - 5º and, - Centro, CEP: 47.800-130 - Barreiras/BA	47.800-130	1 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
8	BA	Av. Getúlio Vargas, nº 3233, Ed. Feira trade center 5º andar Santa Mônica, Feira de Santana-BA, CEP:44077-005	44077-005	1 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
9	BA	Praça Cairu, S/N - Ed. Carlos Pereira Filho - Térreo - Centro - Ilhéus - BA - Cep. 45653-919	45653-919	1 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
10	BA	Rua da Gangorra, Quadra 12, Lt. 148-A – Alves Souza. CEP 48608-240. Paulo Afonso (BA) Justiça Federal	48608-240	1 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
11	BA	Rua Arthur de Azevedo Machado, 1225, 8º andar, Bairro Costa Azul, Salvador/BA, CEP 41.760-000	41.760-000	1 - Tipo 3 2 – Tipo 4 3 – AP Tipo 1 5 – AP Tipo 2
12	BA	ALAMEDA DOS MULUNGUS Nº32 QD.10, CASA - CASA - Caminho das Árvore - Salvador - BA - Cep.41820-490	41820-490	1 - Tipo 3 2 – Tipo 4 3 – AP Tipo 1

				4 – AP Tipo 2
13	BA	AV. OLÍVIA FLORES - N. 286, CENTRO EMPRESARIAL OLÍVIA FLORES, 4º e 5º ANDAR - Vitória da Conquista - BA - Cep. 45028-610	45028-610	1 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
14	CE	Rua Vilebaldo Aguiar, 96, Ed. Duets Office Towers - Torre Norte, 9º, 11º e 12º andares - Cocó - Fortaleza - CE - Cep. 60192-010	60192-010	1 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
15	CE	RUA CATULO DA PAIXÃO CEARENSE, 175- 30º ANDAR JUAZEIRO DO NORTE –CE CEP: 63041162	63041162	1 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
16	CE	Av. Dr. Guarany, nº 351 - - Derby - Sobral - CE - Cep. 62040-730	62040-730	1 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
17	DF	Ed. Sede I - Setor de Autarquias Sul - Quadra 3 - Lote 5/6, Ed. Multi Brasil Corporate - Brasília-DF - CEP 70.070-030	70.610-460	2 – Tipo 1 8 – Tipo 2 20 - Tipo 3 28 – Tipo 4 30 – AP Tipo 1 90 – AP Tipo 2
18	DF	SIG Quadra 6 Lote 800 - Ed. Sede II da AGU - DTI - Setor de Indústrias Gráficas	70.610-460	2 – Tipo 1 10 – Tipo 2 10 - Tipo 3 10 – Tipo 4 20 – AP Tipo 1 35 – AP Tipo 2
19	ES	Rua 25 de Março, 116 - 3º Andar - Centro, CEP: 29300-100 - Cachoeiro de Itapemirim/ES	29300-100	1 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
20	ES	Av, Jones Santos Neves, 538, Centro CEP 29936-090	29936-090	1 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
21	ES	R. José Alexandre Buaiz, nº 160 - Ed. London Office Tower - Sala 1107 - Enseada do Suá - Vitória - ES - Cep. 29050-955	29050-955	1 - Tipo 3 2 – Tipo 4 18 – AP Tipo 1 10 – AP Tipo 2
22	ES	Rua Pietrângelo de Biase nº 56 – 5º e 6º andares – Vitória – Espírito Santo – CEP: 29010-190	29010-190	1 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
23	GO	Rua 10, Quadra F-7, Lotes 82/62, - esquina com a Rua 9, 5º, 6º e 7º andar. - Setor Oeste - Goiânia - GO - Cep. 74120-020	74120-020	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2

24	GO	Rua Rozulino Ferreira Guimarães - nº 1013, 2º Andar - Setor Central - Cep, 75901-260	75901-260	1 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
25	MA	Rodovia BR 010, nº 116 - - Entroncamento - Imperatriz - MA - Cep. 65913-460	65913-460	1 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
26	MA	Rua Monção, quadra 35, lote01 loteamento Boa Vista - edf. ManhattanCenter III - Renascença II - São Luís - MA - Cep. 65075-692	65075-692	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
27	MG	Rua Teobaldo Tolendal, 89, Centro, Barbacena (MG) CEP 36200-338	36200-338	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
28	MG	Rua Santa Catarina nº 480 - 16º ao 23º Andar - Lourdes - Belo Horizonte - MG - Cep. 30170-080	89036-239	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
29	MG	Av. Rio Grande do Sul, 517 - 9º e 10º andares - Centro - Divinópolis - MG - Cep. 35500-025	35500-025	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
30	MG	Rua João Pinheiro, 610 - - Esplanada - Governador Valadares - MG - Cep. 35020-270	35020-270	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
31	MG	Rua Poços de Caldas nº 15 -Centro, CEP 35160-033	35160-033	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
32	MG	Rua Rei Alberto, nº 70 - Centro - Juiz de Fora - MG - Cep, 36016-300	36016-300	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
33	MG	Rua Comandante Soares Junior, 560 - - Bicame - Lavras - MG - Cep. 37200-000	37200-000	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
34	MG	Av. Dulce Sarmento, 140 - 6º Andar - Centro Empresarial Master Center - Bairro São José - Cep, 39400-318	39400-318	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
35	MG	Rua Neca Medeiros, 164, 2º andar, Centro, Passos/MG, CEP 37900-970	37900-970	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
36	MG	Rua Tiradentes, nº 500 - 2º andar - Centro - Cep, 38700-134	38700-134	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
37	MG	Rua Paraíba, nº 166 Bairro - Centro - Cep, 37701-022	37701-022	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2

38	MG	Rua José de Souza Neves, 75 - Marajoara, CEP: 39803-901 - Teófilo Otoni/MG	39803-901	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
39	MG	Rua Luiz Soares, nº 529 - Fabrício - Cep, 38065-260	38065-260	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
40	MG	Av. Rondon Pacheco, 345, 6º aos 9º andares - Condomínio Rondon Praia - Tabajaras - Uberlândia - MG - Cep. 38400-242	38400-242	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
41	MG	Av. João Pessoa, Nº 778 - Martins - Cep, 38400-338	38400-338	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
42	MG	RUA DR, MILTON BANDEIRA, 160, CENTRO, VICOSA, CEP 36570-000	36570-000	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
43	MG	Av. Ministro Bias Fortes, 98 - 2º Andar - Centro - Cep, 37002-450	37002-450	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
44	MS	Av, Afonso Pena, 6,134 - Chácara Cachoeira - Cep, 79040-010	79040-010	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
45	MS	Novo: Rua Zuleide Perez Tabox, 336 - Centro - Cep: 79600-090	79600-090	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
46	MT	Av, Gen, Ramiro de Noronha Monteiro - Nº 294 - Jardim Cuiabá - Cep, 78043-180	78043-180	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
47	MT	Avenida Governador Julio Campos, 1288 - Setor Comercial - Sinop - CEP 78550-242	78550-242	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
48	PA	Travessa Piedade nº 668, Bairro: Campina, Belém-PA CEP: 66053-210	66053-210	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
49	PA	Folha 32, Quadra 19, Lote Especial, 3º andar Nova Marabá - Marabá-PA - CEP - 68508-180	68508-180	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
50	PA	Av. Mal. Rondon, 853 - Esquina com a Av. Curua-Una - PRAINHA - Santarém - PA - Cep. 68005-310	68005-310	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
51	PB	Vice-Prefeito Antônio de Carvalho Souza, 255, Estação Velha, Campina Grande/PB, CEP: 58410-050	58410-050	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2

52	PB	Av. Getúlio Vargas, Nº 255 - - Centro - João Pessoa - PB - Cep. 58013-240	58013-240	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
53	PB	Av. Rio Grande do Sul, 1345, BAIRRO DOS ESTADOS - Ed. Evollution Business Center 12º andar salas 1207 a 1209 João Pessoa - PB, 58030-020	58030-020	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
54	PB	Rua João da Mata, 603 - Centro - Cep, 58400-245	58400-245	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
55	PE	Rua Luiz Malagueta Vieira, 71 - Universitário - Cep, 55016-720	55016-720	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
56	PE	Pça, Dom Moura, s/nº, Edf, Sede do INSS, 1o andar - Centro - Cep, 55295-220	55295-220	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
57	PE	Rua Engenheiro Carlos Pinheiro, 33 - Edf. Moysés Mendes - Centro - Petrolina - PE - Cep. 56302-310	56302-310	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
58	PE	Av, Eng, Domingos Ferreira, 604 - Empresarial Marcela Dubeux - Boa Viagem - Cep, 51011-050	51011-050	10 - Tipo 3 14 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
59	PE	Av, Herculano Bandeira, 716 - Pina - Cep, 51110-130	51110-130	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
60	PE	R, ISNERIO INÁCIO, Nº200, Nossa Sra. da Penha, Serra Talhada-PE, CEP 56903-450	56903-450	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
61	PI	Rua Angélica, nº 1579, 3º andar - Esquina com a Rua Coronel Costa Araújo - Fátima - Cep, 64049-532	64049-532	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
62	PR	Av, Munhoz da Rocha, Nº 1247 - Cabral - Cep, 80035-000	80035-000	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
63	PR	Av, Jorge Schimmelpfeng, nº 265 - Centro - Cep, 85851-110	85851-110	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
64	PR	Av, Paraná, 1,661 - Jardim Pólo Centro, CEP: 85863-720 - Foz do Iguaçu/PR	85863-720	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
65	PR	Rua Guanabara, 410 - Centro, CEP: 85605-300 - Francisco Beltrão/PR	85605-300	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2

66	PR	Avenida Tiradentes, 501, - Edifício Twin Business Tower, 18º andar, Torre 01 - Jardim Shangri-la - Cep.86070-545	86070-545	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
67	PR	Avenida do Café, Nº 543 - Condomínio Palácio do Café - Aeroporto - Cep, 86038-000	86038-000	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
68	PR	Rua Santos Dumont, 3042 - Condomínio Edifício Iracema - sobreloja - Centro - Cep, 87013-050	87013-050	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
69	PR	Av, Horácio Raccanello Filho, 5589 - Edifício Genesis, 6º andar - Novo Centro - Cep,87020-035	87020-035	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
70	PR	Rua Tapajós, 520 - Centro, CEP: 85501-030 - Pato Branco/PR	85501-030	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
71	PR	Rua Dr, Paula Xavier, 246 - Vila Estrela - Cep, 84040-010	84040-010	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
72	PR	Praça da Bíblia Nº 3336 - 1º andar - Ed, CEMED - salas 101/102 - centro - Cep, 87501-055	87501-055	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
73	PR	Rua Uruguai 260, Cascavel-PR, CEP.: 85805-010	85805-010	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
74	PR	Avenida João Gualberto nº 1.000 - Alto da Glória - Curitiba - PR - Cep. 80030-000	80020-290	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
75	PR	Rua XV de Novembro, 7.337 - Centro, CEP: 85010-000 - Guarapuava/PR	85010-000	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
76	RJ	Praça do Santíssimo Salvador nº 62 - 2º e 3º Andar - Centro - Campos dos Goytacazes - RJ - Cep, 28010-000	28010-000	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
77	RJ	Rua XV de Novembro nº 4 A Torre Sul Plaza Shopping - Centro - Cep, 24020-125 Niteroi/RJ	24020-125	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
78	RJ	Av. Alberto Braune, 128 - 3º e 4º Andar - Centro - Nova Friburgo - RJ - Cep. 28613-000	28613-000	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
79	RJ	Rua Dezesesseis de Março, 155 - Sala 302 - Centro - Cep, 25620-040	25620-040	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2

80	RJ	Rua Barão de Teffé, 120 - 4º andar - Centro, CEP: 25620-010 - Petrópolis/RJ	25620-010	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
81	RJ	Av, Rio Branco, 123 - Sala 715 - Centro - Cep, 20040-006	20040-006	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
82	RJ	Avenida Nilo Peçanha, nº 151 - 8º andar - Sala 819 - Centro - Rio de Janeiro - RJ - Cep. 20020-100	20020-100	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
83	RJ	Praça Procópio Ferreira, 86 - 8º andar - Rio de Janeiro - CEP.: 20221-901	20221-901	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
84	RJ	Rua da Assembleia, nº 77 - Centro - Cep, 20011-001 - Rio de Janeiro	20011-001	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
85	RJ	Rua México, nº 74 - Centro - Cep, 20031-140	20031-140	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
86	RJ	AVENIDA AMARAL PEIXOTO - Nº 885 - CENTRO - Volta Redonda - RJ - Cep. 27253-223	27253-223	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
87	RJ	Rua Rodrigo Silva, 26 - 18º andar - Centro - Rio de Janeiro - RJ - Cep. 20011-040	20011-040	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
88	RJ	Av, Rio Branco, 311 - 8º andar - Centro - Cep, 20040-903	20040-903	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
89	RN	Av, Rio Branco, nº 1260 - Centro - Cep, 59611-400 Mossoró/RN	59611-400	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
90	RN	Av, Alexandrino de Alencar, 1402, 2º andar - Bairro Tirol - Cep, 59015-350 - Natal/RN	59015-350	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
91	RN	Avenida Brancas Dunas, 565 - Ed, Aquarius Center - Candelária - Cep, 59064-720 Natal/RN	59064-720	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
92	RN	Av, Prudente de Moraes, 2134 -Barro Vermelho - Cep, 59022-545 Natal/RN	59022-545	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
93	RO	Av, Nações Unidas, 271 - Nossa Senhora das Graças - km 01 - Cep, 76804-110 - Porto Velho/RO	76804-110	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2

94	RR	Rua Souza Júnior, 927 - São Francisco - Boa Vista - RR - Cep. 69305-040	69305-040	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
95	RS	Rua Gomes Carneiro, 1240 - Centro, CEP: 96400-130 - Bagé/RS	96400-130	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
96	RS	Rua Mariana Prezzi, nº 115 - 5º andar - Pio X - Cep, 95034-460 - Caxias do Sul/RS	95034-460	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
97	RS	AV, BENJAMIN CONSTANT, 973, 2º ANDAR, CENTRO, LAJEADO/RS, CEP 95,900-000	95900-000	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
98	RS	Av. Pedro Adams Filho 5757 - 10º E 11º andares - Centro - Cep, 93310-560 - Novo Hamburgo/SC	93310-560	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
99	RS	Rua Antônio Araújo 1190 - 4º Andar - Bairro João Lângaro - Cep, 99010-220 Passo Fundo/RS	99010-220	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
100	RS	Avenida Ferreira Viana nº 900 - esquina com a Rua Procópio Duval Gomes de Freitas na - Pelotas/RS - CEP 96085-000	96020-380	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
101	RS	Rua Mostardeiro, 483 - PRU 4 REGIÃO - Independência - Porto Alegre - RS - Cep. 90430-001	90430-001	20 - Tipo 3 28 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
102	RS	Av, Carlos Gomes, nº 1942/1950 - Conj, 1101 - Três Figueiras - Porto Alegre - RS - Cep, 90480-002	90480-002	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
103	RS	Rua 24 de Maio, 532 - Centro - Cep, 96200-003 Rio Grande/RS	96200-003	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
104	RS	Rua Félix Hoppe, 201 - AVENIDA - Santa Cruz do Sul/RS - CEP: 96815-021	96815-021	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
105	RS	Alameda Antofogasta, 96 - Bloco A - Nossa Sra, das Dores - Cep, 97050-660 Santa Maria/RS	97050-660	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
106	RS	AV ANTONIO MANOEL, 1174, Centro, Santo Angelo-RS, Cep: 98802573	98802-573	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
107	RS	Rua Bento Martins, 2497 - Sala 1102 - Centro - Cep, 97510-001 - Uruguai/RS	97510-001	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2

108	SC	Rua Doutor Léo de Carvalho, 74, 22º andar - salas 2206, 2207 e 2208 - Velha - Blumenau - SC - Cep. 89036-239	89036-239	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
109	SC	Rua Campos Novos, 211 - Centro - Cx, Postal 18, CEP: 89500-000 - Caçador/SC	89500-000	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
110	SC	Rua Barão do Rio Branco 268-D - Tel. 49 3311-2900 - Centro - Chapecó - SC - Cep. 89801-030	89801-030	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
111	SC	Rua Desembargador Pedro Silva nº 180 - Comerciarío - Edifício Bellágio, sala 101 - Cep, 88802-300 - Criciúma/SC	88802-300	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
112	SC	Rua Nossa Senhora de Lourdes, 110 - Agronômica - Cep, 88025-220 - Florianópolis/SC	88025-220	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
113	SC	Rua Padre Schuler, 56 - Centro - Cep, 88010-310 - Florianópolis/SC	88010-310	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
114	SC	Rua José Bonifácio Malburg, 195 - Centro, CEP: 88301-350 - Itajaí/SC	88301-350	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
115	SC	Rua Quinze de Novembro, nº 780 - 2º andar - Centro - Cep, 89201-600 - Joinville/SC	89201-600	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
116	SC	Rua Governador Jorge Lacerda, 126 - Centro, CEP: 88501-120 - Lages/SC	88501-120	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
117	SC	Rua Matias Piechnick, 37 - Centro, CEP: 83300-000 - Mafra/SC	83300-000	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
118	SE	Av, Beira Mar, 53 - 13 de julho Aracaju - SE - Cep, 49020-010	49020-010	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
119	SE	Av, Rio Branco, nº 168 - Centro entro - Aracaju - SE - Cep, 49010-030	49010-030	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
120	SP	Rua Campos Sales, 45 - Tel: 18 3607-8930 - Centro - Araçatuba - SP - Cep, 16010-230	16010-230	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
121	SP	Av. Rodrigo Fernando Grillo, n. 207 - Edifício Victória Business, Salas 103, 104, 105, 106 e 107 - 1º andar - Jardim Manacás - Araraquara - CEP 14.801-534.	14800-390	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2

122	SP	Rua Olga Gonzales de Oliveira, 2-35, Jardim Estoril V, Bauru/SP CEP: 17017-594	17017-594	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
123	SP	Av, Barão de Itapura, 950, 8º e 9º andares - Ed, Tiffany Office Plaza - Jd, Guanabara - Cep, 13020-431 Campinas/SP	13020-431	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
124	SP	Rua Jorge Harrat - nº 95 - Ponte Preta - Cep, 13041-550 - Campinas/SP	13041-550	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
125	SP	AV MAJOR NICACIO 1370 VILA SANTA CRUZ - CEP 14400850, Franca- SP	14400850	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
126	SP	Rua Luiz Gama - 217 - Centro - Cep, 07010-050 - Guarulhos/SP	07010-050	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
127	SP	Rua Barão de Jundiá, 1150 - 2º Piso - Centro - Jundiá/SP - CEP: 13201-012	13201-012	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
128	SP	Avenida Euclides da Cunha, 650 - Térreo - São Miguel - Cep, 17506-180 - Marília/SP	17506-180	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
129	SP	Av. Sampaio Vidal, 904 – Centro - Marília – SP – CEP: 17500-021	17500-021	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
130	SP	Av, Dionisya Alves Barreto, 233 - V, Osasco - Cep, 06086-050	06086-050	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
131	SP	Edifício Cosmopolitan - Avenida Washington Luís, 2728 Andares 9º, 8º, 5º, 2ºAndar - Jardim Paulista - CEP: 19023-450 - Presidente Prudente-SP	19015-770	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
132	SP	Rua Inácio Luiz Pinto, 313 - Alto da Boa Vista - Cep, 14025-680 - Ribeirao Preto/SP	14025-680	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
133	SP	Rua Quintino Bocaiúva, 561 - Edifício - Centro - Cep, 14015-160 - Ribeirão Preto/SP	14015-160	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
134	SP	Praça Barão do Rio Branco, Nº 30 - 7º andar - salas 705/708 - Centro - Cep, 11010-040	11010-040	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2
135	SP	Av, Dr, Pedro Lessa, nº 1930 - Aparecida - Cep, 11025-002. Santos/SP	11025-002	5 - Tipo 3 2 – Tipo 4 1 – AP Tipo 1 1 – AP Tipo 2

136	SP	Av, Maria Adelaide L, Quelhas, 55 - 3º and, - Jd, Olavo Bilac, CEP: 09725-610 - São Bernardo do Campo/SP	09725-610	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
137	SP	Avenida Juscelino Kubitschek de Oliveira, 1020 - 2o, andar - Jardim Maracanã - Cep, 15092-175	15092-175	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
138	SP	Av, Cassiano Ricardo, 521 - Bloco 1, 2º andar, Ed, Aquarius Comercial Center - Jardim Aquarius - Cep, 12240-540 São Jose dos Campos/SP	12240-540	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
139	SP	Rua Baceúnas, 65 - Vila Prudente - São Paulo-SP CEP 03127-060	03127-060	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
140	SP	Av, General Carneiro, 677 - Vila Lucy - Cep, 97050-660 - Socorocaba/SP	97050-660	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
141	SP	Rua Santa Catarina, 3580 - 2º andar - Centro, CEP: 15505-171 - Votuporanga/SP	15505-171	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
142	SP	Rua Bela Cintra, 657 - 12º andar - Consolação - São Paulo - SP - Cep. 01415-003	01415-003	10 - Tipo 3 20 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
143	SP	Rua Curuzu, 1,079 - 3º Pavimento - Centro, CEP: 18600-902 - Botucatu/SP	18600-902	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
144	SP	Rua Olegário Paiva, 275 - 3º Andar - Centro Cívico, CEP: 08780-040 - Mogi das Cruzes/SP	08780-040	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
145	SP	Avenida Santo Estevão, 76 - Vila Rezende - Cep, 13405-249 - Piracicaba/SP	13405-249	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
146	SP	Av, Inglaterra, nº 300 - Jardim das Nações - Cep, 12030-450 - Taubaté/SP	12030-450	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
147	SP	RUA JOAQUIM ALFREDO DE ALMEIDA 295 - Bairro: JARDIM YARA - São João da Boa Vista - SP	13870-511	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2
148	TO	Av, Joaquim Teotônio Segurado - Qd, 402 Sul - Conj, 01 - Lote 13 - Plano Diretor Sul - Cep, 77021-622	77021-622	5 - Tipo 3 2 - Tipo 4 1 - AP Tipo 1 1 - AP Tipo 2

APÊNDICE “C”

MODELO DE PROPOSTA DE PREÇOS

À

ADVOCACIA GERAL DA UNIÃO

Departamento de Tecnologia da Informação - DTI

Advocacia Geral da União - Departamento de Tecnologia da Informação - Setor de Indústrias Gráficas SIG, Quadra 06, Lote 800 – Brasília - DF, CEP: 70610-460.

Referência: Pregão Eletrônico nº ____/____.

Proposta que faz a empresa _____, inscrita no CNPJ nº _____ e inscrição estadual nº _____, estabelecida no(a) _____, para eventual **<CONTRATAÇÃO DE SOLUÇÃO XXXXX>** para atender às necessidades da **ADVOCACIA GERAL DA UNIÃO - AGU**, de acordo com as especificações e condições constantes do Pregão em referência, bem como do respectivo Edital e seus Anexos.

1

GRUPO	ITEM	DESCRIÇÃO	MÉTRICA	QTD	VALOR UNITÁRIO	VALOR TOTAL
	1	Switch Datacenter - Tipo 1 (Spine)	Und	4	R\$	R\$
	2	Switch Datacenter - Tipo 2 (Leaf)	Und	14	R\$	R\$
	3	Switch Acesso tipo 3 (24 portas PoE Base T)	Und	230	R\$	R\$
	4	Switch Acesso tipo 4 (48 portas PoE Base T)	Und	100	R\$	R\$
	5	Interface Ótica (transceiver) 100Gbe QSFP28 100GBase-SR4 MPO	Und	60	R\$	R\$
	6	Interface Ótica (transceiver) 40Gbe QSFP28+ 40GBase-SR4 MPO	Und	40	R\$	R\$
	7	Interface Ótica (transceiver) 25Gbe SFP28+ 25GBase-SR	Und	240	R\$	R\$
	8	Interface Ótica (transceiver) 10Gbe QSFP28	Und	60	R\$	R\$
	9	Access Point Tipo 1 (4x4)	Und	160	R\$	R\$
	10	Access Point Tipo 2 (2x2)	Und	550	R\$	R\$
	11	Solução de Gerenciamento e Controladora	Und	1	R\$	R\$
	12	Solução de NAC	Und	5000	R\$	R\$
	13	Cabo DAC para Empilhamento (Switches Tipo 3 e 4) ou Fibra	Und	170	R\$	R\$
	14	Cabo Ótico 100 Gbe QSFP28 15 mts – MPO	Und	60	R\$	R\$
	15	Cabo Ótico 40 Gbe QSFP28 10 mts - MPO	Und	40	R\$	R\$
	16	Cabo Ótico 25 Gbe SFP28 10 mts	Und	240	R\$	R\$
	17	Cabo Ótico 10 Gbe SFP+ Base-SR MMF LC 10 mts	Und	40	R\$	R\$

18	Serviço de Instalação e Configuração dos Switches de Datacenter Tipos 1 e 2	Und	22	R\$	R\$
19	Serviço de Instalação e Configuração dos Switches de Acesso Tipos 3 e 4	Und	330	R\$	R\$
20	Serviço de Instalação e Configuração dos Access Point Tipos 1 e 2	Und	710	R\$	R\$
TOTAL				R\$	R\$

1) Dados da Proposta:

Valor Total: R\$ _____ (VALOR POR EXTENSO).

SOFTWARE: (deverá ser informado, **obrigatoriamente**, o detalhamento dos softwares a serem fornecidos, quando for o caso, acompanhados dos respectivos *datasheets*)

Nome do Software: _____ Versão: _____

Nome do Fabricante: _____

Procedência: 1. Nacional [] 2. Importado: []

Sítio na WEB do Fabricante: _____

Responsável: _____ Telefone Contato: _____

HARDWARE: (deverá ser informado, **obrigatoriamente**, o detalhamento dos hardwares a serem fornecidos, quando for o caso, acompanhados dos respectivos *datasheets*)

Nome do Hardware: _____ Marca: _____ Modelo: _____

Nome do Fabricante: _____

Procedência: 1. Nacional [] 2. Importado: []

Sítio na WEB do Fabricante: _____

Responsável: _____ Telefone Contato: _____

2) Validade da Proposta: 90 (noventa) dias, a contar da data de sua apresentação.

3) Informamos, por oportuno, que nos preços apresentados acima já estão computados todos os custos necessários decorrentes da prestação dos serviços, bem como já incluídos todos os impostos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, seguros, deslocamentos de pessoal e quaisquer outros que incidam direta ou indiretamente.

4) Dados da empresa:

a) Razão Social: _____

b) CNPJ (MF) nº _____

c) Inscrição Estadual nº: _____

d) Endereço: _____

e) Telefone: _____ Fax: _____ e-mail: _____

f) Cidade: _____ Estado: _____

g) CEP: _____

h) Representante(s) legal(is) com poderes para assinar o contrato:

a. Nome: _____

b. Cargo: _____

c. CPF: _____ RG: _____ - _____

i) Dados Bancários:

a. Banco: _____

b. Agência: _____

c. Conta Corrente: _____

j) Dados para Contato:

a. Nome: _____

b. Telefone/Ramal: _____

Declaramos, para todos os fins e efeitos legais, aceitar, irrestritamente, todas as condições e exigências estabelecidas no Edital da licitação em referência e do Contrato a ser celebrado, cuja minuta constitui o Anexo “___” do Edital.

Declaramos, ainda, que inexistente qualquer vínculo de natureza técnica, comercial, econômica, financeira ou trabalhista com servidor ou dirigente da ADVOCACIA GERAL DA UNIÃO - AGU; e **que foi (realizada a Vistoria nas instalações da AGU, tomando conhecimento dos serviços a serem realizados / apresentada recusa formal de Vistoria)**, não sendo admitidas, em hipótese alguma, alegações posteriores de desenvolvimento dos serviços e de dificuldades técnicas não previstas.

<Local>, <dia> de <mês> de <ano>.

Responsável/Representante da Empresa

<Nome do Responsável>

Cargo

CPF: xxxxxx

APÊNDICE “D”

MODELO DE ORDEM DE FORNECIMENTO DE BENS/ORDEN DE SERVIÇO

INTRODUÇÃO

Por intermédio da Ordem de Serviço (OS) ou Ordem de Fornecimento de Bens (OFB) será solicitado formalmente à Contratada a prestação de serviço ou o fornecimento de bens relativos ao objeto do contrato.

O encaminhamento das demandas deverá ser planejado visando a garantir que os prazos para entrega final de todos os bens e serviços estejam compreendidos dentro do prazo de vigência contratual.

Referência: Art. 32 IN SGD Nº 94/2022.

1 – IDENTIFICAÇÃO

Nº da OS	xxxx/aaaa	Data de emissão da OS	<dd/mm/aaaa>
Contrato nº	xx/aaaa		
Objeto do Contrato	<Descrição do objeto do contrato>		
Contratada	<Nome da contratada>	CNPJ	99.999.999/9999-99
Preposto	<Nome do preposto>		
Início vigência	<dd/mm/aaaa>	Fim vigência	<dd/mm/aaaa>

ÁREA REQUISITANTE

Unidade	< Sigla – Nome da unidade>		
Solicitante	<Nome do solicitante>	E-mail	xxxxxxxxxxxxx

2 – ESPECIFICAÇÃO DOS SERVIÇOS E VOLUMES ESTIMADOS

Item	Descrição do serviço	Métrica	Valor unitário (R\$)	Qtde	Valor Total (R\$)
Valor total estimado da OS					

3 – INSTRUÇÕES/ESPECIFICAÇÕES COMPLEMENTARES

<Incluir instruções complementares à execução da OS/OFB>

<Ex.: Contatar a área solicitante para agendamento do horário de entrega>

<Ex.: Conforme consta no TERMO DE REFERÊNCIA, o recebimento provisório está condicionado à entrega do código no ambiente de homologação, e a documentação do software no repositório oficial de gestão de projetos>

4 – DATAS E PRAZOS PREVISTOS

Data de Início:	<dd/mm/aaaa>	Data do Fim:	<dd/mm/aaaa>
CRONOGRAMA DE EXECUÇÃO/ENTREGA			

Item	Tarefa/entrega	Início	Fim
1		<dd/mm/aaaa>	<dd/mm/aaaa>
...		<dd/mm/aaaa>	<dd/mm/aaaa>

5 – ARTEFATOS / PRODUTOS	
Fornecidos	A serem gerados e/ou atualizados

5 – ASSINATURA E ENCAMINHAMENTO DA DEMANDA

Autoriza-se a execução dos serviços correspondentes à presente OS, no período e nos quantitativos acima identificados.

INTEGRANTE REQUISITANTE	GESTOR DO CONTRATO
Fiscal Requisitante Matrícula/SIAPE: xxxxxx	Fiscal Técnico Matrícula/SIAPE: xxxxxx

APÊNDICE “E”

DECLARAÇÃO DE SUSTENTABILIDADE AMBIENTAL

1 – IDENTIFICAÇÃO			
CONTRATO Nº	xxxx/aaaa		
OBJETO	<objeto do contrato>		
CONTRATADA	<nome da contratada>	CNPJ	xxxxxxxxxxxxx
PREPOSTO	<Nome do Preposto da Contratada>		
GESTOR DO CONTRATO	<Nome do Gestor do Contrato>	MATR.	xxxxxxxxxxxxx

DECLARO, sob as penas da Lei nº 6.938/1981, na qualidade de proponente do procedimento licitatório, sob a modalidade Pregão Eletrônico SRP nº ____/____, instaurado pelo Processo nº _____, que atendemos aos critérios de qualidade ambiental e sustentabilidade socioambiental, respeitando as normas de proteção do meio ambiente.

Estando ciente da obrigatoriedade da apresentação das declarações e certidões pertinentes dos órgãos competentes quando solicitadas como requisito para habilitação e da obrigatoriedade do cumprimento integral ao que estabelece o art. 6º e seus incisos

Por ser a expressão da verdade, firmamos a presente.

Responsável/Representante Legal da Empresa	

<Nome>	
<CPF >	

<Local>, <dia> de <mês> de <ano>.

APÊNDICE “F”

TERMO DE RECEBIMENTO PROVISÓRIO – SERVIÇOS/COMPRAS DE TIC

INTRODUÇÃO

O Termo de Recebimento Provisório trata-se de termo detalhado que declarará que os serviços foram prestados e atendem às exigências de caráter técnico, sem prejuízo de posterior verificação de sua conformidade com as exigências contratuais, baseada nos requisitos e nos critérios de aceitação definidos no Modelo de Gestão do Contrato.

Referência: Inciso XXI, art. 2º, e alínea “i”, inciso II, art. 33 da IN SGD/ME nº 94/2022.

1. IDENTIFICAÇÃO

CONTRATO Nº	xx/aaaa		
CONTRATADA	<Nome da Contratada>	CNPJ	xxxxxxxxxxxx
Nº DA OS	<xxxx/aaaa>		
DATA DA EMISSÃO	<dd/mm/aaaa>		

2. ESPECIFICAÇÃO DOS SERVIÇOS E VOLUMES DE EXECUÇÃO

SOLUÇÃO DE TIC

<Descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado>

ITEM	DESCRIÇÃO DO BEM OU SERVIÇO	MÉTRICA	QUANTIDADE
1	<Descrição igual ao da OS de abertura>	<Ex.: PF>	<n>
...	...	...	...
...	...	...	...
TOTAL DE ITENS			

3. RECEBIMENTO

Para fins de cumprimento do disposto no art. 33, inciso II, alínea “i”, da IN SGD/ME nº 94/2022, por este instrumento ATESTO que os serviços correspondentes à <OS> acima identificada, conforme definido no Modelo de Execução do contrato supracitado, foram executados e <atende(m)/atende(m) parcialmente/não atende(m)> às respectivas exigências de caráter técnico discriminadas abaixo. Não obstante, estarão sujeitos à avaliação específica para verificação do atendimento às demais exigências contratuais, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do contrato.

Ressaltamos que o recebimento definitivo desses serviços ocorrerá somente após a verificação desses requisitos e das demais condições contratuais, desde que não se observem inconformidades ou divergências quanto às especificações constantes do TERMO DE REFERÊNCIA e do Contrato acima identificado que ensejem correções por parte da **CONTRATADA**. Por fim, reitera-se que o objeto poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o contrato.

ITEM	ESPECIFICAÇÃO TÉCNICA	ATENDIMENTO	OBSERVAÇÃO
1	<exigências técnicas definidas no TR>	...	
...	...	...	

4. ASSINATURA

FISCAL TÉCNICO
<Nome do Fiscal Técnico do Contrato> Matrícula: xxxxxx <Local>, <dia> de <mês> de <ano>.
PREPOSTO
<Nome do Preposto do Contrato> Matrícula: xxxxxx <Local>, <dia> de <mês> de <ano>.

APÊNDICE “G”

TERMO DE RECEBIMENTO DEFINITIVO

INTRODUÇÃO				
O Termo de Recebimento Definitivo declarará formalmente à Contratada que os serviços prestados ou que os bens fornecidos foram devidamente avaliados e atendem às exigências contratuais, de acordo com os requisitos e critérios de aceitação estabelecidos.				
Referência: Inciso XXII, Art. 2º e alínea “h” inciso I do art. 33, da IN SGD/ME Nº 94/2022.				
1 – IDENTIFICAÇÃO				
CONTRATO/NOTA DE EMPENHO Nº	xx/aaaa			
CONTRATADA	<Nome da Contratada>	CNPJ	xxxxxxxxxxxx	
Nº DA OS/OFB	<xxxx/aaaa>			
DATA DA EMISSÃO	<dd/mm/aaaa>			
2 – ESPECIFICAÇÃO DOS PRODUTO(S)/BEM(S)/SERVIÇOS E VOLUMES DE EXECUÇÃO				
SOLUÇÃO DE TIC				
<descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado>				
ITEM	DESCRIÇÃO DO BEM OU SERVIÇO	MÉTRICA	QUANTIDADE	TOTAL
1	<descrição igual à da OS/OFB de abertura>	<Ex.: PF>	<n>	<total>
...				
TOTAL DE ITENS				

3 – ATESTE DE RECEBIMENTO

Para fins de cumprimento do disposto no art. 33, inciso II, alínea “h”, da IN SGD/ME nº 94/2022, por este instrumento **ATESTO/ATESTAMOS** que o(s) <serviço(s)/ bem(s)> correspondentes à <OS/OFB> acima identificada foram <prestados/entregues> pela **CONTRATADA** e ATENDEM às exigências contratuais, discriminadas abaixo, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do Contrato acima indicado.

ITEM	EXIGÊNCIA CONTRATUAL	ATENDIMENTO	OBSERVAÇÃO
1	<exigência contratual estabelecida no TR >	...	
...	...	...	

...	...	...	
...	...	...	

4 – DESCONTOS EFETUADOS E VALOR A LIQUIDAR

De acordo com os critérios de aceitação e demais termos contratuais, **<não>** há incidência de descontos por desatendimento dos indicadores de níveis de serviços definidos.

<Não foram / Foram> identificadas inconformidades técnicas ou de negócio que ensejam indicação de glosas e sanções, **<cuja instrução corre em processo administrativo próprio (nº do processo)>**.

Por conseguinte, o valor a liquidar correspondente à **<OS/OFB>** acima identificada monta em R\$ **<valor>** (**<valor por extenso>**).

Referência: **<Relatório de Fiscalização nº xxxx ou Nota Técnica nº yyyy>**.

5 – ASSINATURA

GESTOR DO CONTRATO

<Nome do Gestor do Contrato>
Matrícula Siape: xxxxxxxx

<Local>, **<dia>** de **<mês>** de **<ano>**.

6 – AUTORIZAÇÃO PARA FATURAMENTO

GESTOR DO CONTRATO

Nos termos da alínea “n”, inciso I, art. 33, da IN SGD/ME nº 94/2022, AUTORIZA-SE a **CONTRATADA** a **<faturar os serviços executados / apresentar as notas fiscais dos bens entregues>** relativos à supracitada **<OS/OFB>**, no valor discriminado no item 4, acima.

<Nome do Gestor do Contrato>
Matrícula Siape: xxxxxxxx

<Local>, **<dia>** de **<mês>** de **<ano>**

7 – CIÊNCIA

PREPOSTO

<Nome do Preposto do Contrato>

Matrícula Siape: xxxxxxx

<Local>, <dia> de <mês> de <ano>

APÊNDICE H

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

INTRODUÇÃO

O Termo de Compromisso de Manutenção de Sigilo registra o comprometimento formal da Contratada em cumprir as condições estabelecidas no documento relativas ao acesso e utilização de informações sigilosas da Contratante em decorrência de relação contratual, vigente ou não.

Referência: Art. 18, Inciso V, alínea “a” da IN SGD/ME Nº 94/2022.

Pelo presente instrumento o <NOME DO ÓRGÃO>, sediado em <ENDEREÇO>, CNPJ nº <Nº do CNPJ>, doravante denominado **CONTRATANTE**, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ nº <Nº do CNPJ>, doravante denominada **CONTRATADA**;

CONSIDERANDO que, em razão do **CONTRATO N.º <nº do contrato>** doravante denominado **CONTRATO PRINCIPAL**, a **CONTRATADA** poderá ter acesso a informações sigilosas do **CONTRATANTE**;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação e Privacidade da **CONTRATANTE**;

Resolvem celebrar o presente **TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO**, doravante **TERMO**, vinculado ao **CONTRATO PRINCIPAL**, mediante as seguintes cláusulas e condições abaixo discriminadas.

1. OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela **CONTRATADA**, no que diz respeito ao trato de informações sigilosas disponibilizadas pela **CONTRATANTE** e a observância às normas de segurança da informação e privacidade por força dos procedimentos necessários para a execução do objeto do **CONTRATO PRINCIPAL** celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18 de novembro de 2011, Lei nº 13.709, de 14 de agosto de 2018, e os Decretos 7.724, de 16 de maio de 2012, e 7.845, de 14 de novembro de 2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

[...]

2. CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquela abrangida pelas demais hipóteses legais de sigilo.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

[...]

3. DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: *know-how*, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

[...]

4. DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

- I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;
- II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;
- III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

[...]

5. DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura

organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento prévio e expresso da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmos judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

6. VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

[...]

7. PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme previsto nos arts. 155 a 163 da Lei nº. 14.133, de 2021.

[...]

8. DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações, conforme definição do item 3 deste documento, disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

[...]

9. FORO

A CONTRATANTE elege o foro da <CIDADE DA CONTRATANTE>, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

[...]

10. ASSINATURAS

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

CONTRATADA	CONTRATANTE
<Nome> <Qualificação>	<Nome> Matrícula: xxxxxxxx
TESTEMUNHAS	

<Nome> <Qualificação>	<Nome> <Qualificação>
---	---

<Local>, <dia> de <mês> de <ano>.

APÊNDICE “I”

TERMO DE CIÊNCIA

INTRODUÇÃO

O Termo de Ciência visa obter o comprometimento formal dos empregados da Contratada diretamente envolvidos na contratação quanto ao conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes no órgão/entidade.

No caso de substituição ou inclusão de empregados da contratada, o preposto deverá entregar ao Fiscal Administrativo do Contrato os Termos de Ciência assinados pelos novos empregados envolvidos na execução dos serviços contratados.

Referência: Art. 18, Inciso V, alínea “b” da IN SGD/ME Nº 94/2022.

1. IDENTIFICAÇÃO

CONTRATO Nº	xxxx/aaaa		
OBJETO	<objeto do contrato>		
CONTRATADA	<nome da contratada>	CNPJ	xxxxxxxxxxxxx
PREPOSTO	<Nome do Preposto da Contratada>		
GESTOR DO CONTRATO	<Nome do Gestor do Contrato>	MATR.	xxxxxxxxxxxxx

2. CIÊNCIA

Por este instrumento, os funcionários abaixo identificados declaram ter ciência e conhecer o inteiro teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes da Contratante.

Funcionários da Contratada		
Nome	Matrícula	Assinatura
<Nome do(a) Funcionário(a)>	<xxxxxxxxxx>	
<Nome do(a) Funcionário(a)>	<xxxxxxxxxx>	
...	...	...

APÊNDICE “J”

DECLARAÇÃO DE CUMPRIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS - LEI Nº 13.709/2018

Processo Administrativo nº	Nº do Contrato	Data de Assinatura
Objeto		
Identificação da Empresa Contratada		
Nome da Empresa		
CNPJ	Inscrição Estadual	
Endereço		
Cidade	Estado	
CEP	Telefone	E-mail institucional

por meio de seu representante legal, _____, portador da Carteira de Identidade nº _____, expedida pela _____, e inscrito no CPF sob o nº _____, DECLARA QUE:

- Os eventuais dados pessoais relacionados à LICITANTE/CONTRATADA disponibilizados à AGU para efeito de participação no presente certame e que possam ser exigidos para a execução contratual, serão tratados para finalidade específica, em conformidade com os termos do artigo 7º da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).
- É vedado às partes a utilização de todo e qualquer dado pessoal repassado em decorrência da execução contratual para finalidade distinta daquela do objeto da contratação, sob pena de responsabilização administrativa, civil e criminal.
- As partes se comprometem a manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoais sensíveis – repassados em decorrência da execução contratual, em consonância com o disposto na Lei nº 13.709/2018, sendo vedado o repasse das informações a outras empresas ou pessoas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do edital/instrumento contratual.
- As partes responderão administrativa e judicialmente, em caso de causarem danos patrimoniais, morais,

individuais ou coletivos aos titulares de dados pessoais repassados em decorrência da participação no certame e eventual execução contratual, por inobservância à LGPD.

<Local>, <dia> de <mês> de <ano>.

APÊNDICE “K”

DECLARAÇÃO DE VISTORIA

DECLARO, para fins de participação no Pregão Eletrônico nº ____/____, que eu _____, portador do RG nº _____ e do CPF nº _____, representante da empresa _____, estabelecida no _____, como seu (sua) representante legal para os fins da presente declaração, compareci perante o representante da Advocacia Geral da União - AGU, tomei conhecimento de todas as informações necessárias à execução do objeto, e que vistoriei os locais de execução dos serviços, tomando ciência das condições e grau de dificuldade existentes.

<Local>, <dia> de <mês> de <ano>.

Responsável/Representante da Empresa

<Nome do Responsável>

CPF: xxxxxx

Responsável/Representante da AGU

<Nome do Responsável>

Matrícula Siape: xxxxxx

APÊNDICE “L”

DECLARAÇÃO DE RECUSA DE VISTORIA _____ **DECLARO**, para fins de participação no Pregão Eletrônico nº ____/____, que a empresa _____, CNPJ nº _____ sito à _____ na cidade de _____ UF _____, **OPTOU PELA NÃO REALIZAÇÃO DA VISTORIA TÉCNICA NAS INSTALAÇÕES FÍSICAS DA ADVOCACIA GERAL DA UNIÃO - AGU**, tendo ciência que não poderá alegar em qualquer fase da licitação ou vigência da relação contratual que não realizará os serviços em conformidade com a qualidade e requisitos exigidos.

Responsável/Representante da Empresa

<Nome do Responsável>

CPF: xxxxxx

<Local>, <dia> de <mês> de <ano>.

APÊNDICE “M”

TERMO DE CONFIDENCIALIDADE E SIGILO - VISTORIADOR

1. O colaborador (a) _____, inscrito no CPF nº _____ e em nome da licitante _____, inscrita no CNPJ nº **XX.XXX.XXX/0001-XX** atestam tomar conhecimento de informações sobre o ambiente computacional da Advocacia Geral da União - AGU, aceitam regras, condições e obrigações constantes do presente termo.
2. O objetivo deste Termo de Confidencialidade, Sigilo e uso é prover a necessária e adequada proteção às informações restritas de propriedade exclusiva da AGU reveladas ao signatário em função da vistoria realizada objeto do Edital PE **XX/XXXX**.
3. A expressão “informação restrita” abrangerá toda informação escrita, oral ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: técnicas, projetos, especificações, desenhos, cópias, diagramas, fórmulas, modelos, amostras, fluxogramas, croquis, fotografias, plantas, programas de computador, discos, pen drives, fitas, contratos, planos de negócios, processos, projetos, conceitos de produto, especificações, amostras de ideia, clientes, nomes de revendedores e/ou distribuidores, marcas e modelos utilizados, preços e custos, definições e informações mercadológicas, invenções e ideias, vulnerabilidades existentes, outras informações técnicas, financeiras ou comerciais, entre outros.
4. A licitante e usuário signatário comprometem-se a não reproduzir nem dar conhecimento a terceiros, sem a anuência formal e expressa da AGU, das informações restritas reveladas.
5. A licitante e usuário signatário comprometem-se a não utilizar, de forma diversa da prevista no Edital, as informações restritas reveladas.
6. A licitante e usuário signatário deverão cuidar para que as informações reveladas fiquem limitadas ao conhecimento próprio.
7. A licitante e usuário signatário obrigam-se a informar imediatamente a AGU 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.
8. A quebra do sigilo das informações restritas reveladas, devidamente comprovada, sem autorização expressa da AGU, possibilitará a imediata rescisão de qualquer contrato firmado entre a AGU e o signatário sem qualquer ônus para a AGU. Nesse caso, o signatário, estará sujeito, por ação ou omissão, além das eventuais multas definidas no contrato, ao pagamento ou recomposição de todas as perdas e danos sofridos pela AGU, inclusive os de ordem moral, bem como as de responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo

judicial ou administrativo.

9. O presente Termo tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de assinatura.

10. A licitante e usuário signatário manifestam explícita ciência das Portarias: Portaria nº 202/2008, Portaria-CGTI nº 01/2011, Portaria-CGTI nº 02/2011, Portaria-CGTI nº 03/2011 e Portaria - SEGEPRES nº 03/2014 disponíveis para consulta no Portal TCU.

11. E, por aceitar todas as condições e as obrigações constantes do presente Termo, o signatário assina por meio de seus representantes legais.

<Local>, <dia> de <mês> de <ano>.

Responsável/Representante da Empresa <Nome do Responsável> CPF: xxxxxx

APÊNDICE "N"

MODELO DE COMPROVAÇÃO PONTO-A-PONTO

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
REQUISITOS GERAIS PARA OS ITENS 1 e 2 (SPINE & LEAF)		
A-1	Os equipamentos deverão ser completamente instalados no prazo máximo de 90 (noventa) dias corridos, contados a partir da data de aceite de entrega;	
A-2	Todas as configurações serão realizadas em conformidade com a recomendação do fabricante dos equipamentos e softwares da solução, boas práticas de implementação recomendada pelo fabricante e os requisitos fornecidos pela AGU para o ambiente em questão. Sendo vedada a subcontratação para tais serviços	
A-3	Os serviços de instalação física e as configurações dos equipamentos poderão ocorrer, a critério da AGU, em dias não úteis (sábado e domingo e feriados), no horário acordado com a AGU, podendo ocorrer fora do horário comercial;	
A-4	A CONTRATADA deverá prover serviços profissionais do fabricante ou técnicos certificados pelo fabricante para efetuar a execução dos serviços de implantação;	
A-5	A CONTRATADA deverá fornecer com antecedência mínima de 10 (dias) dias corridos, anteriores a instalação, os dados e a documentação dos profissionais que atuarão na instalação;	
A-6	A CONTRATADA deverá providenciar todos os materiais necessários à instalação física dos equipamentos;	
A-7	A CONTRATADA deve garantir que todos os equipamentos, componentes, acessórios e cabos de conexão para interligar fisicamente todos os componentes da solução sejam entregues;	
A-8	Toda e qualquer despesa relacionada ao transporte, alimentação e hospedagem dos profissionais envolvidos deverá ocorrer por conta da CONTRATADA, sem quaisquer ônus para a AGU;	
A-9	Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;	
A-10	Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;	
A-11	Deve possuir interface dedicada para gerenciamento local do tipo "out-of-band". Esta interface de gerenciamento deverá possuir porta 1000Base-T com conector RJ-45;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
A-12	Deve suportar Q-in-Q, recurso também conhecido como <i>Stacked VLAN</i> ou VLAN sobre VLAN em que é possível configurar duas TAGs de VLAN no mesmo frame conforme padrão IEEE 802.1ad;	
A-13	Deve implementar Flow Control baseado no padrão IEEE 802.3X;	
A-14	Deve suportar o padrão IEEE 802.1Qbb (<i>Priority-based Flow Control</i>);	
A-15	Deve permitir a configuração de links agrupados virtualmente (<i>link aggregation</i>) de acordo com o padrão IEEE 802.3ad (<i>Link Aggregation Control Protocol – LACP</i>);	
A-16	Deve suportar <i>Multi-Chassis Link Aggregation</i> (MCLAG) ou mecanismo similar para agrupar suas interfaces com interfaces de outro switch de mesmo modelo de tal forma que equipamentos terceiros reconheçam as interfaces de ambos os switches como uma única interface lógica;	
A-17	Deve suportar a comutação de Jumbo Frames;	
A-18	Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;	
A-19	Deve suportar a criação de rotas estáticas em IPv4 e IPv6;	
A-20	Deve possuir hardware capaz de suportar roteamento dinâmico através dos protocolos RIP, BGP, OSPF em IPv4 e OSPF em IPv6. É obrigatória a entrega de licenças caso o software exija licenciamento adicional para ativação dos protocolos;	
A-21	Deve possuir hardware capaz de suportar roteamento <i>multicast</i> através do protocolo PIM-SSM (<i>Protocol Independent Multicast - Source-Specific Multicast</i>). É obrigatória a entrega de licenças caso o software exija licenciamento adicional para ativação dos protocolos;	
A-22	Deve possuir hardware capaz de suportar o protocolo VRRP ou mecanismo similar de redundância de gateway. É obrigatória a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo;	
A-23	Deve suportar <i>Bidirectional Forwarding Detection</i> (BFD). É obrigatória a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo;	
A-24	Deve ser capaz de criar múltiplas tabelas de roteamento através de VRF (<i>Virtual Routing and Forwarding</i>). É obrigatória a entrega de licenças caso o software exija licenciamento adicional para ativação deste recurso;	
A-25	Deve permitir configurar determinadas portas físicas do switch como interfaces de camada 3 que tenha suporte às funções de roteamento sem requerer a configuração de uma VLAN;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
A-26	Deve implementar serviço de DHCP Server e DHCP Relay;	
A-27	Deve suportar o protocolo <i>Virtual Extensible LAN (VXLAN)</i> para permitir que o tráfego de camada 2 seja encaminhado para outros locais da rede via roteamento;	
A-28	Deve suportar IGMP <i>Snooping</i> para controle de tráfego de <i>multicast</i> , permitindo a criação de pelo menos 500 (quinhentos) grupos;	
A-29	Deve suportar o protocolo <i>Multicast Listener Discovery (MLD) Snooping</i> para otimizar as comunicações multicast em IPv6;	
A-30	Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch e outro switch da rede (port mirroring / SPAN);	
A-31	Deve permitir o espelhamento de uma porta ou de um grupo de portas para uma porta especificada em outro equipamento através de RSPAN e ERSPAN;	
A-32	Deve implementar <i>Spanning Tree</i> conforme os padrões IEEE 802.1w (<i>Rapid Spanning Tree</i>) e IEEE 802.1s (<i>Multiple Spanning Tree</i>). Deve implementar pelo menos 30 (trinta) instâncias de <i>Multiple Spanning Tree</i> ;	
A-33	Deve implementar recurso conhecido como <i>PortFast</i> ou <i>Edge Port</i> para que uma porta de acesso seja colocada imediatamente no status " <i>Forwarding</i> " do <i>Spanning Tree</i> após sua conexão física;	
A-34	Deve implementar mecanismo de proteção da " <i>root bridge</i> " do algoritmo <i>Spanning Tree</i> para prover defesa contra-ataques do tipo " <i>Denial of Service</i> " no ambiente nível 2;	
A-35	Deve permitir a suspensão de recebimento de BPDUs (<i>Bridge Protocol Data Units</i>) caso a porta esteja colocada no modo " <i>fast forwarding</i> " (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;	
A-36	Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;	
A-37	Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (<i>flapping</i>) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;	
A-38	Deverá possuir controle de <i>broadcast</i> , <i>multicast</i> e <i>unicast</i> nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
A-39	Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;	
A-40	Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;	
A-41	Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);	
A-42	Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF;	
A-43	Deverá implementar ao menos 1 (um) dos seguintes mecanismos de prevenção contra congestão de tráfego: Weighted Round Robin (WRR), WRED (<i>Weighted Random Early Detection</i>) ou <i>Weighted Fair Queuing</i> (WFQ);	
A-44	Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;	
A-45	Deve suportar o mecanismo <i>Explicit Congestion Notification</i> (ECN) para notificar o emissor que há uma congestão ocorrendo e com isso evitar que os pacotes sejam descartados;	
A-46	Deve implementar mecanismo de proteção contra ataques do tipo <i>IPspoofing</i> para mensagens de IPv6 <i>Router Advertisement</i> . A licitante deverá comprovar que esse recurso opera em camada 3 (L3);	
A-47	Deverá implementar mecanismo de proteção contra ataques que utilizam o protocolo ARP. Devendo, no mínimo, proteger contra os seguintes tipos de ataques: man-in-the-middle (IPv4), ARP Spoofing, ARP Storm e ARP Flood Attack;	
A-48	Deve implementar DHCP <i>Snooping</i> em IPv4 e IPv6 para mitigar problemas com servidores DHCP que não estejam autorizados na rede;	
A-49	Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;	
A-50	Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;	
A-51	Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
A-52	Deve suportar MAC <i>Authentication Bypass</i> (MAB);	
A-53	Deve implementar RADIUS CoA (Change of Authorization);	
A-54	Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;	
A-55	Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;	
A-56	Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;	
A-57	Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;	
A-58	Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;	
A-59	Deve suportar RADIUS <i>Authentication</i> e RADIUS <i>Accounting</i> através de IPv6;	
A-60	Deve suportar o protocolo PTP (<i>Precision Time Protocol</i>);	
A-61	Deve implementar <i>Netflow</i> , <i>sFlow</i> ou similar;	
A-62	Deve suportar o envio de mensagens de log para servidores externos através de syslog;	
A-63	Deve suportar o protocolo SNMP (<i>Simple Network Management Protocol</i>) nas versões v1, v2c e v3;	
A-64	Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (<i>Command Line Interface</i>);	
A-65	Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;	
A-66	Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);	
A-67	Deve permitir ser gerenciado através de IPv6;	
A-68	Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;	
A-69	Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
A-70	Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;	
A-71	Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;	
A-72	Deverá suportar protocolo <i>OpenFlow</i> v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;	
A-73	Deverá suportar ser configurado e monitorado através de REST API;	
A-74	Deve possuir ferramenta para captura de pacotes que auxiliarão na identificação de problemas na rede. Deve permitir a utilização de filtros para selecionar o tráfego que deverá ser capturado e permitir a exportação dos pacotes através de arquivo. pcap para análise em software <i>Wireshark</i> ;	
A-75	Deve ser capaz de armazenar no mínimo duas versões de firmware simultaneamente em sua memória flash;	
A-76	Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;	
A-77	Deve suportar temperatura de operação de até 40º Celsius;	
A-78	Deve possuir MTBF (<i>Mean Time Between Failures</i>) igual ou superior a 10 (dez) anos;	
ID	ITEM 1 - SWITCH DATACENTER TIPO 1 - SPINE	
B-1	Camada na arquitetura " <i>Spine-and-Leaf</i> " que deve ser suportada.	
B-2	Deve possuir 32 (trinta e duas) slots QSFP28 para conexão de fibras ópticas do tipo 100GBase-X operando em 40GbE e 100GbE, para interconexão com os servidores, sistemas de armazenamento, firewalls, balanceadores de carga, dentre outros equipamentos de rede.	
B-3	Deve possuir capacidade de comutação de pelo menos 6400 Gbps Duplex;	
B-4	Deve possuir capacidade de encaminhar, no mínimo, 4300 Mpps (Milhões de pacotes por segundo);	
B-5	Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;	
B-6	Deve suportar 1000 (um mil) ACLs de entrada;	
B-7	Latência < 1 us.	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
B-8	16 MB Memória mínima de Buffer (<i>Packet Buffer</i>).	
B-9	Capacidade mínima de 72.000 endereços na tabela MAC (<i>MAC address table size</i>).	
B-10	Direção do fluxo de ar <i>Front to back</i> .	
B-11	Deve ser fornecido com fontes de alimentação redundantes do tipo <i>hotswap</i> , com capacidade para operar em tensões de 110V e 220V;	
B-12	Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;	
ID	ITEM 2 - SWITCH DATACENTER TIPO 2 - LEAF	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
C-1	Camada na arquitetura " <i>Spine-and-Leaf</i> " que deve ser suportada.	
C-2	Deve possuir 48 (quarenta e oito) slots para conexão de fibras ópticas do tipo 1GE/10GE/25GE SFP28, para interconexão com os servidores, sistemas de armazenamento, firewalls, balanceadores de carga, dentre outros equipamentos de rede.	
C-3	Adicionalmente, deve possuir ao menos 8 (oito) slots 40GE/100GE QSFP28 para conexão de fibras ópticas operando com velocidades de 40 e 100 Gigabit Ethernet;	
C-4	Deve possuir capacidade de comutação de pelo menos 4 Tbps Duplex;	
C-5	Deve possuir capacidade de encaminhar no mínimo 2.4 Mbps (Milhões de pacotes por segundo);	
C-6	Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;	
C-7	Deve suportar 3000 (três mil) ACLs de entrada;	
C-8	Latência < 1us.	
C-9	12 MB Memória mínima de Buffer (<i>Packet Buffer</i>).	
C-10	Capacidade mínima de 96.000 endereços na tabela MAC (<i>MAC address table size</i>).	
C-11	Direção do fluxo de ar <i>Front to back</i> .	
C-12	Tipo de rack a ser instalado.	
C-13	Deve ser fornecido com fontes de alimentação redundantes do tipo hot-swap, com capacidade para operar em tensões de 110V e 220V;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
C-14	Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;	
ID	ITEM 3 - SWITCH DE ACESSO 24 PORTAS TIPO 3 (PoE BASE T)	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
D-1	Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;	
D-2	Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a autonegociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);	
D-3	Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;	
D-4	Deverá implementar os padrões IEEE 802.3af (<i>Power over Ethernet – PoE</i>) e IEEE 802.3at (<i>Power over Ethernet Plus – PoE+</i>) com PoE <i>budget</i> de 370W a serem alocados em qualquer uma das portas 1000Base-T;	
D-5	Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;	
D-6	Deve possuir 1 (uma) interface USB;	
D-7	Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 180 Mpps (milhões de pacotes por segundo);	
D-8	Deve suportar 4000 (quatro mil) VLANs ativas de acordo com o padrão IEEE 802.1Q;	
D-9	Deve possuir tabela MAC com suporte a 32.000 endereços;	
D-10	Deve operar com latência igual ou inferior à 1us (microsegundo);	
D-11	Deve implementar Flow Control baseado no padrão IEEE 802.3X;	
D-12	Deve permitir a configuração de links agrupados virtualmente (<i>link aggregation</i>) de acordo com o padrão IEEE 802.3ad (<i>Link Aggregation Control Protocol – LACP</i>);	
D-13	Deve suportar a comutação de Jumbo Frames;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
D-14	Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;	
D-15	Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;	
D-16	Deve suportar a criação de rotas estáticas em IPv4 e IPv6;	
D-17	Deve implementar serviço de DHCP Relay;	
D-18	Deve suportar IGMP <i>snooping</i> para controle de tráfego de <i>multicast</i> , permitindo a criação de pelo menos 1000 (mil) entradas na tabela;	
D-19	Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);	
D-20	Deve implementar <i>Spanning Tree</i> conforme os padrões IEEE 802.1w (<i>Rapid Spanning Tree</i>) e IEEE 802.1s (<i>Multiple Spanning Tree</i>). Deve implementar pelo menos 15 (quinze) instâncias de <i>Multiple Spanning Tree</i> ;	
D-21	Deve implementar recurso conhecido como <i>PortFast</i> ou <i>Edge Port</i> para que uma porta de acesso seja colocada imediatamente no status " <i>Forwarding</i> " do <i>Spanning Tree</i> após sua conexão física;	
D-22	Deve implementar mecanismo de proteção da "root bridge" do algoritmo <i>Spanning Tree</i> para prover defesa contra-ataques do tipo " <i>Denial of Service</i> " no ambiente nível 2;	
D-23	Deve permitir a suspensão de recebimento de BPDUs (<i>Bridge Protocol Data Units</i>) caso a porta esteja colocada no modo " <i>fast forwarding</i> " (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;	
D-24	Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;	
D-25	Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;	
D-26	Deverá possuir controle de <i>broadcast</i> , <i>multicast</i> e <i>unicast</i> nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar <i>rate limit</i> ;	
D-27	Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego:	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
	endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;	
D-28	Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;	
D-29	Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);	
D-30	Deverá implementar priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF;	
D-31	Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;	
D-32	Deverá implementar mecanismo de proteção contra ataques do tipo <i>man-in-the-middle</i> que utilizam o protocolo ARP;	
D-33	Deve implementar DHCP <i>Snooping</i> para mitigar problemas com servidores DHCP que não estejam autorizados na rede;	
D-34	Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;	
D-35	Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;	
D-36	Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;	
D-37	Deve suportar MAC <i>Authentication Bypass</i> (MAB);	
D-38	Deve implementar RADIUS CoA (<i>Change of Authorization</i>);	
D-39	Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;	
D-40	Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;	
D-41	Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;	
D-42	Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
D-43	Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;	
D-44	Deve suportar RADIUS <i>Authentication</i> e RADIUS <i>Accounting</i> através de IPv6;	
D-45	Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;	
D-46	Deve permitir a customização do tempo em segundos em que um determinado MAC <i>Address</i> aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);	
D-47	Deve ser capaz de gerar log de eventos quando um novo endereço MAC <i>Address</i> for aprendido dinamicamente nas interfaces, quando o MAC <i>Address</i> mover entre interfaces do mesmo switch e quando o MAC <i>Address</i> for removido da interface;	
D-48	Deve suportar o protocolo NTP (<i>Network Time Protocol</i>) ou SNTP (<i>Simple Network Time Protocol</i>) para a sincronização do relógio;	
D-49	Deve suportar o envio de mensagens de log para servidores externos através de syslog;	
D-50	Deve suportar o protocolo SNMP (<i>Simple Network Management Protocol</i>) nas versões v1, v2c e v3;	
D-51	Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);	
D-52	Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;	
D-53	Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);	
D-54	Deve permitir ser gerenciado através de IPv6;	
D-55	Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;	
D-56	Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;	
D-57	Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
D-58	Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;	
D-59	Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;	
D-60	Deverá suportar protocolo <i>OpenFlow</i> v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;	
D-61	Deverá suportar ser configurado e monitorado através de REST API;	
D-62	Deve suportar o padrão IEEE 802.3az (<i>Energy Efficient Ethernet</i> - EEE);	
D-63	Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;	
D-64	Deve suportar temperatura de operação de até 45º Celsius;	
D-65	Deve possuir MTBF (<i>Mean Time Between Failures</i>) igual ou superior a 10 (dez) anos;	
D-66	Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;	
D-67	Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;	
ID	ITEM 4 - SWITCH DE ACESSO 48 PORTAS TIPO 4 (PoE BASE T)	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
D-68	Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;	
D-69	Deve possuir 48 (quarenta e oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a autonegociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);	
D-70	Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
D-71	Deverá implementar os padrões IEEE 802.3af (<i>Power over Ethernet – PoE</i>) e IEEE 802.3at (<i>Power over Ethernet Plus – PoE+</i>) com PoE <i>budget</i> de 740W a serem alocados em qualquer uma das portas 1000Base-T;	
D-72	Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;	
D-73	Deve possuir 1 (uma) interface USB;	
D-74	Deve possuir capacidade de comutação de pelo menos 176 Gbps e ser capaz de encaminhar até 250 Mpps (milhões de pacotes por segundo);	
D-75	Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;	
D-76	Deve possuir tabela MAC com suporte a 32.000 endereços;	
D-77	Deve operar com latência igual ou inferior à 1us (microsegundo);	
D-78	Deve implementar Flow Control baseado no padrão IEEE 802.3X;	
D-79	Deve permitir a configuração de links agrupados virtualmente (<i>link aggregation</i>) de acordo com o padrão IEEE 802.3ad (<i>Link Aggregation Control Protocol – LACP</i>);	
D-80	Deve suportar a comutação de Jumbo Frames;	
D-81	Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;	
D-82	Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;	
D-83	Deve suportar a criação de rotas estáticas em IPv4 e IPv6;	
D-84	Deve implementar serviço de DHCP Relay;	
D-85	Deve suportar IGMP <i>snooping</i> para controle de tráfego de <i>multicast</i> , permitindo a criação de pelo menos 1000 (mil) entradas na tabela;	
D-86	Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (<i>port mirroring / SPAN</i>);	
D-87	Deve implementar <i>Spanning Tree</i> conforme os padrões IEEE 802.1w (<i>Rapid Spanning Tree</i>) e IEEE 802.1s (<i>Multiple Spanning Tree</i>). Deve implementar pelo menos 15 (quinze) instâncias de <i>Multiple Spanning Tree</i> ;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
D-88	Deve implementar recurso conhecido como <i>PortFast</i> ou <i>Edge Port</i> para que uma porta de acesso seja colocada imediatamente no status " <i>Forwarding</i> " do <i>Spanning Tree</i> após sua conexão física;	
D-89	Deve implementar mecanismo de proteção da "root bridge" do algoritmo <i>Spanning Tree</i> para prover defesa contra-ataques do tipo " <i>Denial of Service</i> " no ambiente nível 2;	
D-90	Deve permitir a suspensão de recebimento de BPDUs (<i>Bridge Protocol Data Units</i>) caso a porta esteja colocada no modo " <i>fast forwarding</i> " (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;	
D-91	Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;	
D-92	Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (<i>flapping</i>) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;	
D-93	Deverá possuir controle de <i>broadcast</i> , <i>multicast</i> e <i>unicast</i> nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;	
D-94	Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;	
D-95	Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;	
D-96	Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);	
D-97	Deverá implementar priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF;	
D-98	Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;	
D-99	Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;	
D-100	Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
D-101	Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;	
D-102	Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;	
D-103	Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;	
D-104	Deve suportar MAC Authentication Bypass (MAB);	
D-105	Deve implementar RADIUS CoA (Change of Authorization);	
D-106	Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;	
D-107	Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;	
D-108	Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;	
D-109	Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;	
D-110	Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;	
D-111	Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;	
D-112	Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;	
D-113	Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);	
D-114	Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;	
D-115	Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
D-116	Deve suportar o envio de mensagens de log para servidores externos através de syslog;	
D-117	Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;	
D-118	Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);	
D-119	Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;	
D-120	Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);	
D-121	Deve permitir ser gerenciado através de IPv6;	
D-122	Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;	
D-123	Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;	
D-124	Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;	
D-125	Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;	
D-126	Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;	
D-127	Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;	
D-128	Deverá suportar ser configurado e monitorado através de REST API;	
D-129	Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);	
D-130	Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;	
D-131	Deve suportar temperatura de operação de até 45º Celsius;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
D-132	Deve possuir MTBF (<i>Mean Time Between Failures</i>) igual ou superior a 10 (dez) anos;	
D-133	Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;	
D-134	Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;	
ID	ITEM 5 - PONTO DE ACESSO TIPO 1 – 2X2	
E-1	Ponto de acesso (AP) que permita acesso dos dispositivos à rede através do wireless e que possua todas as suas configurações centralizadas em controlador/gerenciador wireless;	
E-2	Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;	
E-3	Deve identificar automaticamente o controlador/gerenciador wireless ao qual se conectará;	
E-4	Deve permitir ser gerenciado remotamente através de links WAN;	
E-5	Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;	
E-6	Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;	
E-7	O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (wIDS/wIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação;	
E-8	Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;	
E-9	Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente;	
E-10	Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN;	
E-11	Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
E-12	Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;	
E-13	Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at.	
E-14	O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless;	
E-15	Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPsec;	
E-16	Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;	
E-17	Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;	
E-18	Deve permitir operação em modo Mesh;	
E-19	Deve possuir potência de irradiação mínima de 21dBm em ambas as frequências;	
E-20	Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio;	
E-21	Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);	
E-22	Deve suportar OFDMA;	
E-23	Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax;	
E-24	Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;	
E-25	Deve suportar BSS Coloring;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
E-26	Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;	
E-27	Deve possuir sensibilidade mínima de -94dBm quando operando em 5GHz com MCS0 (HT20);	
E-28	Deve possuir antenas internas ao equipamento com ganho mínimo de 2.6dBi em 2.4GHz e 3.75 dBi em 5GHz;	
E-29	Em conjunto com o controlador/gerenciador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;	
E-30	Em conjunto com o controlador/gerenciador wireless, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;	
E-31	Em conjunto com o controlador/gerenciador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz;	
E-32	Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;	
E-33	Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS);	
E-34	Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 14 (quatorze) SSIDs com operação simultânea;	
E-35	Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);	
E-36	Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3;	
E-37	Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;	
E-38	Deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAPMSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST;	
E-39	Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
E-40	Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;	
E-41	Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;	
E-42	Deve implementar o padrão IEEE 802.11e;	
E-43	Deve implementar o padrão IEEE 802.11h;	
E-44	Deve implementar o padrão IEEE 802.3az;	
E-45	Deve suportar ser gerenciado via SNMP;	
E-46	Deve suportar consultas via REST API;	
E-47	Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação;	
E-48	Deve ser capaz de operar em ambientes com temperaturas entre 0 e 40° C;	
E-49	Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar;	
E-50	Deve possuir indicadores luminosos (LED) para indicação de status;	
E-51	O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores/gerenciador wireless deste processo;	
E-52	Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste TERMO DE REFERÊNCIA deverão ser fornecidos;	
E-53	Deve possuir certificado emitido pela Wi-Fi Alliance;	
ID	ITEM 6 - PONTO DE ACESSO TIPO 2 – 4X4	
F-1	Ponto de acesso (AP) que permita acesso dos dispositivos à rede através do wireless e que possua todas as suas configurações centralizadas em controlador/gerenciador wireless;	
F-2	Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador/gerenciador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;	
F-3	Deve identificar automaticamente o controlador/gerenciador wireless ao qual se conectará;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
F-4	Deve permitir ser gerenciado remotamente através de links WAN;	
F-5	Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;	
F-6	Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;	
F-7	O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (wIDS/wIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação;	
F-8	Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;	
F-9	Deve permitir a conexão de 500 (quinhentos) clientes wireless simultaneamente;	
F-10	Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN;	
F-11	Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;	
F-12	Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;	
F-13	Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at.	
F-14	O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless;	
F-15	Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPsec;	
F-16	Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador,	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
	ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;	
F-17	Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;	
F-18	Deve permitir operação em modo Mesh;	
F-19	Deve possuir potência de irradiação mínima de 23dBm em ambas as frequências;	
F-20	Deve suportar, no mínimo, operação MIMO 4x4 com 4 fluxos espaciais permitindo data rates de até 2400 Mbps em um único rádio;	
F-21	Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);	
F-22	Deve suportar OFDMA;	
F-23	Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax;	
F-24	Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;	
F-25	Deve suportar BSS Coloring;	
F-26	Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;	
F-27	Deve possuir sensibilidade mínima de -94dBm quando operando em 5GHz com MCS0 (HT20);	
F-28	Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz e 5GHz;	
F-29	Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;	
F-30	Em conjunto com o controlador wireless, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;	
F-31	Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
F-32	Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;	
F-33	Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS);	
F-34	Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 14 (quatorze) SSIDs com operação simultânea;	
F-35	Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES) com 802.1x ou Chave pré-compartilhada, WEP, Captive Portal, lista de bloqueio e lista de permissões MAC;	
F-36	Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3;	
F-37	Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;	
F-38	Deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAPMSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST;	
F-39	Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;	
F-40	Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;	
F-41	Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;	
F-42	Deve implementar o padrão IEEE 802.11e;	
F-43	Deve implementar o padrão IEEE 802.11h;	
F-44	Deve implementar o padrão IEEE 802.3az;	
F-45	Deve suportar ser gerenciado via SNMP;	
F-46	Deve suportar consultas via REST API;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
F-47	Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação;	
F-48	Deve ser capaz de operar em ambientes com temperaturas entre 0 e 40° C;	
F-49	Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar;	
F-50	Deve possuir indicadores luminosos (LED) para indicação de status;	
F-51	O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;	
F-52	Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste TERMO DE REFERÊNCIA deverão ser fornecidos;	
F-53	Deve possuir certificado emitido pela Wi-Fi Alliance;	
ID	ITEM 7 – SOLUÇÃO DE GERENCIAMENTO E CONTROLADORA	
G-1	A solução deve ser baseada em máquina virtual ou appliance físico do mesmo fabricante da solução ofertada objeto deste certame que vão do item 1 a 6, e ter como objetivo gerenciar de modo centralizado todos os equipamentos a partir de uma única console de administração;	
G-2	Caso a solução seja fornecida em Appliance Virtual compatível com as plataformas a seguir. Será de responsabilidade da contratada o fornecimento do servidor/hardware com todos os licenciamentos necessários para a plena funcionalidade da solução.	
G-3	Caso seja necessário complemento de outras soluções para atendimento dos itens descritos ele deverá ser do mesmo fabricante.	
G-4	Deverá estar devidamente licenciada de maneira perpétua;	
G-5	Gerenciar, no mínimo, 2000 (duas mil) unidades dos equipamentos da solução do Item 1 a 6 de forma simultânea;	
G-6	Caso a solução seja entregue como appliance virtual, este deve suportar:	
G-7	Deve ser compatível com pelo menos 1(um) dos hypervisors VMWare 6.5 e superiores, Hyper-V 2016 e superiores e KVM;	
G-8	A Solução deverá ser fornecida com o número de vCPU necessário para atendimento do item.	
G-9	Deve suportar vMotion com o intuito de possibilitar alta disponibilidade da máquina virtual a nível de servidor físico. Caso esta funcionalidade não seja suportada, a solução deve ser entregue em alta disponibilidade;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
G-10	Caso a solução seja entregue como appliance físico, este deve suportar:	
G-11	Pelo menos 2x RJ45 10GE ports, 2x SFP+ ports;	
G-12	Suportar a configuração de RAID 0/1,1s/5,5s/6,6s/10/50/60 para os discos internos;	
G-13	Possuir fonte de alimentação interna, redundante e hot-swap;	
G-14	Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;	
G-15	Deve suportar o conceito de multi-tenancy visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução.	
G-16	A solução deve permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança;	
G-17	Solução que permita administrar de maneira centralizada todos os elementos responsáveis pelo gerenciamento da segurança e infraestrutura de rede e que garanta suporte a processos relativos à LGPD;	
G-18	A solução deverá estar devidamente licenciada para administrar todos os pontos de acesso, switches e elementos responsáveis pelo gerenciamento da segurança e infraestrutura de rede deste processo pelo período do contrato;	
G-19	Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste TERMO DE REFERÊNCIA deverão ser fornecidos;	
G-20	A solução deve possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem/conflitem com outras (shadowing) ou ainda garantir que esta exigência seja plenamente atendida por meio diverso;	
G-21	A solução deve permitir agendamento para a execução de configurações nos elementos administrados;	
G-22	A solução deve permitir a criação e execução de scripts em elementos administrados de maneira programada;	
G-23	A solução deverá permitir uma configuração simplificada do painel de controle, que permita ao gerenciador da rede obter rapidamente uma visão da saúde de sua rede, incluindo Wi-Fi, Ethernet, e verificar se há algo que requer atenção.	
G-24	A solução deverá permitir utilizar informações de tendência e SLAs configurados para determinar a saúde boa ou ruim da sua rede.	
G-25	A solução deverá permitir rapidamente obter sugestões de remediação para problemas de rede detectados.	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
G-26	A solução deverá permitir que a solução de gerenciamento entregue diretamente às informações de seu interesse e permita que o gerenciador da rede aprofunde o quanto desejar nas informações registradas sobre o dispositivo.	
G-27	A solução deverá permitir prever problemas potenciais antes que ocorram, receber ações recomendadas e automatizarem tarefas, como correções, através Aprendizado de Máquina (Machine Learning).	
G-28	A solução deve permitir a criação de templates de configuração a serem aplicados de maneira centralizada e padronizada em elementos da rede sem fio e switches;	
G-29	As seguintes características do SSID devem ser configuradas nos pontos de acesso através dos templates: nome do SSID, endereçamento DHCP a ser entregue aos clientes wireless, métodos de autenticação e agendamento da disponibilidade do SSID;	
G-30	As seguintes características devem ser configuradas nos pontos de acesso através dos templates: potência de transmissão Wi-Fi, escolha do canal, tamanho do canal, configuração do algoritmo de seleção automática de potência e canal, configuração de short guard interval, modo de operação e acesso administrativo ao ponto de acesso;	
G-31	As seguintes características de segurança devem ser configuradas na rede sem fio através dos templates: configuração da detecção de Rogue Aps e configuração de assinaturas de wIDS ou wIPS;	
G-32	A solução deve listar os elementos administrados e seu status de operação;	
G-33	A solução deve listar todos os clientes conectados na rede sem fio, o nome do ponto de acesso ao qual o cliente está conectado, qualidade do sinal da conexão de cada cliente, tipo de dispositivo utilizado na conexão e nome do SSID;	
G-34	A solução deve listar todos os rogue APs na rede sem fio, nome do SSID do propagado, canal impactado, nível de sinal detectado e nome do ponto de acesso que detectou o Rogue AP;	
G-35	A solução deve garantir visão centralizada do status e estatísticas de uso das interfaces dos switches;	
G-36	A solução deve permitir o agrupamento dos elementos administrados para aplicação de políticas ou templates de configuração;	
G-37	A solução deverá realizar o backup automático das configurações dos elementos e permitir o retorno (rollback) de uma versão de configuração salva previamente;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
G-38	A solução deverá possibilitar que o administrador visualize e compare diferentes versões de configurações dos elementos, sejam elas configurações vigentes, configurações anteriores e configurações antigas;	
G-39	A solução deverá possuir sistema de backup e restauração de todas as configurações da própria ferramenta de administração centralizada;	
G-40	A solução deverá identificar a versão de firmware em execução nos elementos administrados e garantir que quando houver novas versões de software para eles, que seja realizada a distribuição e instalação remota de maneira centralizada;	
G-41	A solução deve permitir criar políticas/templates que definam a versão de firmware a ser distribuída e instalada em elementos administrados.	
G-42	A solução deve garantir visão centralizada das estatísticas de uso da rede sem fio;	
G-43	A solução deve garantir visão centralizada das aplicações mais acessadas na rede, com informações sobre o volume total de dados trafegados para cada aplicação e a identificação dos usuários que fizeram os acessos;	
G-44	A solução deve garantir visão centralizada das categorias de websites mais acessados na rede, com informações sobre o volume total de dados trafegados para cada categoria e a identificação dos usuários que fizeram os acessos;	
G-45	A solução deve garantir visão centralizada dos usuários que mais trafegaram dados na rede, com informações sobre os hosts aos quais o usuário estava conectado, volume de dados trafegados e os endereços de destino que foram acessados;	
G-46	Deverá garantir a integridade do item de configuração, através de bloqueio de alterações, em caso de acesso simultâneo de dois ou mais administradores no mesmo ativo;	
G-47	Permitir acesso concorrente de administradores, permitindo ainda que seja definida uma cadeia de aprovação das alterações realizadas;	
G-48	Como parte da visibilidade dos dispositivos gerenciados centralmente, a solução deve ter visibilidade das verificações de saúde do link, desempenho da aplicação, utilização da largura de banda e conformidade com o nível de serviço definido;	
G-49	Deve ter a capacidade de permitir o provisionamento de comunidades VPN e monitorar as conexões VPN de todos os dispositivos gerenciados a partir de uma única console, além de exibir sua localização geográfica em um mapa;	
G-50	Permitir usar palavras chaves ou cores para facilitar identificação de regras;	
G-51	Permitir localizar em quais regras um objeto (ex. computador, serviço etc.) está sendo utilizado;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
G-52	Permitir criação de regras que fiquem ativas em horário definido;	
G-53	Realizar o backup das configurações para permitir o retorno de uma configuração salva;	
G-54	Possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras, ou garantir que esta exigência seja plenamente atendida por meio diverso.	
G-55	Possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;	
G-56	Possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;	
G-57	Garantir que quando houver novas versões de software dos equipamentos, seja realizada a distribuição e instalação remota de maneira centralizada;	
G-58	Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;	
G-59	Deve suportar a definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;	
G-60	Deve suportar autenticação de administradores em base local e de modo remoto por meio de RADIUS, LDAP, TACACS+ e PKI.	
G-61	Permitir criar na solução de gerência templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração;	
G-62	Permitir criar scripts personalizados, que sejam executados de forma centralizada em um ou mais dispositivos gerenciados com comandos de CLI dos mesmos;	
G-63	Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;	
G-64	A gerência centralizada deve vir acompanhada com solução de visualização de logs e geração de relatórios. Esta solução pode ser disponibilizada no mesmo equipamento de gerenciamento centralizado, ou fornecido em equipamento externo do mesmo fabricante;	
G-65	Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;	
G-66	A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
G-67	Solução que deverá administrar e controlar de maneira centralizada os switches do mesmo fabricante da solução ofertada;	
G-68	A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso;	
G-69	A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;	
G-70	A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados;	
G-71	A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de, no mínimo, 11.312 (onze mil e trezentos e doze) portas de switch ou um total de 352 (trezentos e cinquenta e dois) switches (Spine 4 switches = 128 portas, Leafs 18 switches = 864 portas, Acesso 24 portas 230 switches = 5.520 portas, Acesso 48 portas 100 switches = 4.800 portas que compõe esse projeto);	
G-72	A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas;	
G-73	A solução deve permitir, através da interface gráfica, configurar VLANs e distribuí-las automaticamente nos switches e pontos de acesso por ela gerenciados;	
G-74	A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;	
G-75	A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;	
G-76	A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;	
G-77	A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;	
G-78	A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;	
G-79	A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;	
G-80	A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
G-81	A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;	
G-82	Solução que deverá administrar e controlar de maneira centralizada os pontos de acesso wireless do mesmo fabricante da solução ofertada;	
G-83	Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste TERMO DE REFERÊNCIA deverão ser fornecidos;	
G-84	A solução deve estar pronta e licenciada para garantir o gerenciamento de até 710 (setecentos e dez) pontos de acesso wireless simultaneamente em um único appliance;	
G-85	Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;	
G-86	Deve permitir a conexão de dispositivos wireless que transmitam tráfego IPv4 e IPv6;	
G-87	A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor;	
G-88	A solução deverá ser capaz de gerenciar pontos de acesso que estejam conectados remotamente através de links WAN e Internet;	
G-89	O controlador wireless deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;	
G-90	A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;	
G-91	Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;	
G-92	O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional para suportar a conexão dos túneis originados dos pontos de acesso;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
G-93	Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPsec;	
G-94	Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso de Split-Tunneling por SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;	
G-95	Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;	
G-96	Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre controladora e ponto de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X;	
G-97	A solução deve permitir definir quais redes serão tuneladas até o controlador e quais redes serão comutadas diretamente pela interface do ponto de acesso;	
G-98	A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;	
G-99	A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;	
G-100	A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;	
G-101	A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;	
G-102	A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
	ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;	
G-103	A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;	
G-104	A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de off-channel/Background scanning. Quando realizada através de off-channel/Background scanning, a solução deve ser capaz de mensurar a utilização do ponto de acesso para caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;	
G-105	A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;	
G-106	A solução deve permitir a adição de controlador redundante que deve monitorar a disponibilidade e sincronizar as configurações do controlador principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;	
G-107	A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;	
G-108	A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;	
G-109	A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;	
G-110	Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;	
G-111	A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;	
G-112	A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
G-113	A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;	
G-114	A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;	
G-115	A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;	
G-116	A solução deve implementar técnicas de <i>Call Admission Control</i> para limitar o número de chamadas simultâneas;	
G-117	A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;	
G-118	Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;	
G-119	A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados;	
G-120	A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de <i>Airtime</i> ;	
G-121	A solução deve suportar a configuração do BLE (<i>Bluetooth Low Energy</i>) nos pontos de acesso que tenham este recurso;	
G-122	A solução deve suportar recurso que ignore <i>Probe Requests</i> de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os <i>Probe Requests</i> sejam ignorados;	
G-123	A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;	
G-124	A solução deve permitir a configuração de <i>Short Guard Interval</i> para o rádio 5GHz;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
G-125	A solução deve implementar recurso conhecido como <i>Airtime Fairness</i> (ATF) para controlar o uso de airtime nos SSIDs;	
G-126	A solução deve ser capaz de reconfigurar automaticamente os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências;	
G-127	A solução deve implementar recurso para controle de URLs acessadas na rede wireless através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários e SSID;	
G-128	A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede wireless;	
G-129	O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria;	
G-130	A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas;	
G-131	A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução;	
G-132	A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento;	
G-133	A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e para websites/domínios específicos;	
G-134	A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS;	
G-135	A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede wireless com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig;	
G-136	O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
G-137	A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução;	
G-138	A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede wireless;	
G-139	A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução;	
G-140	A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações;	
G-141	A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI;	
G-142	A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada SSID;	
G-143	A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS;	
G-144	A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes wireless;	
G-145	A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: - Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); - Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; - ASLEAP; - Null Probe Response or Null SSID Probe Response; - Long Duration; - Ataques contra Wireless Bridges; - Weak WEP; - Invalid MAC OUI.	
G-146	A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication;	
G-147	A solução deve implementar mecanismos de proteção contra ataques do tipo ARP <i>Poisoning</i> na rede wireless;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
G-148	Permitir configurar o bloqueio na comunicação entre os clientes wireless conectados a um determinado SSID;	
G-149	Deve implementar autenticação administrativa através dos protocolos RADIUS ou TACACS;	
G-150	Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA, WPA2, and WPA3;	
G-151	Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;	
G-152	A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;	
G-153	Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;	
G-154	A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;	
G-155	A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (<i>Change of Authorization</i>) para autenticações 802.1X;	
G-156	Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;	
G-157	A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informar as credenciais válidas para acesso à rede;	
G-158	A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;	
G-159	A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;	
G-160	A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;	
G-161	A solução deve permitir que a página de autenticação seja hospedada em servidor externo;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
G-162	A solução deve permitir a configuração do captive portal com endereço IPv6;	
G-163	A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;	
G-164	A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;	
G-165	Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;	
G-166	A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários;	
G-167	A solução deverá suportar <i>Single Sign-On</i> (SSO);	
G-168	A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada;	
G-169	A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede;	
G-170	A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;	
G-171	A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;	
G-172	A solução deve permitir a configuração do captive portal com endereço IPv6;	
G-173	A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;	
G-174	A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;	
G-175	Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
G-176	A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários;	
G-177	A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários;	
G-178	O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria;	
G-179	A solução deverá permitir a customização de página de bloqueio apresentada aos usuários;	
G-180	Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo continuar;	
G-181	A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados;	
G-182	A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas;	
G-183	A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução;	
G-184	A solução deve implementar recurso de DHCP Server (em IPv4 e IPv6) para facilitar a configuração de redes visitantes;	
G-185	A solução deve suportar o protocolo OSPF em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura de rede LAN e WLAN;	
G-186	A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;	
G-187	A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;	
G-188	A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;	
G-189	A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
G-190	A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no equipamento ao qual os APs estejam fisicamente conectados;	
G-191	A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;	
G-192	A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;	
G-193	A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps;	
G-194	A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;	
G-195	A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);	
G-196	A solução deve permitir a captura de pacotes na rede wireless e exportá-los em arquivos no formato .pcap;	
G-197	A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;	
G-198	A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;	
G-199	A solução deve permitir o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;	
G-200	A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;	
G-201	A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;	
G-202	A solução deve permitir a atualização de firmware individualmente nos pontos de acesso, garantindo a gestão e operação simultânea de pontos de acesso com firmwares diferentes;	
G-203	A solução deve possuir ferramentas de diagnósticos e debug;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
G-204	A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de um ponto de acesso;	
G-205	A solução deve suportar comunicação com elementos externos através de REST API;	
G-206	A solução deverá ser compatível e gerenciar os pontos de acesso deste processo;	
G-207	Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;	
ID	ITEM 7 – SOLUÇÃO DE GERENCIAMENTO E CONTROLADORA – Solução de Identificação e Autenticação Centralizada	
H-1	Características E Funcionalidades Gerais	
H-2	Poderá ser entregue em equipamento único ou com composição de equipamentos. para atender as funcionalidades exigidas.	
H-3	Deverá ser compatível e integrável com itens deste termo.	
H-4	Deverá possuir licenciamento para, no mínimo, 15.000 usuários locais ou remotos;	
H-5	Deverá possuir licenciamento para até 800 grupos de usuários,	
H-6	Deverá possuir licenciamento para até 50 certificados de usuários.	
H-7	Deverá possuir licenciamento para até 15.000 tokens para dispositivos móveis, compatíveis com sistemas Android e iOS.	
H-8	Requisitos gerais:	
H-9	Suportar administração em interface gráfica (GUI) por HTTP e/ou HTTPS;	
H-10	Suporta administração em interface baseada em linhas de comando (CLI) por TELNET e/ou SSH;	
H-11	Permitir definir perfis de administradores para a solução, de modo que possa segmentar a responsabilidade dos administradores por tarefas operativas;	
H-12	Possuir Indicador visual, centralizado, de informações críticas (estado da licença, versão de firmware, consumo de CPU/Memória/Disco, quantidade de usuários criados e licenciados);	
H-13	Suportar a atualização do firmware via interface gráfica, por processo simplificado e intuitivo;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
H-14	Suportar customização de mensagens padrão da solução como páginas de erro, portais de autenticação, auto registro, reset de senha e outros. Suportar também a inclusão, alteração e remoção de imagens nas mensagens/páginas sem a necessidade de recursos ou conectividade externa;	
H-15	Suportar configuração de Alta Disponibilidade (HA), reduzindo ao máximo os períodos de interrupção;	
H-16	Suportar implementações de HA como "Ativo-Passivo" ou sincronizando configurações entre duas caixas ativas;	
H-17	Permitir sincronismo automático de configurações entre todos os equipamentos que componham a solução em HA;	
H-18	Suportar implementação de HA sincronizando configurações com appliances em localidades geograficamente separadas;	
H-19	Suportar a opção de backup criptografado;	
H-20	Suportar backup automatizado (agendados por critérios pré-definidos), não somente sob demanda;	
H-21	Suportar o backup completo da configuração, incluindo base de usuários, grupos, tokens, certificados, configurações de single-sign-on e etc. A solução deve também permitir a restauração de toda configuração diretamente da interface gráfica;	
H-22	Suportar NTP (Network Time Protocol), visando o sincronismo de hora/data;	
H-23	Suportar SNMP v1, v2 e v3 permitindo consultar MIB própria e envio de Traps;	
H-24	Suportar nativamente Trap SNMP indicando mudança de status de HÁ;	
H-25	Suportar captura de pacotes através da interface gráfica para Troubleshoot avançado em ferramentas de análise de pacotes (ex.: Wireshark);	
H-26	O equipamento deve permitir o envio de e-mails relacionados a reset de senha, aprovação de novos usuários, auto-registro de usuários e autenticação de segundo fator (token);	
H-27	Deve suportar o envio de mensagens SMS para os usuários através de gateways SMS de terceiros ou seu próprio serviço de envio de SMS, sendo este segundo licenciado ou não;	
H-28	Deve suportar o registro de todos os eventos que os usuários de sua base de dados local realizem com suas contas, tais como criação de um usuário, troca de senha de um usuário e alteração de informação gerais;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
H-29	Autenticação:	
H-30	A solução deve efetuar autenticação para a gerência de identidade dos usuários da rede, ajudando a simplificar a administração dos mesmos sendo um ponto central de controle de autenticação, onde múltiplos métodos de autenticação possam ser consolidados;	
H-31	Deve suportar autenticação em dois fatores (two-factor authentication);	
H-32	Deve possuir suporte a autenticação de dois fatores em pelo menos dois tipos diferentes de tokens, sendo o primeiro físico (token), e o segundo lógico como software para dispositivos móveis, e-mail ou SMS, permitindo que seja dada a escolha de qual dos tipos utilizar para cada usuário;	
H-33	A solução deve permitir que se defina um perfil de complexidade mínimo para as senhas de todos os usuários cadastrados na base de dados local, possibilitando a definição de número mínimo de letras minúsculas, letras maiúsculas, caracteres numéricos, caracteres especiais e etc;	
H-34	A solução deve permitir a criação de política de bloqueio automático de usuários após uma quantidade de falhas de autenticação, assim evitando ataques de força bruta;	
H-35	A solução deve suportar a criação de usuários em base local, que poderão ser utilizados na autenticação dos dispositivos conforme necessidade;	
H-36	A solução deve permitir a criação em massa de usuários na base de dados local através da importação de lista de usuários a serem criados contida em arquivos externos;	
H-37	A solução deve permitir a criação de novos usuários na base de dados local e que o criador/administrador possa definir uma senha no momento de criação;	
H-38	A solução deve permitir a criação de novos usuários na base de dados local de forma que o equipamento gere uma senha aleatória e envie automaticamente ao usuário;	
H-39	A solução deve permitir a criação de novos usuários na base de dados local sem a definição de senha, exigindo que o mesmo utilize o token como único fator de autenticação;	
H-40	Deve permitir associar os tokens aos usuários criados localmente na base de dados;	
H-41	Deve permitir que os próprios usuários façam o registro dos seus tokens e relatem a perda de um token automaticamente, sem necessidade de envolver um administrador;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
H-42	Remoção automática em massa de usuários desabilitados, baseado em critérios definidos;	
H-43	A solução deve possuir formas que permitam que os usuários locais possam fazer o reset de suas senhas de forma segura sem a intervenção de administradores, através de correio eletrônico ou pergunta de segurança;	
H-44	Deve suportar a criação de grupos de usuários, que poderão ser utilizados na autenticação dos dispositivos conforme necessidade;	
H-45	Os tokens deverão gerar códigos com no mínimo 6 dígitos e intervalos não superiores à 60 segundos	
H-46	Suportar autenticação em dois fatores por hardware dedicado (Token);	
H-47	Suportar autenticação em dois fatores por aplicativo mobile (iOS e Android);	
H-48	Suportar autenticação em dois fatores por envio de mensagem SMS;	
H-49	Suportar autenticação em dois fatores por envio de e-mail;	
H-50	Suportar a sincronização com dispositivo em hardware de geração de OTP (One Time Password);	
H-51	Deve permitir sincronizar os tokens com o equipamento para o correto funcionamento dos mesmos	
H-52	Deve permitir desabilitar um token quando este seja roubado ou extraviado, permitindo sua reativação posterior quando/se for recuperado;	
H-53	Deve permitir a desassociação de um token a um usuário e associá-lo à outro usuário quando necessário, permitindo assim que sejam reaproveitados;	
H-54	Deve continuar permitindo a autenticação de dois fatores em clientes windows mesmo com a máquina offline;	
H-55	Deve prover um portal web para o auto-registro dos usuários, de forma que o mesmo acesse, preencha os seus dados e submeta o registro. Após o usuário efetuar o registro, o administrador deverá ser notificado automaticamente para aprovar ou negar o cadastro do mesmo antes de que ele seja ativado;	
H-56	A solução deve funcionar como servidor RADIUS (Remote Authentication Dial-In User Server), proporcionando autenticação aos dispositivos compatíveis com tal protocolo;	
H-57	A solução deve suportar a integração com servidor RADIUS remoto;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
H-58	A solução pode funcionar como servidor LDAP (Lightweight Directory Access Protocol), proporcionando autenticação aos dispositivos compatíveis com tal protocolo;	
H-59	A solução deve suportar a integração com servidor LDAP remoto (como Microsoft Active Directory);	
H-60	A solução deve suportar autenticação de usuários com credenciais de mídias sociais de terceiros como Facebook, Twitter, LinkedIn e Google+;	
H-61	A solução deve permitir que usuários que não possuam uma conta local ou em mídias sociais se autentiquem através de um rápido cadastro, que garanta o mínimo de rastreabilidade, através da validação de endereços de e-mail ou número de telefone;	
H-62	A solução deve permitir o login automático de usuários visitantes depois de se registrarem com sucesso;	
H-63	A solução deve permitir configurar os parâmetros de rede (como as configurações de WiFi) em um endpoint baixando um script ou um executável através do portal de visitantes;	
H-64	Deve suportar Security Assertion Markup Language (SAML), agindo como um Provedor de Identidade (Identity Provider - IDP) estabelecendo um relacionamento de confiança para autenticação segura de usuários tentando acessar um Provedor de Serviços (Service Provider -SP);	
H-65	Deve permitir integração com bases do Azure Directory e GSuite;	
H-66	Por meio do SAML, deve permitir integrações com SPs variados, tais como Office 365;	
H-67	Deve suportar FIDO;	
H-68	A solução deve apontar a última vez (data) em que um token foi utilizado;	
H-69	A solução deve suportar OpenID Connect (OIDC);	
H-70	Deve suportar autenticação adaptativa;	
H-71	Deve suportar regras granulares no processo de autenticação. Ex: usuários se autenticando na VPN precisam utilizar MFA, mas, o mesmo usuário, em portal web, não precise informar o token;	
H-72	Deve suportar push notification;	
H-73	Controle baseado em porta:	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
H-74	A solução deve suportar nativamente (sem redirecionamentos) a integração e autenticação de switches e outros dispositivos compatíveis com o padrão 802.1X	
H-75	Suportar os seguintes métodos 802.1X EAP: PEAP (MSCHAPv2), EAP-TTLS, EAP-TLS e EAP-GTC	
H-76	Suportar interoperabilidade com equipamentos de acesso (switches) de outros fabricantes, para autenticação de portas junto a solução, através dos padrões 802.1X	
H-77	Deve suportar bypass de autenticação 802.1X para dispositivos conhecidos que não suportem 802.1X, a liberação deverá ser feita baseada no endereço MAC dos equipamentos previamente cadastrados, estes terão acesso a rede sem necessidade de autenticação ou ação do usuário ou dispositivo	
H-78	Certificados:	
H-79	A solução deve atuar como Autoridade Certificadora (CA)	
H-80	Deve permitir a administração de certificados digitais, com emissão e revogação	
H-81	Deve permitir o uso de CA's confiáveis para validação de certificados emitidos por CA's externas	
H-82	Deve suportar OCSP para que se possa fornecer uma lista de certificados revogados (CRL)	
H-83	Deve prover repositório para autenticação de VPN Site-to-Site através de Certificados	
H-84	Deve suportar SCEP Server (Simple Certificate Enrollment Protocol), permitindo a assinatura de requisições de certificados digitais (CSR) automaticamente ou com interação do administrador	
H-85	Deve ser capaz de importar outros certificados de CA's assim como a lista de certificados revogados	
H-86	Deve ser capaz de permitir ao administrador do sistema gerar, assinar e revogar certificados digitais para os usuários	
H-87	Suportar ao protocolo ACME para geração de certificados	
H-88	Serviço De Autenticação Única (Single Sign-On)	
H-89	A solução deve prover capacidade de serviço SSO (Single Sign-On), com autenticação transparente (passiva) de usuários em sistemas compatíveis	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
H-90	Deve ser capaz de integrar-se a um diretório ativo (Windows AD) e poder oferecer a funcionalidade de SSO, onde a autenticação automática/transparente via SSO para os serviços necessários é baseada na autenticação prévia feita pelo usuário no domínio	
H-91	Deve permitir definir uma lista de usuários de SSO que serão ignorados, evitando assim interferência de contas de serviços tais como antivírus ou scripts via GPO	
H-92	Deve suportar análise de arquivos syslog enviados de fonte remota, para uso pelo serviço de SSO	
H-93	Deve suportar Security Assertion Markup Language (SAML), agindo como autenticador de um Provedor de Serviços (Service Provider - SP) solicitando informações de identidade de usuários a Provedores de Identidade (Identity Providers - IDP's) de terceiros	
H-94	Deve suportar SSO baseado em Radius (RSSO - RADIUS Single Sign-On)	
H-95	Deve suportar RSSO Accounting Proxy permitindo a recepção de pacotes radius de accounting, a modificação destes pacotes e o encaminhamento dos mesmos para vários outros pontos	
H-96	Segundo Fator De Autenticação Para Redes Privadas Virtuais	
H-97	Deve ser do mesmo fabricante dos itens 1, 2, 3, 4, 9 e 10 que compõe a presente solução.	
H-98	Possuir licenciamento perpétuo de token e sem limites de transferência para outros dispositivos.	
H-99	Permitir o download gratuito do seu provisionamento.	
H-100	Suportar exclusão e adição de novos tokens.	
H-101	Instalado no dispositivo móvel sem que haja a necessidade de alteração de sua configuração, ou mesmo a capacidade de formatar o dispositivo móvel de forma remota.	
H-102	Garantir a privacidade do dispositivo móvel.	
H-103	Deve requerer a permissão do proprietário para envio de notificações ou qualquer tipo de alteração nas configurações.	
H-104	Deve suportar, no mínimo, as principais plataformas de mobile do mercado: iOS, Android e Windows	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
H-105	Suportar a geração dinâmica das sementes de token, minimizando a exposição online.	
H-106	Suportar ativação através da utilização de QR Codes e manual.	
H-107	Criptografar o armazenamento de sementes utilizadas na geração do token.	
H-108	Ter a capacidade de gerar senhas de uso único (One Time Programmable - OTP) baseado em tempo (TOTP) ou evento (HTOP) compatível com OATH.	
H-109	Suportar a ocultação do token para tokens baseados em tempo (TOTP).	
H-110	Ter a capacidade de proteger abertura do aplicativo através de PIN, Impressão Digital e Face Security.	
H-111	Exibir o intervalo de tempo OTP.	
H-112	Exibir do número de série do token.	
H-113	Ser compatível com o relógio da Apple ou relógios Smart watch.	
H-114	Suportar que a senha gerada possa ser copiada para a área de transferência.	
H-115	Suportar detalhes de login enviados ao telefone para aprovação com um toque.	
H-116	Ter um serviço de provisionamento dinâmico, onde apenas na atribuição de um token a um usuário a semente é criada e é removida durante o download ou após um tempo limite configurável.	
H-117	Homologado para as especificações OTP RFC6238 e RFC4226.	
H-118	Ter a capacidade de realizar vinculação com o dispositivo móvel;	
H-119	Suportar à sua utilização como segundo fator de autenticação para acesso VPN via SSL ou IPSEC, sem a necessidade de utilização de um servidor RADIUS.	
ID	ITEM 7 – SOLUÇÃO DE GERENCIAMENTO E CONTROLADORA – Gerencia centralizada para coleta, armazenamento e análise automatizada de registros	
I-1	A solução deve ser baseada em máquina virtual ou appliance físico do mesmo fabricante da solução do 1 à 6 e ter como objetivo a coleta, armazenamento e análise automatizada de registros em modo centralizado de todos os equipamentos a partir de uma única console de administração;	
I-2	Poderá ser entregue em formato de appliance físico ou appliance virtual;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
I-3	Deverá estar devidamente licenciada para:	
I-4	Suportar a coleta de, no mínimo, 150 GB de logs diários;	
I-5	Permitir espaço de armazenamento de, no mínimo, 24 TB;	
I-6	Deve possuir solução de retenção de logs com capacidade mínima para armazenar os logs da solução por 6 (seis) meses. (Marco Civil Art.13 – 1 ano)	
I-7	A solução dedicada de logs, deve suportar relatórios listando os endpoints por localidade e fabricante, usuários associados, além de relatórios de inventário, devices registrados e roques.	
I-8	Caso a solução seja entregue como appliance virtual, este deve suportar:	
I-9	Deve ser compatível com pelo menos 1 (um) dos hypervisors VMWare 6.5 e superiores, Hyper-V 2016 e superiores, e KVM;	
I-10	A Solução deverá ser fornecida com o número de vCPU necessário para atendimento do item.	
I-11	Não deverá existir limite para a expansão da memória RAM no appliance virtual;	
I-12	Deve suportar vMotion com o intuito de possibilitar alta disponibilidade da máquina virtual a nível de servidor físico. Caso esta funcionalidade não seja suportada, a solução deve ser entregue em alta disponibilidade;	
I-13	Caso a solução seja entregue como appliance físico, este deve suportar:	
I-14	Pelo menos 4 x RJ45 GE e 2 x SFP;	
I-15	Suportar a configuração de RAID 0/1,1s/5,5s/10 para os discos internos;	
I-16	Possuir fonte de alimentação interna, redundante e hot-swap;	
I-17	Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;	
I-18	Realizar o backup das configurações para permitir o retorno de uma configuração salva;	
I-19	Possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;	
I-20	Deve suportar a definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
I-21	Deve suportar o conceito de multi-tenancy visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução.	
I-22	A solução deve permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança;	
I-23	Através da análise de tráfego de rede, web e DNS, deve suportar a verificação de máquinas potencialmente comprometidas ou usuários com uso de rede suspeito;	
I-24	Realizar agregação via pontuação, para geração de um veredito sobre máquinas comprometidas na rede e atividades suspeitas;	
I-25	Utilizar técnicas de machine learning para a captura de índices de comprometimento, através de URLs, domínios e endereços IPs maliciosos;	
I-26	Deve possuir um painel com as informações de máquinas comprometidas indicando informações de endereço IP dos usuários, veredito, número de incidentes etc.;	
I-27	Deve oferecer um portal do cliente fácil de usar permitindo acesso às capacidades seguras como: monitoramento e políticas e objetos, painéis analíticos, visualizações e relatórios, auditoria e recursos adicionais, como documentação;	
I-28	Suporte a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;	
I-29	Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;	
I-30	Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;	
I-31	Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;	
I-32	Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;	
I-33	Deve possuir mecanismos de remoção automática para logs antigos;	
I-34	Permitir importação e exportação de relatórios	
I-35	Deve ter a capacidade de criar relatórios no formato HTML, PDF, XML e CSV;	
I-36	Deve permitir exportar os logs no formato CSV;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
I-37	Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;	
I-38	Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;	
I-39	A solução deve ter relatórios predefinidos;	
I-40	Deve permitir o envio automático dos logs para um servidor FTP externo a solução;	
I-41	Deve ter a capacidade de personalizar a capa dos relatórios obtidos;	
I-42	Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;	
I-43	Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;	
I-44	Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;	
I-45	Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;	
I-46	Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;	
I-47	Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;	
I-48	Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;	
I-49	Permitir o envio por e-mail relatórios automaticamente;	
I-50	Deve permitir que o relatório seja enviado por e-mail para o destinatário específico;	
I-51	Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;	
I-52	Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;	
I-53	Deve permitir o uso de filtros nos relatórios;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
I-54	Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;	
I-55	Permitir especificar o idioma dos relatórios criados;	
I-56	Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;	
I-57	Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;	
I-58	Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;	
I-59	Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;	
I-60	Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;	
I-61	Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;	
I-62	Deve permitir visualizar em tempo real os logs recebidos;	
I-63	Deve permitir o encaminhamento de log no formato syslog;	
I-64	Deve permitir o encaminhamento de log no formato CEF (Common Event Format);	
I-65	Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;	
I-66	Deve ser capaz de visualizar alertas de surtos e baixar automaticamente manipuladores de eventos e relatórios relacionados;	
I-67	Deve permitir o time de resposta a incidentes identificar se um artefato malicioso de "Zero Day" encontrado na rede faz parte de alguma campanha específica de malware, se foi visto até o momento somente na rede da instituição;	
I-68	Caso o malware faça parte de alguma campanha, deve ser detalhado qual o objetivo dela, tipos de indústria que já foram alvo do malware, comportamento malicioso conhecido sobre o malware e quais são os autores;	
I-69	Deve permitir gerar alertas de eventos a partir de logs recebidos;	
I-70	A solução deve possuir garantia, suporte e atualizações ao software durante a vigência do contrato;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
ID	ITEM 8 – SOLUÇÃO DE NAC	
J-1	Solução de controle de acesso à rede	
J-2	Solução de controle de acesso à rede, a ser ofertado em formato de appliance físico ou virtual, este que deverá estar disponível para as plataformas Vmware ESXi, AWS e Microsoft Azure;	
J-3	Deve ser uma solução multi-vendor capaz de suportar os switches e concentrador VPN da AGU;	
J-4	A solução deve suportar capacidade de expansão para até 25.000 endpoints simultâneos, sem demandar do cliente a troca do hardware/VM;	
J-5	A solução deve estar licenciada para operação com, pelo menos, 5000 endpoints conectados simultaneamente;	
J-6	A solução deve ser entregue em alta disponibilidade;	
J-7	A solução deve ser capaz de inspecionar tanto IoT quanto estações/notebooks, sem depender de recursos como 802.1X e Mac-address bypass (MAB);	
J-8	Para estações de trabalho, deve suportar verificação de compliance em VPN IPsec e SSL;	
J-9	A licença contemplada deverá suportar todas as características exigidas neste TERMO DE REFERÊNCIA;	
J-10	A solução deve permitir diferentes perfis de administração, com a capacidade de limitar e controlar a quantidade de acesso permitido às funcionalidades disponíveis, dependendo do grupo administrativo da organização ao qual o usuário pertence;	
J-11	Deve detectar e classificar automaticamente o tipo dos dispositivos conectados na rede sem a necessidade de softwares instalados nos dispositivos;	
J-12	Deve permitir determinar o perfil dos dispositivos descobertos por meio de métodos que não exigem a instalação de agentes, incluindo pelo menos os seguintes:	
J-13	Consultas em DHCP Fingerprint;	
J-14	Consultas via protocolos HTTP/HTTPS;	
J-15	Consultas via protocolo SNMP;	
J-16	Consultas via protocolo SSH;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
J-17	Consultas via protocolo Telnet;	
J-18	Consultas de portas TCP;	
J-19	Consultas de portas UDP;	
J-20	MAC OUI;	
J-21	Consultas via protocolo WMI;	
J-22	Protocolo ONVIF;	
J-23	Base assinaturas pré-definidas;	
J-24	A solução deve ser capaz de reconhecer as seguintes informações sobre os dispositivos conectados à rede:	
J-25	Endereço MAC;	
J-26	Endereço IP;	
J-27	Sistema operacional;	
J-28	Nome do host;	
J-29	Horário de conexão;	
J-30	Usuário conectado;	
J-31	Localização.	
J-32	A solução deve ser capaz de reconhecer os seguintes sistemas operacionais em execução nos dispositivos conectados à rede:	
J-33	Android;	
J-34	Apple iOS para iPhone, iPod e iPad;	
J-35	Chrome OS;	
J-36	Linux;	
J-37	MacOS X;	
J-38	Windows 10 ou superior;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
J-39	Deve lembrar o perfil atribuído a cada dispositivo e verificar sua validade a cada conexão;	
J-40	Deve permitir a designação de um sponsor para autorizar a categorização dos dispositivos;	
J-41	Deve permitir a recategorização periódica de dispositivos;	
J-42	Deve permitir a importação de um arquivo CSV contendo informações sobre os dispositivos a serem registrados;	
J-43	A solução deve incluir a detecção de dispositivos desconhecidos conectados à rede e adotar medidas de controle para limitar o acesso;	
J-44	A solução deve suportar autenticação através de EAP-PEAP e EAP-TLS;	
J-45	A solução deve suportar RADIUS Change of Authorization;	
J-46	A solução deve suportar MAC Address Bypass;	
J-47	A solução deve consultar bases LDAP e Active Directory para a identificação de usuários e grupos de usuários;	
J-48	A solução deve permitir a criação de políticas de controle que combinem informações sobre a identidade do usuário e tipo de dispositivo com objetivo de autorizar dinamicamente o acesso à rede;	
J-49	Deve permitir a definição dos horários em que os dispositivos serão autorizados a conectar na rede;	
J-50	Deve garantir a segmentação dinâmica da rede e aplicação de políticas de segurança, tendo como base variadas combinações, como login do AD e atributos (departamento, cidade, e-mail, telefone), características da máquina (asset tag, hostname), localidade e horário;	
J-51	A solução deve incluir recursos de gerenciamento de visitantes, permitindo a criação de diferentes perfis de utilização e autorização a serem associados aos usuários, distinguindo por exemplo prestadores de serviços dos visitantes;	
J-52	A solução deve permitir o cadastro dos usuários visitantes na base interna da ferramenta para que não seja necessário realizar consultas em bases externas;	
J-53	A solução deve possuir ferramenta que permita a geração automática de credenciais para usuários visitantes com login e respectivas senhas;	
J-54	A solução deve possuir ferramenta que permita a criação de credenciais para eventos;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
J-55	Deve permitir a definição de complexidade da senha dos usuários visitantes;	
J-56	Deve ser possível definir um período de validade para as contas de usuários visitantes;	
J-57	Deve ser possível definir data e horário para início e encerramento das contas de usuários visitantes;	
J-58	A autenticação e autorização dos usuários visitantes deve ocorrer através de portal captivo acessível via browser web;	
J-59	Os visitantes em hipótese alguma deverão ter acesso à Internet e rede interna antes que a autenticação seja concluída e o usuário seja autorizado;	
J-60	A solução deve vincular o login do visitante à máquina utilizada no acesso;	
J-61	Deve suportar a validação de credenciais:	
J-62	Em base local interna à ferramenta;	
J-63	Em servidores RADIUS;	
J-64	Em servidores LDAP.	
J-65	A solução deve autenticar usuários visitantes através das seguintes redes sociais: Facebook, LinkedIn e Twitter;	
J-66	A ferramenta deve permitir que os usuários visitantes possam realizar auto registro através do preenchimento de cadastro disponível em portal web;	
J-67	Deve permitir a customização dos campos obrigatórios e opcionais para o cadastro de auto registro;	
J-68	A solução deve suportar o envio da senha de acesso aos visitantes através de SMS e e-mail;	
J-69	Deve ser possível definir um período para que os usuários visitantes sejam obrigados a se reautenticar;	
J-70	Deve permitir a designação de grupos de usuários com função de sponsor que ficarão responsáveis por autorizar o acesso dos usuários visitantes e prestadores de serviços;	
J-71	Os usuários do tipo sponsor poderão cadastrar previamente um usuário visitante. O portal de cadastro e gerenciamento de usuários visitantes não deve permitir gerência administrativa dos demais recursos da solução;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
J-72	A solução deve permitir a customização da aparência do captive portal, permitindo editar textos e inserir imagens;	
J-73	Os usuários do tipo sponsor podem ser cadastrados na base local da ferramenta ou fazer parte de grupo de usuários em base LDAP/Active Directory;	
J-74	A solução deve incluir recursos de conformidade de endpoint. Antes de permitir que os dispositivos acessem a rede, a solução deve garantir que estes cumpram requisitos de segurança, integridade e conformidade;	
J-75	Deve permitir o uso de software agente instalado no dispositivo e agentes evanescentes que não precisam ser instalados;	
J-76	Tanto para IoTs quanto para estações de trabalho, se configurado, não devem ter qualquer acesso à rede de produção enquanto não forem inspecionados e identificados;	
J-77	Se um dispositivo não passar os testes de conformidade, deve ser possível:	
J-78	Não forçar a remediação;	
J-79	Forçar a remediação imediatamente enviando o dispositivo à rede de quarentena;	
J-80	Permitir a remediação retardada, ou seja, dando um período de tolerância para que o usuário corrija o problema. Caso os problemas persistam, o dispositivo deve ser colocado em quarentena;	
J-81	A solução deve permitir verificações de conformidade em endpoint que façam uso do sistema operacional:	
J-82	Windows 10 ou superior;	
J-83	MacOS;	
J-84	Linux.	
J-85	Para garantir a conformidade com as políticas de segurança, a solução deve permitir que sejam verificados os seguintes itens antes de autorizar o acesso de um endpoint na rede:	
J-86	Presença de software de antivírus instalado e em execução;	
J-87	Versão do sistema operacional;	
J-88	Nome de domínio do Active Directory ao qual a estação Windows pertença;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
J-89	Serviços em execução para estações Windows;	
J-90	Informações sobre um determinado certificado digital em estações Windows;	
J-91	Registros ou chaves de registro para estações Windows;	
J-92	Processos em execução para estações Windows, Linux e MacOS;	
J-93	Arquivo armazenado em um determinado diretório para estações Windows, Linux e MacOS;	
J-94	Pacotes instalados em estações Linux e MacOS.	
J-95	A solução deve ser capaz de monitorar quando um serviço requerido for desabilitado ou interrompido em computadores. Além disso deve enviar a estação para quarentena de forma a garantir a conformidade com a política de segurança;	
J-96	Deve possuir serviço RADIUS interno, além de permitir o uso de RADIUS externos;	
J-97	Deve permitir a distribuição de agentes através de, pelo menos, os seguintes métodos: a) Programas de gerenciamento e distribuição de software; b) GPO do Active Directory; c) Captive Portal	
J-98	Deve permitir a atualização automática ou programada dos agentes instalados nas máquinas;	
J-99	O agente instalado nos computadores deve notificar os usuários com mensagens informativas em casos de eventos;	
J-100	Quando em quarentena, um portal web deve ser apresentado aos usuários com informações sobre as razões pelas quais estes foram movidos para o isolamento;	
J-101	A solução deve compartilhar a identificação dos usuários e/ou dispositivos autenticados para a plataforma de segurança da rede via SSO, de forma que sejam vinculadas aos acessos de Internet, provendo rastreabilidade futura;	
J-102	No que tange compliance, quando houver sucesso, falha ou alerta, a solução deve permitir as seguintes ações: alerta, envio de e-mail e SMS, desabilitar o host, envio de mensagem direta para o host envolvido e executar políticas adicionais de compliance;	
J-103	A solução deve integrar com plataformas de MDM, suportando pelo menos: Air Watch, Google GSuite, JAMF, MaaS360, Microsoft Intune, Mobile Iron, Nozomi, Citrix Endpoint Management;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
J-104	Deve suportar integração com soluções de patching;	
J-105	Deve suportar integração com soluções de análise de vulnerabilidades;	
J-106	A solução deve possuir dashboard que apresente informações e estatísticas relevantes de forma resumida;	
J-107	A solução deve permitir a customização do dashboard para apresentar as informações que o administrador considera relevante;	
J-108	A solução deve permitir a consulta de informações e alteração de parâmetros de configuração via REST API;	
J-109	A solução deve armazenar os eventos internamente e permitir que sejam exportados;	
J-110	A solução deve permitir a exportação dos eventos através de syslog;	
J-111	Deve suportar alta disponibilidade, suportando todos os registros e autenticações caso um nó da solução esteja indisponível;	
J-112	A solução deve ser capaz de isolar hosts na quarentena mesmo quando estes estão conectados em redes de localidades remotas, tais como filiais. Não deve ser necessário estender a VLAN para isso;	
J-113	Deve possuir registro dos eventos ocorridos na solução, bem como auditoria das configurações efetuadas;	
J-114	Deve possibilitar o rastreamento de dispositivos, notificando a localização deles quando se conectarem à rede;	
J-115	Instalação e configuração:	
J-116	A solução de NAC deverá ser do mesmo fabricante dos equipamentos itens 1 a 6.	
J-117	Deve possuir solução de retenção de logs com capacidade mínima para armazenar os logs da solução por <u>6 (seis) meses</u> . (Marco Civil Art.13 – 1 ano)	
J-118	Dentre os relatórios disponibilizados pela solução dedicada de logs, deve suportar relatórios listando os <i>endpoints</i> por localidade e fabricante, usuários associados, além de relatórios de inventário, devices registrados e rogues;	
ID	ITEM 9 – CABO DAC PARA EMPILHAMENTO (SWITCHES TIPO 3 E TIPO 4) ou AOC com CONECTORES	
K-1	Ser do tipo <i>Direct Attached</i> . Será aceito conexão passiva (<i>passive cooper cable</i>) ou ativa (<i>active optical</i> - AOC) com os conectores;	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
K-2	Não serão aceitos cabos do tipo <i>Breakout</i> ;	
K-3	Ser utilizado para empilhamento dos switches tipo 3 e tipo 4;	
K-4	Suportar a velocidade de 10Gbps full-duplex;	
K-5	Deve ser do tipo <i>hot swappable</i> , permitindo sua instalação/remoção com o equipamento em operação;	
K-6	Deve possuir, no mínimo, 1 (um) metro de comprimento;	
K-7	Deve ser compatível com os switches ofertados	
K-8	Deve ser do mesmo fabricante dos switches ofertados.	
ID	ITEM 10 – INTERFACE ÓTICA (TRANSCEIVER) 100GBE QSFP28 100GBASE-SR4 MPO	
L-1	Ser do tipo QSFP28 de 100GBASE-SR4	
L-2	Suportar a velocidade de 100Gbps full-duplex	
L-3	Conector MPO	
L-4	Deve ser do tipo <i>hot swappable</i> , permitindo sua instalação/remoção com o equipamento em operação	
ID	ITEM 11 – TRANSCEIVER 40G QSFP28 40GBASE-SR MPO	
M-1	Ser do tipo QSFP28+ de 40GBASE-SR	
M-2	Suportar a velocidade de 40Gbps full-duplex	
M-3	Conector MPO	
M-4	Deve ser do tipo <i>hot swappable</i> , permitindo sua instalação/remoção com o equipamento em operação	
ID	ITEM 12 – INTERFACE ÓTICA (TRANSCEIVER) 25GBE SFP28 25GBASE-SR	
N-1	Ser do tipo SFP28 de 25GBase-SR	
N-2	Suportar a velocidade de 25Gbps full-duplex	
N-3	Conector Duplex LC	
N-4	Deve ser do tipo <i>hot swappable</i> , permitindo sua instalação/remoção com o equipamento em operação	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
ID	ITEM 13 – INTERFACE ÓTICA (TRANSCEIVER) 10GBE SFP+ 10GBASE-SR	
O-1	Ser do tipo SFP+ de 10GBase-SR	
O-2	Suportar a velocidade de 10Gbps full-duplex	
O-3	Conector Duplex LC	
O-4	Deve ser do tipo <i>hot swappable</i> , permitindo sua instalação/remoção com o equipamento em operação	
ID	ITEM 14 – CABO ÓTICO 100G QSFP28 100GBASE-SR MMF	
P-1	O cordão óptico deverá possuir, no mínimo, 15 (quinze metros) de comprimento, constituído por fibras ópticas do tipo multimodo (MM) duplex, com conectores tipo MPO/MPO, compatível com o transceiver item 1 dessa cotação.	
P-2	Suportar a velocidade de 100Gbps full-duplex.	
ID	ITEM 15 – CABO ÓTICO 40G QSFP+ 40GBASE-SR MMF	
Q-1	O cordão óptico deverá possuir, no mínimo, 10 (dez metros) de comprimento, constituído por fibras ópticas do tipo multimodo (MM) duplex, com conectores tipo MPO/MPO, compatível com o transceiver item 2 desse pedido de cotação.	
Q-2	Suportar a velocidade de 40Gbps full-duplex	
ID	ITEM 16 – CABO ÓTICO 25 GBE SFP28 10 MTS	
R-1	O cordão óptico deverá possuir, no mínimo, 10 (dez metros) de comprimento, constituído por fibras ópticas do tipo multimodo (MM) duplex, com conectores tipo LC/LC, compatível com o transceiver item 3 desse pedido de cotação.	
R-2	Suportar a velocidade de 25Gbps full-duplex	
ID	ITEM 17 – CABO ÓTICO 10G SFP+ 10GBASE-SR MMF LC	
S-1	O cordão óptico deverá possuir, no mínimo, 10 (dez metros) de comprimento, constituído por fibras ópticas do tipo multimodo (MM) duplex, com conectores tipo LC/LC, compatível com o transceiver item 4 desse pedido de cotação.	
S-2	Suportar a velocidade de 10Gbps full-duplex	
ID	ITEM 18 – SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DOS SWITCHES DE DATACENTER TIPOS 1 E 2, SOLUÇÃO DE GERENCIAMENTO E SOLUÇÃO DE NAC.	
T-1	Deverá apresentado cronograma de atividades para aprovação, bem como a realização de alinhamento técnico dos requisitos e premissas do projeto.	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
T-2	Após a avaliação, o especialista da Contratada designado desenvolverá o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos.	
T-3	O plano será modificado de acordo com os requisitos da AGU, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente.	
PRÉ-INSTALAÇÃO		
T-4	Deverá a contratada realizar a avaliação das necessidades de rede e design personalizado de topologia <i>spine-and-leaf</i> .	
T-5	Planejamento da Topologia de Rede.	
T-6	Verificação dos Requisitos de Energia e Refrigeração.	
T-7	Preparação de Cabos e Conectores.	
T-8	Configuração de Endereços IP e DHCP.	
T-9	Testes de funcionamento.	
T-10	Segurança da Rede	
T-11	Neste prazo está incluída a elaboração e entrega do cronograma de atividades definitivo para desenvolvimento dos serviços, consoante os requerimentos constantes ao longo do edital de licitação e seus anexos.	
EXECUÇÃO DO PROJETO		
T-12	A Contratada deverá desenvolver as ações estabelecidas no projeto aprovado e finalizar as atividades discriminadas, atendendo rigorosamente todos os quesitos constantes ao longo deste documento.	
T-13	Deverá a contratada realizar alguns dos seguintes serviços:	
T-14	Instalação Física	
T-15	Configuração Lógica	
T-16	Configuração de Alta Disponibilidade e Redundância	
T-17	Implementação de Segurança e Monitoramento	
T-18	Testes e Validação	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
T-19	Passagem de Conhecimento e Documentação	
T-20	Os serviços de entrega, instalação, configuração e testes do ambiente poderão ser realizados em horários extraordinários (período noturno, finais de semana e/ou feriados), a critério da Contratante, com entendimentos prévios junto à Contratada, de sorte a minimizar eventuais intervenções no ambiente de produção das entidades.	
T-21	A instalação e configuração da solução serão acompanhadas e supervisionadas pela equipe técnica da AGU.	
T-22	A configuração deverá ser realizada de acordo com as recomendações do fabricante (<i>recommended settings</i>).	
T-23	Depois de concluída a instalação e configuração da solução, a Contratada deverá fornecer a documentação detalhada de todo esse processo de instalação e configuração.	
CONCLUSÃO DA IMPLANTAÇÃO		
T-24	A formalização do fim da implantação, concluídas todas as etapas do projeto pela Contratada, se processará após análise e validação da AGU. Posteriormente, a Contratada, por meio de documento de sua própria emissão, formalizará a finalização dessa fase do projeto.	
SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO DE GERENCIAMENTO		
T-25	Deverá apresentado cronograma de atividades para aprovação, bem como a realização de alinhamento técnico dos requisitos e premissas do projeto.	
T-26	Após a avaliação, o especialista da Contratada designado desenvolverá o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos.	
T-27	O plano será modificado de acordo com os requisitos da AGU, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente.	
PRÉ-INSTALAÇÃO		
T-28	Deverá a contratada realizar a avaliação das necessidades de rede e design personalizado de topologia de Rede da AGU.	
T-29	Planejamento da Topologia de Rede.	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
T-30	Verificação dos Requisitos de Energia e Refrigeração.	
T-31	Preparação de Cabos e Conectores.	
T-32	Configuração de Endereços IP e DHCP.	
T-33	Testes de funcionamento.	
T-34	Segurança da Rede	
T-35	Neste prazo está incluída a elaboração e entrega do cronograma de atividades definitivo para desenvolvimento dos serviços, consoante os requerimentos constantes ao longo do edital de licitação e seus anexos.	
EXECUÇÃO DO PROJETO		
T-36	A Contratada deverá desenvolver as ações estabelecidas no projeto aprovado e finalizar as atividades discriminadas, atendendo rigorosamente todos os quesitos constantes ao longo deste documento.	
T-37	Deverá a contratada realizar alguns dos seguintes serviços:	
T-38	Instalação Física	
T-39	Configuração Lógica	
T-40	Implementação gerenciamento dos equipamentos dos itens 1 a 6.	
T-41	Criação de Dashboard para Gerenciamento	
T-42	Provisionamento e Configuração	
T-43	Configurar políticas de segurança.	
T-44	Definir regras e implementar políticas de VPN através da solução de Gerenciamento.	
T-45	Criação de Dashboard para Monitoramento	
T-46	Geração de Relatórios periódicos a ser encaminhado a contratada.	
T-47	Configuração da solução de Autenticação	
T-48	Configurar o Gerenciamento de Logs a fim de armazenar logs de eventos de segurança e tráfego para fins de auditoria e investigação de incidentes.	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
T-49	Configuração de Automação para tomada de ação em caso de problemas ocasionados na rede.	
T-50	Configuração do MFA e Token.	
T-51	Configurar o controle de acesso segregando por grupos a ser definido pela AGU.	
T-52	Inclusão de dispositivos a serem monitorados;	
T-53	Ajuste de filtros de segurança para acesso de conteúdo;	
T-54	Configuração de backup de dispositivos de rede;	
T-55	Configuração de relatórios do ambiente de redes;	
T-56	Criação de SSIDs, com autenticação, integração na rede e requisitos básicos de segurança;	
T-57	Configuração das APs em cluster;	
T-58	Configuração de <i>Captive Portal</i> ;	
T-59	Implementação de Segurança e Monitoramento	
T-60	Testes e Validação	
T-61	Passagem de Conhecimento e Documentação	
T-62	Os serviços de entrega, instalação, configuração e testes do ambiente poderão ser realizados em horários extraordinários (período noturno, finais de semana e/ou feriados), a critério da Contratante, com entendimentos prévios junto à Contratada, de sorte a minimizar eventuais intervenções no ambiente de produção das entidades.	
T-63	A instalação e configuração da solução serão acompanhadas e supervisionadas pela equipe técnica da AGU.	
T-64	A configuração deverá ser realizada de acordo com as recomendações do fabricante (<i>recommended settings</i>).	
T-65	Depois de concluída a instalação e configuração da solução, a Contratada deverá fornecer a documentação detalhada de todo esse processo de instalação e configuração.	
CONCLUSÃO DA IMPLANTAÇÃO		

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
T-66	A formalização do fim da implantação, concluídas todas as etapas do projeto pela Contratada, se processará após análise e validação da AGU. Posteriormente, a Contratada, por meio de documento de sua própria emissão, formalizará a finalização dessa fase do projeto.	
SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO NAC		
T-67	Deverá apresentado cronograma de atividades para aprovação, bem como a realização de alinhamento técnico dos requisitos e premissas do projeto.	
T-68	Após a avaliação, o especialista da Contratada designado desenvolverá o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos.	
T-69	O plano será modificado de acordo com os requisitos da AGU, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente.	
PRÉ-INSTALAÇÃO		
T-70	Deverá a contratada realizar a avaliação das necessidades de rede e design personalizado de topologia de switches de acesso LAN.	
T-71	Planejamento da Topologia de Rede.	
T-72	Verificação dos Requisitos de Energia e Refrigeração.	
T-73	Preparação de Cabos e Conectores.	
T-74	Configuração de Endereços IP e DHCP.	
T-75	Testes de funcionamento.	
T-76	Segurança da Rede	
T-77	Neste prazo está incluída a elaboração e entrega do cronograma de atividades definitivo para desenvolvimento dos serviços, consoante os requerimentos constantes ao longo do edital de licitação e seus anexos.	
EXECUÇÃO DO PROJETO		
T-78	A Contratada deverá desenvolver as ações estabelecidas no projeto aprovado e finalizar as atividades discriminadas, atendendo rigorosamente todos os quesitos constantes ao longo deste documento.	
T-79	Deverá a contratada realizar alguns dos seguintes serviços:	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
T-80	Instalação Física	
T-81	Configuração Lógica	
T-82	Configuração Perfil de dispositivo	
T-83	Configuração com a solução de Autenticação e Registro.	
T-84	Configuração do gerenciamento de usuários visitantes e posturas	
T-85	Configuração de perfis de host/usuários	
T-86	Configuração da Network Access Policies	
T-87	Configuração de Políticas de compliance para dispositivos de usuários da AGU e Visitantes.	
T-88	Criação de Dashboard para Gerenciamento	
T-89	Provisionamento e Configuração	
T-90	Configurar políticas de segurança.	
T-91	Definir regras e implementar políticas de VPN através da solução de Gerenciamento.	
T-92	Criação de Dashboard para Monitoramento	
T-93	Geração de Relatórios periódicos a ser encaminhado a contratada.	
T-94	Configuração de Automação para tomada de ação em caso de problemas ocasionados na rede.	
T-95	Configurar o controle de acesso segregando por grupos a ser definido pela AGU.	
T-96	Inclusão de dispositivos a serem monitorados;	
T-97	Ajuste de filtros de segurança para acesso de conteúdo;	
T-98	Configuração de backup de dispositivos de rede;	
T-99	Configuração de relatórios do ambiente de redes;	
T-100	Configuração de <i>Captive Portal</i> ;	
T-101	Implementação de Segurança e Monitoramento	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
T-102	Testes e Validação	
T-103	Passagem de Conhecimento e Documentação	
T-104	Os serviços de entrega, instalação, configuração e testes do ambiente poderão ser realizados em horários extraordinários (período noturno, finais de semana e/ou feriados), a critério da Contratante, com entendimentos prévios junto à Contratada, de sorte a minimizar eventuais intervenções no ambiente de produção das entidades.	
T-105	A instalação e configuração da solução serão acompanhadas e supervisionadas pela equipe técnica da AGU.	
T-106	A configuração deverá ser realizada de acordo com as recomendações do fabricante (<i>recommended settings</i>).	
T-107	Depois de concluída a instalação e configuração da solução, a Contratada deverá fornecer a documentação detalhada de todo esse processo de instalação e configuração.	
CONCLUSÃO DA IMPLANTAÇÃO		
T-108	A formalização do fim da implantação, concluídas todas as etapas do projeto pela Contratada, se processará após análise e validação da AGU. Posteriormente, a Contratada, por meio de documento de sua própria emissão, formalizará a finalização dessa fase do projeto.	
ID	ITEM 19 – SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DOS SWITCHES DE ACESSO TIPOS 3 E 4	
U-1	Deverá apresentado cronograma de atividades para aprovação, bem como a realização de alinhamento técnico dos requisitos e premissas do projeto.	
U-2	Após a avaliação, o especialista da Contratada designado desenvolverá o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos.	
U-3	O plano será modificado de acordo com os requisitos da AGU, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente.	
PRÉ-INSTALAÇÃO		
U-4	Deverá a contratada realizar a avaliação das necessidades de rede e design personalizado de topologia de switches de acesso LAN.	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
U-5	Planejamento da Topologia de Rede.	
U-6	Verificação dos Requisitos de Energia e Refrigeração.	
U-7	Preparação de Cabos e Conectores.	
U-8	Configuração de Endereços IP e DHCP.	
U-9	Testes de funcionamento.	
U-10	Segurança da Rede	
U-11	Neste prazo está incluída a elaboração e entrega do cronograma de atividades definitivo para desenvolvimento dos serviços, consoante os requerimentos constantes ao longo do edital de licitação e seus anexos.	
EXECUÇÃO DO PROJETO		
U-12	A Contratada deverá desenvolver as ações estabelecidas no projeto aprovado e finalizar as atividades discriminadas, atendendo rigorosamente todos os quesitos constantes ao longo deste documento.	
U-13	Deverá a contratada realizar alguns dos seguintes serviços:	
U-14	Instalação Física	
U-15	Configuração Lógica	
U-16	Configuração de Alta Disponibilidade e Redundância	
U-17	Implementação lógica de software de gerenciamento	
U-18	Implementação de Segurança e Monitoramento	
U-19	Testes e Validação	
U-20	Passagem de Conhecimento e Documentação	
U-21	Os serviços de entrega, instalação, configuração e testes do ambiente poderão ser realizados em horários extraordinários (período noturno, finais de semana e/ou feriados), a critério da Contratante, com entendimentos prévios junto à Contratada, de sorte a minimizar eventuais intervenções no ambiente de produção das entidades.	
U-22	A instalação e configuração da solução serão acompanhadas e supervisionadas pela equipe técnica da AGU.	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
U-23	A configuração deverá ser realizada de acordo com as recomendações do fabricante (<i>recommended settings</i>).	
U-24	Depois de concluída a instalação e configuração da solução, a Contratada deverá fornecer a documentação detalhada de todo esse processo de instalação e configuração.	
CONCLUSÃO DA IMPLANTAÇÃO		
U-25	A formalização do fim da implantação, concluídas todas as etapas do projeto pela Contratada, se processará após análise e validação da AGU. Posteriormente, a Contratada, por meio de documento de sua própria emissão, formalizará a finalização dessa fase do projeto.	
ID	ITEM 20 – SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DOS ACCESS POINT TIPOS 1 E 2	
V-1	Deverá apresentado cronograma de atividades para aprovação, bem como a realização de alinhamento técnico dos requisitos e premissas do projeto.	
V-2	Após a avaliação, o especialista da Contratada designado desenvolverá o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos.	
V-3	O plano será modificado de acordo com os requisitos da AGU, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente.	
PRÉ-INSTALAÇÃO		
V-4	Deverá a contratada realizar a avaliação das necessidades de rede e design personalizado de topologia de switches de acesso WLAN.	
V-5	Planejamento da Topologia de Rede.	
V-6	Verificação dos Requisitos de Energia e Refrigeração.	
V-7	Preparação de Cabos e Conectores.	
V-8	Configuração de Endereços IP e DHCP.	
V-9	Testes de funcionamento.	
V-10	Segurança da Rede	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
V-11	Neste prazo está incluída a elaboração e entrega do cronograma de atividades definitivo para desenvolvimento dos serviços, consoante os requerimentos constantes ao longo do edital de licitação e seus anexos.	
	EXECUÇÃO DO PROJETO	
V-12	A Contratada deverá desenvolver as ações estabelecidas no projeto aprovado e finalizar as atividades discriminadas, atendendo rigorosamente todos os quesitos constantes ao longo deste documento.	
V-13	Deverá a contratada realizar alguns dos seguintes serviços:	
V-14	Instalação Física	
V-15	Configuração Logica	
V-16	Implementação logica do equipamento com a controladora.	
V-17	Instalação de licenças na plataforma;	
V-18	Inclusão de dispositivos a serem monitorados;	
V-19	Ajuste de filtros de segurança para acesso de conteúdo;	
V-20	Configuração de backup de dispositivos de rede;	
V-21	Configuração de relatórios do ambiente de redes;	
V-22	Criação de SSIDs, com autenticação, integração na rede e requisitos básicos de segurança;	
V-23	Configuração das APs em cluster;	
V-24	Configuração de Captive Portal;	
V-25	Implementação de Segurança e Monitoramento	
V-26	Testes e Validação	
V-27	Passagem de Conhecimento e Documentação	
V-28	Os serviços de entrega, instalação, configuração e testes do ambiente poderão ser realizados em horários extraordinários (período noturno, finais de semana e/ou feriados), a critério da Contratante, com entendimentos prévios junto à Contratada, de sorte a minimizar eventuais intervenções no ambiente de produção das entidades.	

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO	COMPROVAÇÃO (documentos oficiais, manuais, datasheets, sites oficiais, etc.)
V-29	A instalação e configuração da solução serão acompanhadas e supervisionadas pela equipe técnica da AGU.	
V-30	A configuração deverá ser realizada de acordo com as recomendações do fabricante (recommended settings).	
V-31	Depois de concluída a instalação e configuração da solução, a Contratada deverá fornecer a documentação detalhada de todo esse processo de instalação e configuração.	
	CONCLUSÃO DA IMPLANTAÇÃO	
V-32	A formalização do fim da implantação, concluídas todas as etapas do projeto pela Contratada, se processará após análise e validação da AGU. Posteriormente, a Contratada, por meio de documento de sua própria emissão, formalizará a finalização dessa fase do projeto.	