



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

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

Lei nº 14.133, de 1º de abril de 2021

Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022

Processo Administrativo nº 00693.000791/2023-11

Registro de Preços para eventual Contratação de solução de rede unificada, incluindo instalação, configuração, suporte técnico e garantia para a AGU.



Brasília, 19 de abril de 2024

Histórico de Revisões

DATA	VERSÃO	DESCRIÇÃO	AUTOR
03/05/2021	1.0	Versão inicial do documento	Integrante Requisitante e Técnico
03/10/2023	2.0	Primeira versão do documento	Integrante Requisitante e Técnico
10/11/2023	3.0	Segunda versão dos documentos ajustes	Integrante Requisitante e Técnico
04/12/2023	4.0	Revisão do documento após análise jurídica	Integrante Requisitante e Técnico
02/01/2024	4.0	Evento de Suspensão publicado para readequação dos artefatos	Equipe de Planejamento da Contratação
19/04/2024	5.0	Versão readequação dos artefatos	Equipe de Planejamento da Contratação

ESTUDO TÉCNICO PRELIMINAR DA CONTRATAÇÃO

(Inciso XI, do art. 2º e art. 11 da IN SGD/ME nº 94/2022)

1. INFORMAÇÕES BÁSICAS

1.1. Processo nº 00693.00791/2023-11

1.2. O ETP tem por objetivo identificar e analisar os cenários para o atendimento de demanda registrada no Documento de Formalização da Demanda – DFD (Seq. 175), Registro de Preços para eventual Contratação de solução de rede unificada para a AGU”, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar a tomada de decisão e o prosseguimento do respectivo processo de contratação. “

1.3. A “Contratação de solução de rede unificada para a AGU” enquadra-se na categoria de Aquisição de Bens e Serviços de TIC.

1.4. No presente documento, a EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO – ora designada por meio da Portaria nº DLOG/SGA/AGU nº 00099/2023 de 20 de junho de 2023 – dedica-se a analisar aspectos fundamentais relacionados à demanda em questão, tais como: adequação técnica; funcionalidades e requisitos; adequação às normas vigentes; modelos de execução; capacidade do mercado; estimativa preliminar de custos e viabilidade econômico-financeira do objeto.

2. DESCRIÇÃO DAS NECESSIDADES

2.1. Motivação/Justificativa

2.1.1. 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.

2.1.2. 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.

2.1.3. 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.

2.1.4. A motivação da presente pretensão contratual decorre da necessidade de substituir os equipamentos atualmente defasados, fora da garantia de suporte e sem qualquer atualização. Além disso a presente contratação objetiva atender às unidades da AGU com os serviços (sinal) de rede Wireless devidamente conectado na rede AGU. Por fim, por se tratar de uma solução que deve ser projetada para permitir que toda a comunicação ocorra de maneira segura, lançando mão de recursos e funcionalidades

avancadas de segurança de rede os equipamentos que compõe os Datacenters da AGU em Brasília, sedes I e II, estarão igualmente envolvidos nessa troca. Tal qual idealizado deve-se garantir que períodos de indisponibilidade e roubo de informações, em razão de problemas relacionados a ataques hackers, deve ser minimizado e controlado por meio de uma solução integrada que permita obter a visibilidade necessária bem como ser dotada de funcionalidades capazes de tomar ações automaticamente caso ocorram situações de ataques.

2.1.5. Atualmente o núcleo da rede do centro de dados da AGU é composto por switches do fabricante Dell que estão interligados em uma topologia lógica do tipo “Spine and Leaf”. Estes equipamentos foram adquiridos pela AGU em 2021 contrato nº 01/2021 e encontram-se descritos na tabela abaixo. De maneira racional identificamos que às necessidades das localidades da AGU nas capitais podem ser atendidas com os equipamentos atualmente instalados no Datacenter da AGU em Brasília dando continuidade ao prazo de garantia e suporte sem qualquer prejuízo. Nesse caminho as unidades da AGU possuem seus switches de borda (switches de acesso) sem qualquer suporte/garantia, em operação a mais de 10 (dez) anos e já apresentando problemas de quebra/defeito, problemas relacionados a falta de gestão, sem funcionalidades de segurança da informação e integração. Compreendendo às atuais necessidades outro componente igualmente importante e necessário é a disponibilização do ambiente de redes sem fio (wireless) seguro nas unidades da AGU. Como caminha a tecnologia além das necessidades de adequação dos ambientes de trabalho ao teletrabalho entendemos que essa pode ser a última contratação massiva de switches de borda vislumbrando um ambiente mais sem fios nas unidades. Como ambiente corporativo de rede sem fio hoje a AGU dispõe apenas dos seus 2 (dois) edifícios/sedes em Brasília montados com uma infraestrutura wireless baseado em equipamentos do fabricante Huawei, 650 (seiscentos e cinquenta) Access Points e 1 (uma) controladora, adquiridos em 2016 (contrato nº 044/2016) e já fora da garantia e suporte. De um todo a falta de garantia e suporte não é a única razão para atender às necessidades desse projeto visto que a necessidade de evolução tecnológica seja em aspectos relacionados a performance e desempenho seja em aspectos relacionados a uma solução que atenda nas características de gestão, segurança da informação e que forneça um ambiente limpo, de fácil administração e que possua a rastreabilidade necessária para se combater os problemas relacionados às diversas formas de exploração de ataques baseadas em vulnerabilidades e brechas. Dessa maneira segue, na tabela abaixo, a listagem dos equipamentos com seus respectivos quantitativos, tipos, modelos e fabricantes das soluções atualmente em uso na AGU:

Item	Descrição	Quantidade
1	Switches de Datacenter Spine (Dell)	10

2	Switches de Datacenter Leaf (Dell)	6
3	Switches Acesso (CISCO/3COM/Extreme/Huawei/Datacom/Enterasys/Intelbras/Linksys 24/48 portas)	1.076
4	Access Point (Huawei)	650
5	Solução de Gerência Wireless (Huawei)	1

2.1.6. Como os switches de datacenter itens 1 e 2 da tabela acima ainda estão cobertos por garantia, a estratégia é a de deslocá-los para as unidades de São Paulo, Recife, Rio de Janeiro, Belo Horizonte e Porto Alegre visto que a migração e instalação ocorrerá em etapas. Esse processo trata-se da construção de uma Ata de Registro de Preços para que possamos fazer a implementação por etapas.

2.1.7. No aspecto da segurança da informação podemos evidenciar o rápido avanço de informações através da Internet aumentou a possibilidade de vulnerabilidades e gerou novas formas de atividades intrusivas. Desta forma torna-se fundamental a aplicação de camadas de segurança em alto nível para proteger os ativos de rede contra ameaças para garantir a integridade, a confidencialidade e a disponibilidade dos dados trafegados.

2.1.8. Conforme estatísticas apresentadas pelo Centro de Estudos, Resposta e Tratamento de Incidentes e Segurança no Brasil (CERT.br), o número de incidentes é crescente e volumoso (Figura 1). A Figura 2 mostra os tipos de ataques mais frequentes em 2023. O CERT.br destaca ainda que no ano de 2023 houve um aumento de 19% de ataques em servidores Web, em relação ao ano anterior (Fonte: <https://stats.cert.br/incidentes/>). Diante desse contexto, a AGU se vê obrigada a adotar medidas contra-ataques cibernéticos, buscando de forma segura, inteligente, integrada e automatizada, mecanismos de detecção e análise avançada de ameaças cibernéticas.

Notificações de incidentes recebidas pelo CERT.br

2012 a Fevereiro de 2023

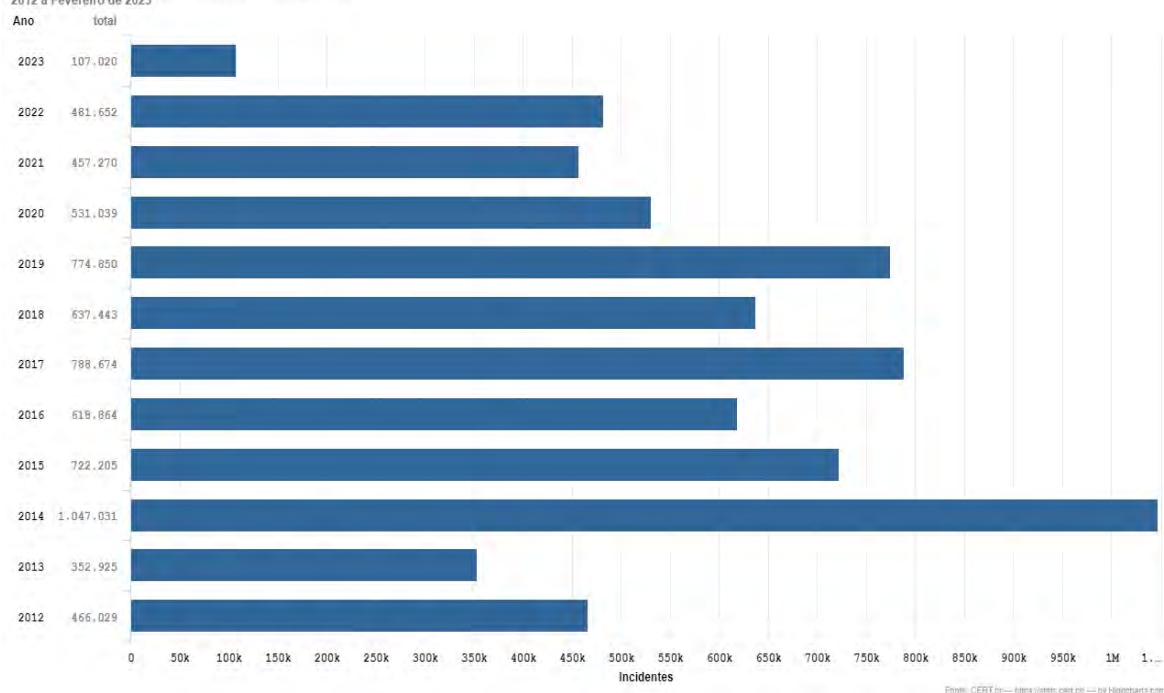


Figura 1: Notificação de Incidentes recebidas pelo CERT.br (<https://stats.cert.br/incidentes/>)

Notificações sobre equipamentos participando em ataques DoS

2012 a Fevereiro de 2023

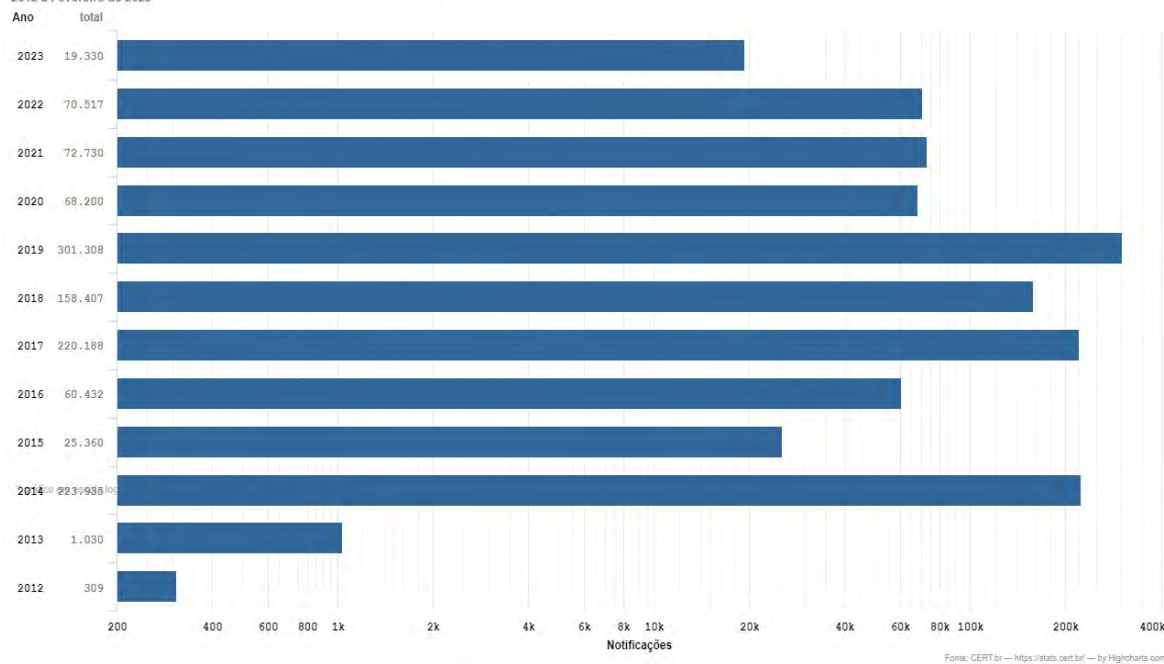


Figura 2: Notificações sobre equipamentos participando em ataques DOS (<https://stats.cert.br/incidentes/>)

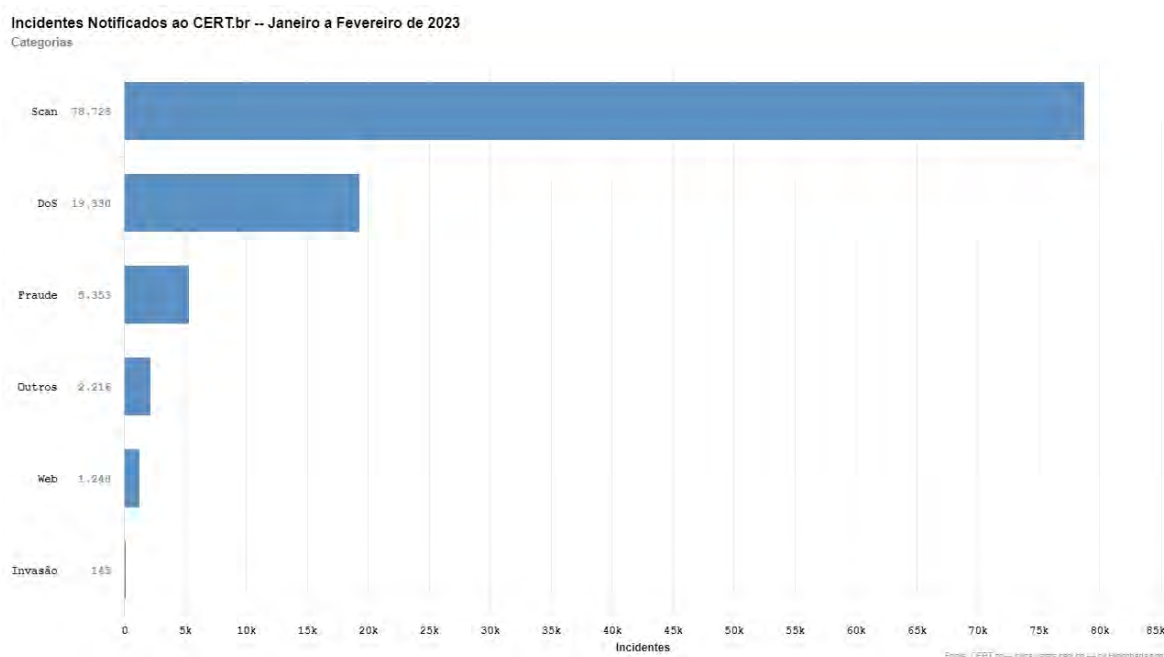


Figura 3: Incidentes Notificados ao CERT.br (<https://stats.cert.br/incidentes/>)

2.1.9. Considerando o aumento de ataques direcionados a órgãos importantes do governo e a velocidade de surgimento de novas e complexas ameaças, tais como SQL Injection, manipulação de URL, backdoor malwares e ransomware, esta última em franca expansão, que não se limitam apenas as estações de trabalho dos usuários, mas também ao ambiente de datacenter (virtualizado ou físico), torna-se uma necessidade, cada vez mais importante, manter todo ambiente de TIC atualizado e seguro, devido à dimensão e importância dos serviços prestados pela AGU à sociedade.

2.1.10. Nesse sentido, é essencial que se mantenha uma solução de segurança atualizada e em garantia com o intuito de evitar falhas, elevando-se assim o grau de segurança necessário para o ambiente de TIC e para o funcionamento do órgão como um todo, em especial para a proteção das informações que são transitadas em seus principais sistemas.

2.1.11. Outro ponto de extrema relevância está nas questões de proteção de dados pessoais, o que nos remete à Lei Geral de Proteção de Dados Pessoais – LGPD, Lei nº 13.709/2018. Com a solução objeto deste estudo, a AGU realiza uma atualização tecnológica, necessária para a adequação do novo cenário de cibersegurança, quanto para a LGPD.

2.1.12. Nesse sentido o Tribunal de Contas da União TCU, por meio do TC 001.873/2020-2 (<https://portal.tcu.gov.br/imprensa/noticias/avaliacao-do-tcu-aponta-que-ataques-ciberneticos-mercem-atencao-governamental.htm> - Rel. Min. Vital do Rêgo) que culminou com o Acórdão 4.035/2020-TCU-Plenário (<https://pesquisa.apps.tcu.gov.br/#/documento/acordao-completo/187320202.PROC/%2520DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0/%2520?uuid=e052e8c0-3e39-11eb-a2e2-479b45fdacff>) registrou levantamento com o objetivo

de conhecer a macroestrutura de governança e gestão de segurança da informação e de segurança cibernética na Administração Pública Federal (APF), incluindo aspectos referentes a legislação, políticas, normativos, atores, papéis e responsabilidades atinentes a essas áreas.

2.1.13. Em decorrência das deliberações expostas no Acórdão supra o TCU está realizando acompanhamento de controles críticos de Segurança Cibernética (SegCiber) das organizações públicas federais em total aderência com a versão 8 do framework do Center for Internet Security (CIS) (<https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/fiscalizacoes/>).

2.1.14. O controle 12 do CIS v8 – Gestão de infraestrutura de rede: reforça a necessidade de se Estabeleça, implemente e gerencie ativamente (rastreie, reporte, corrija) os dispositivos de rede, a fim de evitar que atacantes explorem serviços de rede e pontos de acesso vulneráveis, no caso, da AGU. A infraestrutura de rede segura é uma defesa essencial contra ataques. Isso inclui uma arquitetura de segurança apropriada, abordando vulnerabilidades que são, muitas vezes, introduzidas com configurações padrão, monitoramento de alterações e reavaliação das configurações atuais. A infraestrutura de rede inclui dispositivos como gateways físicos e virtualizados, firewalls, pontos de acesso sem fio, roteadores e switches. Por essa razão, tratar o ambiente de interconexão de rede com soluções integradas e recursos/funcionalidades de segurança da informação torna-se tão essencial como se ter a conexão. Não resolve os problemas de contenção e proteção se esse ambiente não for tratado com a devida importância.

2.1.15. A segurança da rede é um ambiente em constante mudança que exige uma reavaliação regular dos diagramas de arquitetura, configurações, controles de acesso e fluxos de tráfego permitidos. Os atacantes tiram proveito das configurações de dispositivos de rede que se tornam menos seguras com o tempo, à medida que os usuários exigem exceções para necessidades de negócio específicas. Às vezes, as exceções são implantadas, mas não removidas quando não são mais aplicáveis às necessidades do negócio. Em alguns casos, o risco de segurança de uma exceção não é devidamente analisado nem medido tampouco acompanhado em relação à necessidade de negócios associada e pode mudar com o tempo.

2.1.16. Dentro desse cenário, esse mesmo controle aponta a necessidade de se acompanhar o fim do ciclo de vida dos componentes de rede (EOL – end of life) indicando que esses componentes devem ser trocados sempre que ficarem sem suporte.

2.1.17. Como medida de segurança, essa contratação vislumbra o atendimento às medidas de segurança 12.1, 12.2, 12.3, 12.4 e o 12.6 todas do controle 12, conforme abaixo:

Medidas de Segurança

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA/ DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
12.1	Assegurar que a infraestrutura de rede esteja atualizada Assegure que a infraestrutura de rede seja mantida atualizada. Exemplos de implementações incluem a execução da versão estável mais recente do software e/ou o uso de ofertas de network-as-a-service (NaaS) atualmente suportadas. Revise as versões do software mensalmente, ou com mais frequência, para verificar o suporte do software.	Rede	Proteger			
12.2	Estabelecer e manter uma arquitetura de rede segura Estabeleça e mantenha uma arquitetura de rede segura. Uma arquitetura de rede segura deve abordar segmentação, privilégio mínimo e disponibilidade, no mínimo.	Rede	Proteger			
12.3	Gerenciar infraestrutura de rede com segurança Gerencie com segurança a infraestrutura de rede. Exemplos de implementações incluem versão controlada de infraestrutura como código e o uso de protocolos de rede seguros, como SSH e HTTPS.	Rede	Proteger			
12.4	Estabelecer e manter diagrama(s) de arquitetura Estabeleça e mantenha diagrama(s) de arquitetura e/ou outra documentação de sistema de rede. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.	Rede	Identificar			
12.5	Centralizar a autenticação, autorização e auditoria (AAA) de rede Centralize AAA de rede.	Rede	Proteger			
12.6	Usar protocolos de comunicação e gestão de rede seguros Use protocolos de comunicação e gestão de rede seguros (por exemplo, 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise ou superior).	Rede	Proteger			
12.7	Assegurar que os dispositivos remotos utilizem uma VPN e estejam se conectando a uma infraestrutura AAA da empresa Exigir que os usuários se autenticuem em serviços de autenticação e VPN gerenciados pela empresa antes de acessar os recursos da empresa em dispositivos de usuário final.	Dispositivo	Proteger			
12.8	Estabelecer e manter recursos de computação dedicados para todo o trabalho administrativo Estabeleça e mantenha recursos de computação dedicados, fisicamente ou logicamente separados, para todas as tarefas administrativas ou tarefas que requeiram acesso administrativo. Os recursos de computação devem ser segmentados da rede primária da empresa e não deve ser permitido o acesso à Internet.	Dispositivo	Proteger			

Figura 4: Medidas de Segurança Controle 12 CIS v8

(<https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F7BE7E97D017C4DAEAD1E11B4>)
página nº 39

2.1.18. Já o controle 13 do CIS 8 Monitoramento e defesa de rede: possui como objetivo a melhoria da capacidade de operar processos e ferramentas para estabelecer e manter monitoramento e defesa de rede abrangente contra ameaças de segurança em toda a infraestrutura de rede corporativa e base de usuários. Esse controle 13 aponta sobre a evolução e amadurecimento dos atacantes, algo não muito diferente do que se observa nos dias atuais. Ataques cada vez mais sofisticados que, em grande parte, se aproveita de falhas e vulnerabilidades no ambiente da vítima, no caso a AGU. As ferramentas de segurança só podem ser eficazes se oferecerem suporte a um processo de monitoramento contínuo que permita à equipe ser alertada e responder rapidamente a incidentes de segurança. As organizações que adotam uma abordagem puramente orientada para a tecnologia também terão mais falsos positivos, devido ao excesso de confiança nos alertas das ferramentas. Identificar e responder a essas ameaças requer visibilidade de todos os vetores de ameaças da infraestrutura e aproveitamento de pessoas no

processo de detecção, análise e resposta. É essencial para essas organizações terem uma capacidade de operações de segurança para prevenir, detectar e responder rapidamente às ameaças cibernéticas antes que elas possam impactar a empresa. Este processo irá gerar relatórios de atividades e métricas que ajudarão a aprimorar as políticas de segurança e apoiar a conformidade regulatória para muitas organizações.

2.1.19. Dessa maneira esse controle 13 traz algumas medidas de segurança que são atendidas com o objeto da pretensa contratação. São elas as medidas 13.3, 13.4, 13.6 e 13.9 conforme abaixo:

Medidas de Segurança

MEDIDAS DE SEGURANÇA	TÍTULO DA MEDIDA DE SEGURANÇA / DESCRIÇÃO DA MEDIDA DE SEGURANÇA	TIPO DE ATIVO	FUNÇÃO DE SEGURANÇA	IG1	IG2	IG3
13.1	Centralizar o alerta de eventos de segurança Centralize os alertas de eventos de segurança em ativos corporativos para correlação e análise de log. A melhor prática requer o uso de um SIEM, que inclui alertas de correlação de eventos definidos pelo fornecedor. Uma plataforma de análise de log configurada com alertas de correlação relevantes para a segurança também atende a esta medida de segurança.	Rede	Detectar			
13.2	Implantar solução de detecção de intrusão baseada em host Implante uma solução de detecção de intrusão baseada em host em ativos corporativos, quando apropriado e/ou com suporte.	Dispositivo	Detectar			
13.3	Implantar uma solução de detecção de intrusão de rede Implante uma solução de detecção de intrusão de rede em ativos corporativos, quando apropriado. Exemplos de implementações incluem o uso de um Network Intrusion Detection System (NIDS) ou serviço de provedor de serviço de nuvem equivalente (CSP).	Rede	Detectar			
13.4	Realizar filtragem de tráfego entre segmentos de rede Execute a filtragem de tráfego entre segmentos de rede, quando apropriado.	Rede	Proteger			
13.5	Gerenciar controle de acesso para ativos remotos Gerencie o controle de acesso para ativos que se conectam remotamente aos recursos da empresa. Determine a quantidade de acesso aos recursos da empresa com base em: software anti-malware atualizado instalado, conformidade de configuração com o processo de configurações seguras da empresa e garantia de que o sistema operacional e as aplicações estão atualizados.	Dispositivo	Proteger			
13.6	Coletar logs de fluxo de tráfego da rede Colete logs de fluxo de tráfego de rede e/ou tráfego de rede para revisar e alertar sobre dispositivos de rede.	Rede	Detectar			
13.7	Implantar solução de prevenção de intrusão baseada em host Implante uma solução de prevenção de intrusão baseada em host em ativos corporativos, quando apropriado e/ou com suporte. Exemplos de implementações incluem o uso de um cliente Endpoint Detection and Response (EDR) ou agente IPS baseado em host.	Dispositivo	Proteger			
13.8	Implantar uma solução de prevenção de intrusão de rede Implante uma solução de prevenção de intrusão de rede, quando apropriado. Exemplos de implementações incluem o uso de um Network Intrusion Prevention System (NIPS) ou serviço CSP equivalente.	Rede	Proteger			
13.9	Implantar controle de acesso no nível de porta Implante o controle de acesso no nível de porta. O controle de acesso no nível de porta utiliza 802.1x ou protocolos de controle de acesso à rede semelhantes, como certificados, e pode incorporar autenticação de usuário e/ou dispositivo.	Dispositivo	Proteger			
13.10	Executar filtragem da camada de aplicação Execute a filtragem da camada de aplicação. Exemplos de implementações incluem um proxy de filtragem, firewall de camada de aplicação ou gateway.	Rede	Proteger			
13.11	Ajustar Limites de Alerta de Eventos de Segurança Ajuste os limites de alerta de eventos de segurança mensalmente ou com mais frequência.	Rede	Detectar			

Figura 5: Medidas de Segurança Controle 13 CIS v8

(<https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F7BE7E97D017C4DAEAD1E11B4>)
página nº 42

2.1.20. O Departamento de Tecnologia da Informação – DTI tem em sua missão de acordo seu

Plano Diretor de Tecnologia da Informação e Comunicações - PDTIC 2023 a 2025:

“Prover soluções de TI necessárias ao cumprimento da missão institucional da AGU por meio da adoção das melhores práticas de Governança e Gestão”.

2.1.21. Em seu planejamento sobre a perspectiva de Governança de TI a DTI tem como Objetivo Estratégico:

- OE.05 - Garantir a infraestrutura de TI apropriada às necessidades da AGU

2.1.22. Já em seu planejamento, no intuito de alcançar seus objetivos estratégicos de Governança e Gestão de TI, o PDTIC colocar como iniciativas estratégicas necessárias:

- IE.03 - Aprimorar a infraestrutura de TI das unidades da AGU.

2.1.23. Motiva-se nesse cenário, os diversos objetivos e iniciativas estratégicas da Governança e Gestão de TI para atender o Plano Diretor de Tecnologia da Informação e Comunicações - PDTIC 2023 a 2025.

2.1.24. A Advocacia-Geral da União AGU foi criada em 1993, por meio da lei complementar nº 73, de 10 de fevereiro, tendo nascido da necessidade de distinguir as atribuições de defesa do Estado daquelas de defesa da sociedade e de fiscalização da lei, antes concentradas no Ministério Público. A partir da criação da AGU, o Ministério Público deixou de fazer a representação da União, que costumava ser feita por um órgão denominado Consultoria Geral da República. Com vistas a fazer frente e apoiar o trabalho jurídico e consultivo nas localidades os órgãos da AGU (PGU, PGF e CGU) se encontram presentes em todas as capitais de Estado e nas cidades mais importantes do interior do país, em uma distribuição que procura acompanhar a distribuição regional dos Tribunais de Justiça Federais em 6 regiões. Dessa maneira as Procuradorias-Gerais são compostas por Procuradorias Regionais, que, por sua vez, se subdividem em Procuradorias Estaduais e Procuradorias Seccionais. A Procuradoria-Geral Federal, especificamente, também conta com procuradorias especializadas em determinadas matérias, que tem atuação semelhante as das Consultorias Jurídicas dos Ministérios.

2.1.25. Dessa maneira, a AGU possui, hoje, 148 (cento e quarenta e oito) unidades físicas descentralizadas (Anexo I). Dessas 2 (duas) delas, as Sedes I e II localizadas em Brasília-DF, possuem ambiente de Datacenter composto por todos os subsistemas de precisão e geração ininterrupta de energia que seja minimamente capaz de sustentar todos os componentes de infraestrutura tecnológica da AGU. As instalações físicas possuem, além dos aspectos de infraestrutura física, uma solução de monitoramento da sala e de seus subsistemas. Nesses ambientes funcionam os serviços que hoje a AGU disponibiliza para a realização de todas as suas atividades fim tais como:

2.1.26. **SUPER SAPIENS**

2.1.26.1. O SUPER SAPIENS é um Sistema de Inteligência Jurídica que possui avançados recursos de apoio à produção de conteúdo jurídico e de controle de fluxos administrativos, focado na integração com os sistemas informatizados do Poder Judiciário e do Poder Executivo.

2.1.26.2. Este sistema procura simplificar rotinas e expedientes, além de auxiliar, com suas ferramentas de inteligência, no Processo de tomada de decisão e na elaboração de documentos.

2.1.26.3. O SUPER SAPIENS unifica e relaciona os elementos constantes dos Processos administrativos, inclusive dossiês judiciais, colocando a AGU definitivamente na era da virtualização e do processo administrativo eletrônico. Nesse momento o sistema passou a incorporar em seu bojo um poderoso sistema de Inteligência Artificial que eleva, ainda mais, sua importância não só para a AGU como para o Estado Brasileiro.

2.1.26.4. Promove, ainda, a orquestração dos vários sistemas informatizados da administração pública, de forma transparente para o Usuário. Gerencia e oportuniza a adoção de modelos e teses de direito padronizadas em âmbito nacional, de forma a tornar coesa a atuação dos Advogados Públicos Federais em todo o território nacional e em todas as instâncias.

2.1.26.5. O SAPIENS é híbrido, isto é, comporta documentos digitais e documentos físicos. Inclui operações como: captura de documentos, aplicação do plano de classificação, controle de versões, controle sobre os prazos de guarda e destinação, armazenamento seguro e procedimentos que garantam o acesso e a preservação a médio e longo prazo de documentos arquivísticos digitais e não digitais confiáveis e autênticos.

2.1.26.6. No caso dos documentos digitais, o SAPIENS abrange todos os tipos de documentos arquivísticos da AGU, ou seja, textos, imagens, vídeos, gravações sonoras, mensagens de correio eletrônico, páginas web, bases de dados, dentre outras possibilidades de um vasto repertório de diversidade crescente.

2.1.26.7. O Sistema de Inteligência Jurídica – SAPIENS, o qual, alcançou a marca de 6 milhões de processos administrativos no sistema, tendo 12 mil usuários distintos utilizando-o diariamente, podendo alcançar até 6 mil acessos simultaneamente. Ainda, são abertas por mês cerca de 1,5 milhão tarefas, sendo cadastradas 50 intimações todos os dias e mais de 300 mil documentos são produzidos ou juntados diariamente ao sistema. Sendo também que o SAPIENS possui atualmente cerca de 170 milhões de componentes digitais, e recebe cerca de 300 mil novos componentes digitais por dia.

2.1.26.8. Tal sistema municia a todos os Advogados e procuradores da AGU, com o acompanhamento dos processos jurídicos em tramitação na esfera da Justiça Federal, assim como, regi todas as demandas administrativas da AGU.

2.1.27. LABORATÓRIO DE RECUPERAÇÃO DE ATIVOS – LABRA

2.1.27.1. O Laboratório de Recuperação de Ativos da Advocacia-Geral da União - LABRA/AGU foi criado pela Portaria AGU nº 511, de 4 de dezembro de 2015, com o objetivo de "propiciar apoio às atividades finalísticas da Advocacia-Geral da União exclusivamente no tocante à cobrança e recuperação de ativos, por meio da produção de conhecimento e de informações estratégicas destinadas a subsidiar sua atuação judicial" (art. 2º).

2.1.27.2. O sisLABRA - Sistema de Auxílio à Identificação e Localização de Pessoas e Patrimônio constitui a principal estratégia do LABRA/AGU para a consecução desse objetivo. Lançado em novembro de 2017 em versão beta, o sisLABRA é uma poderosa ferramenta (web) destinada à correlação de dados de pessoas físicas e jurídicas, visando ao aprimoramento da atividade de cobrança e recuperação de ativos das unidades de execução da Procuradoria-Geral da União - PGU e da Procuradoria-Geral Federal - PGF, contando atualmente com 600 usuários habilitados para sua utilização com finalidade específica. O sisLABRA passa constantemente por atualizações e melhoramentos, tanto em suas bases de dados quanto em seus mecanismos de inteligência, de modo a oferecer aos usuários, com os recursos disponíveis, resultados cada vez mais completos e precisos.

2.1.28. VIRTUALIZAÇÃO, SISTEMAS, SERVIÇOS E APLICAÇÕES

2.1.28.1. O ambiente de produção é composto por vários sistemas e aplicações, como o sistema de processo eletrônico digitalizado, o ambiente de bancos de dados Oracle, ambiente de servidor de arquivos corporativo, sistema de correio eletrônico Exchange e ambiente virtualizado VMware/HyperV. Esse ambiente fornece a infraestrutura física e lógica para dezenas de aplicações e serviços de TI providos pelos datacenters da AGU em Brasília/DF.

2.1.28.2. Esses são apenas alguns dos exemplos de sistemas, tecnologias e elementos que se encontram hospedados nos datacenters e nas unidades da AGU pelo Brasil.

2.1.28.3. Pelo todo exposto, a contratação pretendida visa dar continuidade no serviço de conectividade interna de todo o ambiente da AGU com segurança, resiliência, suporte, atualização e gerência única, por meio de uma solução de rede unificada (Unified Network) integrando os switches de datacenter, de borda/acesso e de rede sem fio (wireless).

3. ÁREA REQUISITANTE

3.1. Departamento de Tecnologia da Informação – DTI, da Advocacia Geral da União – AGU:

IDENTIFICAÇÃO DA ÁREA REQUISITANTE	NOME DO RESPONSÁVEL
DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO	ÁLVARO DA COSTA RONDON NETO
	UENDEL DA SILVA TAVARES
	THIAGO DE SOUSA MARTINS

4. NECESSIDADES DE NEGÓCIO

- 4.1. De maneira inicial e não exaustiva podemos listar as seguintes necessidades 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).
- 4.2. O objeto da contratação está previsto no Plano de Contratações Anual 2024, conforme detalhamento a seguir:

ID PCA no PNCP	Data de publicação no PNCP	Id do item no PCA	Classe/Grupo :	Identificador da Futura Contratação
26994558000123-0-000008/2024	19/05/2023	90/2024	7050	110792-90112/2024

- 4.3. Além disso, o objeto da contratação encontra-se alinhada ao Plano Diretor de Tecnologia da Informação e Comunicação da AGU - PDTIC 2023-2025, conforme tabela abaixo:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	Objetivos Estratégicos
OE.05	Garantir a Infraestrutura de TI apropriada às necessidades da AGU.

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

5. NECESSIDADES TECNOLÓGICAS

5.1. As necessidades tecnológicas a serem atendidas pela presente demanda envolvem essencialmente:

- 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) Criação de regras e perfis de acesso a rede por meio da premissa do menor acesso;
- d) Atualização de componentes físicos e lógicos (firmwares, SO e funcionalidades) da solução de redes unificada;
- e) Possibilidade de avaliação de postura dos equipamentos que acessem a rede da AGU;
- f) Controlar todo o tipo de acesso a rede gerindo aqueles acessos que necessitem de maior nível de privilégio; e
- g) Tratar todo o tráfego de rede, seja cabeado ou sem fio, de igual maneira inclusive com gerenciamento e gestão por perfil.

6. DEMAIS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DE SOLUÇÃO DE TIC

6.1. 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.

6.2. 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.

6.3. 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.

6.4. 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.

- 6.5. Informar à AGU, formalmente e tempestivamente, sobre quaisquer necessidades de atualização ou mudança na configuração dos serviços prestados.
- 6.6. Prestar os esclarecimentos necessários, bem como informações concernentes à natureza e andamento dos serviços executados, ou em execução.
- 6.7. 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.
- 6.8. Não divulgar, mesmo que em caráter estatístico, quaisquer informações originadas na AGU, sem prévia autorização.
- 6.9. Prover segurança através da utilização de identificação individual dos profissionais envolvidos na execução dos serviços.
- 6.10. 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.
- 6.11. Deverá acatar e obedecer às normas de utilização e segurança das instalações da AGU.
- 6.12. Deverá manter os seus profissionais informados quanto às normas disciplinares, exigindo sua fiel observância, especialmente quanto à utilização e segurança das instalações.
- 6.13. 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.
- 6.14. Essa transferência se dará ao longo dos projetos, através do repasse de toda documentação e código-fonte da solução produzida, pelo menos quando entregue em ambiente de produção, ou quando for mais conveniente para o requisitante, principalmente quando o repasse de conhecimento for necessário para a homologação da entrega.
- 6.15. Entendemos, ainda, que os requisitos necessários e suficientes à escolha da solução estão presentes ao longo deste estudo técnico e, ainda, descritos no ANEXO II deste mesmo estudo técnico. 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 na comunicação;
- b) **Eficácia:** Resolver os atuais problemas reportados pelo suporte de TI, pelas áreas da AGU e pelo DTI;
- c) **Otimização de custos:** Contratação de uma solução que atenda às necessidades;

- d) **Visibilidade:** Apoiar a gestão fornecendo completa visibilidade no acesso aos recursos da AGU; e
- e) **Disponibilidade Nacional:** Atendimento aos 2 (dois) datacenters da AGU em Brasília-DF (Sede I e Sede II) e todas as unidades da AGU.

6.16. A CONTRATADA deverá fornecer solução integrada (unified network) de comunicação interna, switches de datacenter, de acesso e rede sem fio (wireless). Essa solução deverá ser disponibilizada por equipamentos novos, de primeiro uso, com solução de gerenciamento e gestão integrada com funcionalidades de segurança da informação e NAC (Network Access Control). Toda a instalação e configuração da solução completa deverá estar incluída nos valores cobrados pela solução de maneira que a AGU não precise arcar com nenhuma despesa adicional. Dessa maneira, 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 dos mesmos.

6.17. O objeto a ser contratado trata-se de aquisição de equipamentos do tipo switches de datacenter do tipo spine leaf, switches de borda/acesso e ambiente de rede wireless. O licenciamento da solução de gerenciamento, NAC e demais componentes que se fizerem necessário para a entrega completas descrita nas características técnicas no Anexo II deste Estudo Técnico.

6.18. A prestação desses serviços visa atender as demandas de conectividade de rede do Datacenter Principal – SEDE II e Datacenter Secundário – SEDE I além de todo o ambiente de rede cabeada e sem fio das demais unidades da AGU. A solução definida neste documento busca obter a proposta mais vantajosa para a AGU.

6.19. Por fim, nos últimos 3 (três) meses precedentes ao encerramento do contrato deverá haver repasse de conhecimentos sobre processos e tecnologias, com o objetivo de garantir a continuidade do serviço pelo requisitante ou por terceiros por ele indicados. Todos os serviços entregues pelo provedor deverão ser cobertos por garantia técnica durante a vigência do contrato. Durante o prazo de garantia do serviço, o fornecedor deverá manter canal de comunicação por telefone, e-mail ou sistema informatizado e cumprir os prazos definidos no Acordo de Nível de Serviço para as atividades de garantia técnica.

7. ESTIMATIVA DA DEMANDA - QUANTIDADE DE BENS E SERVIÇOS

7.1. A demanda estimada para atender ao objeto deste Estudo Técnico é o seguinte:

ITEM	DESCRIÇÃO	MÉT.	QTD.
------	-----------	------	------

1	Switch Datacenter - Tipo 1 (Spine)	Und	4
2	Switch Datacenter - Tipo 2 (Leaf)	Und	14
3	Switch Acesso tipo 3 (24 portas PoE Base T)	Und	230
4	Switch Acesso tipo 4 (48 portas PoE Base T)	Und	100
5	Interface Ótica (transceiver) 100Gbe QSFP28 100GBase-SR4 MPO	Und	60
6	Interface Ótica (transceiver) 40Gbe QSFP28+ 40GBase-SR4 MPO	Und	40
7	Interface Ótica (transceiver) 25Gbe SFP28+ 25GBase-SR	Und	240
8	Interface Ótica (transceiver) 10Gbe QSFP28	Und	60
9	Access Point Tipo 1 (4x4)	Und	160
10	Access Point Tipo 2 (2x2)	Und	550
11	Solução de Gerenciamento e Controladora	Und	1
12	Solução de NAC	Und	5000
13	Cabo DAC para Empilhamento (Switches Tipo 3 e 4) ou Fibra	Und	170
14	Cabo Ótico 100 Gbe QSFP28 15 mts – MPO	Und	60
15	Cabo Ótico 40 Gbe QSFP28 10 mts - MPO	Und	40
16	Cabo Ótico 25 Gbe SFP28 10 mts	Und	240
17	Cabo Ótico 10 Gbe SFP+ Base-SR MMF LC 10 mts	Und	40
18	Serviço de Instalação e Configuração dos Switches de Datacenter Tipos 1 e 2	Und	18
19	Serviço de Instalação e Configuração dos Switches de Acesso Tipos 3 e 4	Und	330
20	Serviço de Instalação e Configuração dos Access Point Tipos 1 e 2	Und	710

7.2. Importa destacar que para as demandas do Datacenter Sedes I e II da AGU em Brasília DF foram considerados a densidade de portas atualmente utilizadas em cada um dos datacenters além de uma necessidade projetada de crescimento.

7.3. Uma outra questão, é a contratação de mão de obra especializada, reconhecida pelo fabricante,

neste sentido, deverá ser exigido, com fulcro no art. 41, inciso IV, da Lei nº 14.133/21, em caso do fornecedor sendo, revendedor ou distribuidor, a declaração do fabricante que assegure a licitante ser revenda autorizada a comercializar, instalar, prestar manutenção e garantia nos equipamentos de sua fabricação.

7.4. Até para não criar exigência restritivas ao mercado e em outro prisma resguardar a Administração entendemos que a exigência acima deverá recair sobre todos os equipamentos e serviços não se aplicando aos itens que se refere aos cabos/cordões óticos, itens 10 a 17.

8. LEVANTAMENTO DE SOLUÇÕES

8.1. A análise comparativa de soluções, nos termos do inc. II do art. 11 da IN-94/2022 – SGD/ME, visa a elencar as alternativas de atendimento à demanda considerando, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação.

8.2. Dessa maneira foram identificados 2 (duas) possíveis soluções para atendimento das necessidades objeto desse Estudo Técnico, conforme relacionadas na tabela a seguir:

Id Solução	Descrição da alternativa ou cenário identificado
A	Contratação de suporte e manutenção para solução implantada e licenças adicionais de NAC
B	Substituição completa da solução implantada

8.3. Entendemos que uma análise comparativa se torna viável e necessária visto que existem 2 (duas) possibilidades de atendimento à necessidade, dessa forma deve-se considerar que a solução existente há mais de 10 (dez) anos na AGU para os switches de borda, 3 (três) anos para os switches de datacenter e nova para o ambiente sem fio (wireless) apresenta-se como imprescindível visto a defasagem tecnológica, falta de suporte e atualização, sem plataforma de gerenciamento, sem solução de segurança da informação e sem ambiente sem fio nas localidades.

8.4. Em relação às possibilidades em alinhamento ao inciso II do art. 11 da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, tem-se que:

- O Software Público brasileiro não atende o objeto dessa contratação.
- As políticas, os modelos e os padrões da arquitetura e-PING de Interoperabilidade de Governo Eletrônico não se aplicam nessa contratação, visto que o objeto não abrange serviços disponibilizados pelo governo eletrônico que trabalham conjuntamente com interação e troca de informações.
- Não há necessidade de adequação do ambiente da AGU para viabilizar a execução contratual.

9. ANÁLISE COMPARATIVA DAS SOLUÇÕES

Id Solução	Descrição da alternativa ou cenário identificado	Item
A	Contratação de suporte e manutenção para solução implantada e licenças adicionais de NAC	
B	Substituição completa da solução implantada	

9.1. A solução para a demanda não foi encontrada nos Catálogos de Soluções de TIC com condições padrões definidos pelo Órgão Central do SISP.

Tabela de Requisitos 01:

Requisitos		Soluções	
		A	B
Negócio	Atualização/modernização tecnológica do ambiente de redes da AGU	Não Atende	Atende
	Tratar todo o tráfego de rede interna com segurança e gestão	Não Atende	Atende
	Garantir a resiliência de rede	Não Atende	Atende
	Ampliar o ambiente de rede sem fio para todas as unidades da AGU	Atende	Atende
	Manter a solução de redes sustentadas, atualizadas e com suporte técnico (garantia)	Atende	Atende
	Prover uma infraestrutura de rede com maior escalabilidade que acompanhe os movimentos de crescimento e diminuição de unidades físicas da AGU	Não Atende	Atende
	Redução de custos	Não Atende	Atende
	Melhor gerenciamento dos riscos	Não Atende	Atende
	Melhor eficiência	Não Atende	Atende
	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	Não Atende	Atende
	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).	Atende	Atende
	Visibilidade e controle	Atende	Atende
Tecnológico	Redução no tempo de indisponibilidade dos serviços, através do tempo para recuperação de falhas nos equipamentos	Atende	Atende
	Redução nos riscos de interrupção dos serviços, com a identificação prévia de potenciais problemas e adoção de ações	Não Atende	Atende

	preventivas em tempo hábil		
	Criação de regras e perfis de acesso a rede por meio da premissa do menor acesso	Não Atende	Atende
	Atualização de componentes físicos e lógicos (firmwares, SO e funcionalidades) da solução de redes unificada.	Atende	Atende
	Possibilidade de avaliação de postura dos equipamentos que acessem a rede da AGU.	Atende	Atende
	Controlar todo o tipo de acesso a rede gerindo aqueles acessos que necessitem de maior nível de privilégio	Atende	Atende
	Tratar todo o tráfego de rede, seja cabeado ou sem fio, de igual maneira inclusive com gerenciamento e gestão por perfil	Não Atende	Atende
Resultado da Análise		Não Atende	Atende

Id solução	Descrição da alternativa ou cenário identificado	Item
A	Contratação de suporte e manutenção para solução implantada e licenças adicionais de NAC	A contratação de suporte e garantia para os atuais equipamentos de acesso (borda) que já possuem mais de 10 (dez) anos de uso e do atual ambiente de rede Wireless que atende as sedes em Brasília DF. Aquisição de novo ambiente de rede Wireless para promover expansão para as demais unidades da AGU no Brasil. Aquisição de solução de NAC para fornecer funcionalidades de segurança no ambiente de rede.
B	Substituição completa da solução implantada	Atualização e Modernização de toda a solução de rede com fio e sem fio com garantia e suporte por 60 (sessenta) meses.

9.2. Importa destacar que em todas as soluções identificadas a AGU não irá promover a ingerência no corpo técnico tampouco exigências com relação ao quantitativo de profissionais a serem alocados para a realização do serviço que sempre estará associado a entrega/resultados sobre os NMS.

10. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

10.1. **SOLUÇÃO A:** Contratação de suporte e manutenção para solução implantada e licenças adicionais de NAC

10.1.1. A proposta de contratação de suporte e manutenção para solução implantada foi identificada com uma das soluções para se manter continuidade da solução de comutação de rede de dados de acesso (borda) e wireless da AGU com garantia e suporte técnico, entretanto, a presente solução não demonstra ser viável, posto que os equipamentos em uso na AGU, já possuem mais de 10 (dez) anos de utilização nos switches de acesso (borda) e 5 (cinco) anos nos equipamentos de rede sem fio (wireless) das sedes I e II em Brasília, ou seja, já estão em fase de obsolescência, considerando o ciclo de vida de 5 (cinco) anos, conforme orientação da Secretaria de Logística e Tecnologia da Informação do MPOG, atual Secretaria de Governo Digital, por meio da Portaria nº 20/2016.

10.1.2. Assim, quando os equipamentos chegam na fase de fim do ciclo de vida devem ser

observados os seguintes pontos críticos:

- a) A probabilidade de defeitos é elevada, causando indisponibilidades e prejudicando as atividades diárias da instituição;
- b) O fornecedor poderá ter dificuldade de provimento de peças de reposição, aumentando o risco descumprir os níveis de serviço exigidos para reparo dos equipamentos;
- c) O fabricante deixa de liberar quaisquer versões de manutenção de software finais ou correções de bugs;
- d) O fabricante deixa de analisar falhas de rotina que podem ser realizados para determinar a causa da falha do produto de hardware ou defeito;
- e) Ajuste de SLA para o reparo ou substituição de ativo antigo, em decorrência da dificuldade de se conseguir peças.

10.1.3. De forma geral a contratação de serviços de manutenção para ativos fora de garantia, usualmente é mais onerosa para a Administração do que quando o bem é adquirido com garantia para toda sua vida útil. Assim, os contratos de manutenção têm seus custos elevados na medida em que os bens se tornam obsoletos. Ou seja, quanto mais antigo for o ativo de TI, menor seu valor comercial e maior será seu custo de manutenção, devido à dificuldade de provimento de peças de reposição e do maior risco de o fornecedor descumprir os níveis de serviço exigidos para reparo desses equipamentos.

10.1.4. Outro ponto a ser destacado é o que tange a capacidade tecnológica e recursos/funcionalidades que tais equipamentos não possuem frente à novas soluções existentes no mercado.

10.1.5. Além disso, em consulta realizada no sítio do fabricante CISCO (<https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-c-series-switches/eos-eol-notice-c51-744343.pdf>) foi identificado que todos os componentes da solução já encontram-se em end-of-sale (EOS) e end-of-life (EOL) da última data de suporte do hardware (Last Date of Support: HW) em 31 de dezembro de 2020.

10.1.6. Após essa data, todos os serviços de suporte para o componente estarão indisponíveis e o produto se tornará obsoleto.

10.1.7. Assim, diante do exposto observa-se que de acordo com os pontos levantados a escolha de manter os equipamentos atuais com uma contratação de manutenção e suporte apresentam sérios riscos ao negócio, demonstrando ir na contramão dos princípios balizadores das contratações públicas, quais sejam: eficiência, eficácia e economicidade.

10.1.8. Pelo exposto, não seria conveniente ou oportuna a manutenção da solução implantada, cujo contratos de suporte técnico e garantia já estão vencidos. Em vista disso, principalmente pelos fatos de

não proporcionar a evolução tecnológica, expor a infraestrutura de rede a maior risco de indisponibilidade e ir de encontro às orientações do SISP, conclui-se que a presente alternativa é tecnicamente inviável.

10.2. SOLUÇÃO B: Substituição completa da solução implantada

10.2.1. A substituição da solução implantada foi identificada com uma segunda solução para se manter o parque tecnológico da AGU com garantia e disponibilidade, gestão centralizada e com funcionalidades de segurança avançada de modo a manter a continuidade das atividades da AGU. Esta proposta se trata de uma nova solução, completa, contando com hardware e software novos, em linha de fabricação e com garantia pelo período de 60 (sessenta) meses.

11. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

11.1. A análise comparativa de custos foi elaborada considerando as soluções técnica e funcionalmente viáveis, nos termos do inc. III art. 11 da IN-01/2019/SGD, de acordo com os menores preços obtidos para cada alternativa de solução elencada nos itens

11.2. Todos os editais localizados são similares a solução escolhida, assim, houve registro de boa parte da solução, não sendo necessário a pesquisa de preço no mercado.

11.3. Para este TCO, entende-se que o custo unitário dos serviços contratados equivale ao custo total de propriedade, já que o período de suporte técnico, incluindo substituição de peças, previsto para a contratação abrangerá toda a vigência do contrato. Assim, após o desembolso inicial realizado na compra, não é necessário investimento posterior da Administração durante a vida útil do equipamento.

11.4. Os valores da Solução B foram extraídos de PESQUISA DE PREÇOS, anexa a este Estudo Técnico, na qual estão especificadas as fontes adotadas.

11.5. Portanto, têm-se o seguinte Custo Total de Propriedade (para o período de 5 anos).

11.6. Mapa comparativo dos cálculos totais de propriedade (TCO)

ESTIMATIVA DE TCO AO LONGO DO ANO		
Descrição da solução	Ano (2024)	Total R\$
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.	R\$ 19.876.855,56	R\$ 19.876.855,56

12. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

12.1. Para o ambiente de datacenter que contempla as duas sedes de Brasília (Sedes I e II) pretende-se adotar a modelagem lógica recomendada pelo Gartner em sua publicação Market Guide for Data Center Switching (<https://www.gartner.com/document/4023324?ref=solrAll&refval=373757412&>). Recomendações que estamos seguindo na elaboração dessa contratação acompanham aquelas já trazidas no bojo do documento mencionado, tais como:

- a) Otimize a seleção de fornecedores concentrando-se em software (incluindo gerenciamento, automação e integração com sistemas de orquestração de data center mais amplos) em vez de hardware.
- b) Verifique se a oferta de gerenciamento de malha de um fornecedor atende aos seus requisitos específicos de automação, testando a automação do provisionamento inicial e das atividades operacionais comuns, incluindo a solução de problemas em um piloto, antes da compra.
- c) Crie malhas de comutação de data center baseadas em padrões “bons o suficiente” e planeje um ciclo de vida de três a cinco anos implantando uma topologia *spine-leaf* com switches de fator de forma fixo e interfaces com capacidade de 25/100G.

12.2. Falando da topologia spine-leaf, cumpre detalhar que esta nova solução irá se basear em redes de núcleo distribuído comumente referida como arquitetura spine-and-leaf, empregando dois tipos de nós: um que conecta os servidores ou elementos de topo de rack (leaf) e o segundo, que interconecta todos os switches (spine), oferecendo um desempenho sem bloqueio e latência extremamente baixa entre quaisquer duas portas da malha. Nesse mesmo documento o Gartner demonstra a esta arquitetura, conforme abaixo:

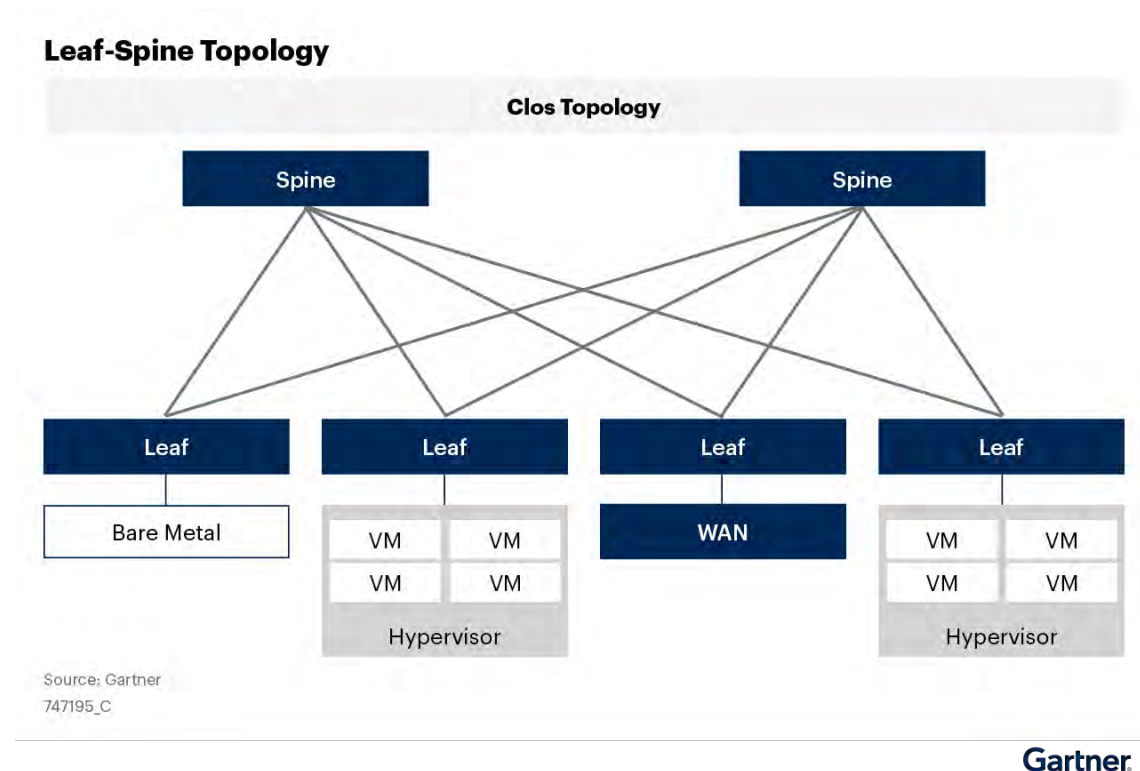


Figura 8: Topologia *Spine-Leaf* (<https://www.gartner.com/document/4023324?ref=solrAll&refval=373757412&>)

12.3. Como recomendação, nesse mesmo sentido, o Gartner recomenda que a implementação seja feita tomando como base protocolos abertos tais como o BGP (*Border Gateway Protocol*), Ethernet VPN e VxLan (*Virtual Extensible LAN*). Para essa implantação entendemos que a melhor disposição é a que acompanha o design recomendado pelo Gartner e se materializa, conforme abaixo:

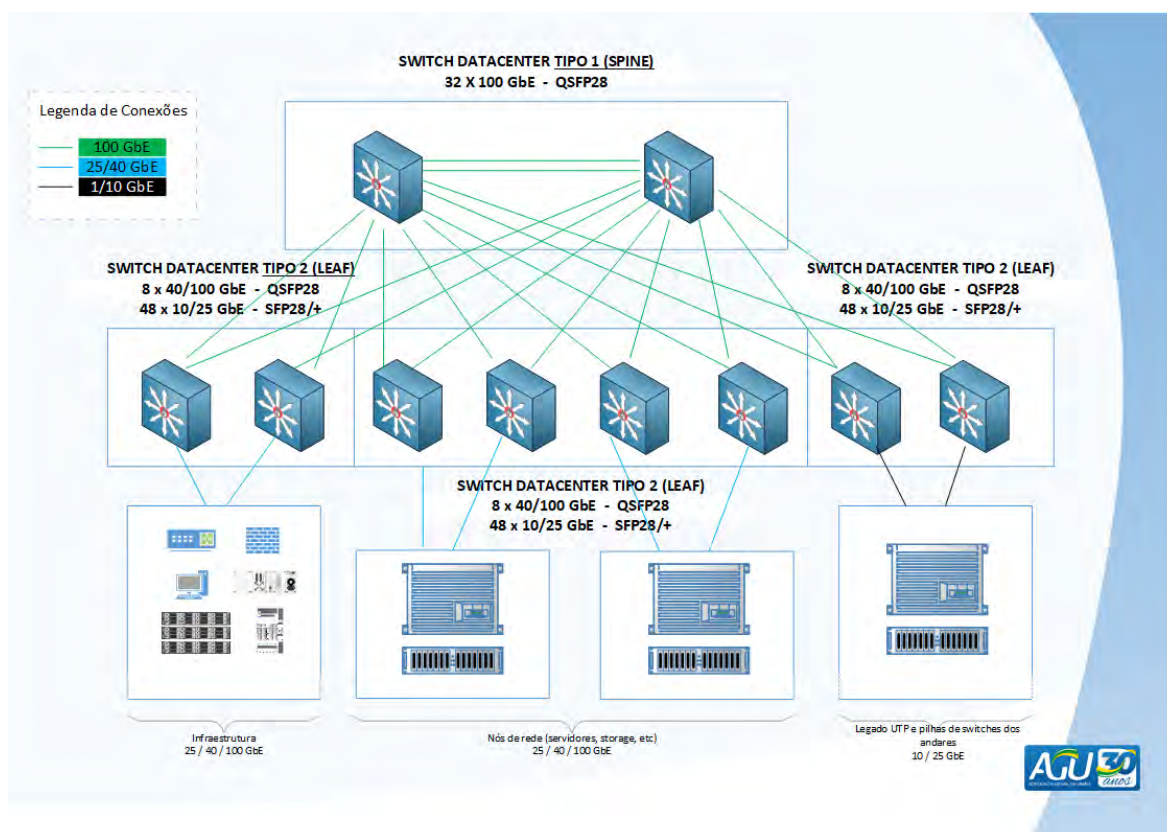


Figura 9: Topologia *Spine-Leaf* da AGU

12.4. Algumas vantagens desse modelo de arquitetura de duas camadas (*Spine-Leaf*) são os seguintes:

- a) Economia: O núcleo pode ser altamente escalonado através do uso de diversos switches Ethernet de baixo custo e de baixo consumo energético, em comparação aos sistemas caros em chassi;
- b) Alto desempenho: Há uma largura de banda bisseccional para comunicação de qualquer ponto com qualquer outro ponto da rede;
- c) Otimizado para Clusters: Qualquer host pode se comunicar com qualquer outro host na rede à largura de banda total da sua interface de rede;
- d) Resiliência: Os “nós” de switch podem ser reiniciados ou substituídos sem interromper toda a malha de switches;
- e) Flexibilidade de Plano de Controle: Uma malha de núcleo distribuído pode utilizar protocolos de IP (OSPF, BGP) ou Ethernet (TRILL) baseados em padrões de mercado.

12.5. A arquitetura de núcleo distribuído oferece uma maior escalabilidade, maior largura de banda e maior resiliência como base da rede para o Centro de Dados da AGU, que lida com grande quantidade de tráfego de dados e que emprega clusters de computação.

12.6. Para a opção de escolha da solução de acesso, está mais simples, baseia-se no conceito de switches de acesso (borda) podendo ou não serem empilhados entre si permitindo tratar a pilha de

switches como um único conjunto capaz de trafegar os dados de uplink por meio de um único par de fibra de uplink. Em casos em que a unidade não possua fibra o uplink será provido por meio de par metálico RJ45. Uma necessidade real nesse caso é que esses switches sejam dimensionados adequadamente e possuam recursos de POE e POE2 para permitir que equipamentos de VOIP e Access Points possam ser energizados e controlados pelo switch. Tratando, ainda, do ambiente de Switches de Acesso (Borda) temos a necessidade de que esses ativos acompanhem às necessidades das unidades da AGU em fornecer um ambiente de rede, por onde trafegam dados e credenciais a todo instante, que seja seguro e resiliente. É preciso determinar, por exemplo, se um equipamento particular do usuário (smartfone ou notebook) está seguro o suficiente para se integrar na rede AGU. É muito comum os usuários ligarem os cabos de rede do ambiente da AGU em seus notebooks e passem a acessar a rede da AGU livremente. É algo comum, tão comum quanto conectar seu aparelho, seja notebook ou smartfone, na rede wireless e passar a acessar a rede como se fosse um equipamento próprio da AGU. Sendo assim os switches de acesso (borda) foram dimensionados e quantificados considerando o quantitativo de usuários que cada uma das unidades da AGU possui. Serão 2 (dois) tipos de equipamentos 24 e 48 portas que objetivam atender às necessidades da casa. Detalhes desse estudo de dimensionamento encontra-se na planilha Anexo I deste Estudo Técnico.

12.7. Já o ambiente de rede sem fio (Wireless) é de igual maneira uma premissa básica que seja totalmente integrada e faça parte de uma mesma camada de gestão. Deve permitir que às soluções de segurança sejam aplicadas, igualmente, nesse ambiente. E deve trazer funcionalidades específicas do ambiente sem fio que será detalhada nas especificações técnicas da solução.

12.8. Dessa maneira, igualmente aplicada, considerou-se a tabela do Anexo I para dimensionar o tamanho dos equipamentos já que a quantidade de clientes simultâneos é o fator capaz de definir o porte dos Access Points.

12.9. Para atender às necessidades e acompanhar as Boas Práticas, hoje o mercado dispõe de solução de ferramentas de segurança, gestão e controle do ambiente de rede unificada (Unified Network).

12.10. O Gartner em sua publicação (Critical Capabilities for Enterprise Wired and Wireless LAN Infrastructure (<https://www.gartner.com/document/4022674?ref=solrAll&refval=373758889&>)) de janeiro de 2023, traz estudo de casos onde se analisa a solução completa cabeada e sem fio na visão por fabricantes. Pode-se relacionar no estudo pelo menos 12 (doze) fabricantes com ampla condição de atendimento de uma necessidade de solução unificada. Um dos quesitos mais importantes em se tratando de redes unificadas trata-se das funcionalidades de NAC (Network Access Control – Controle de Acesso em Rede). O Gartner traz em sua publicação (Market Guide for Network Access Control (<https://www.gartner.com/document/4002144?ref=solrAll&refval=373758889&>)) uma visão geral do

mercado e fornecedores de solução NAC.

12.11. Uma solução NAC se propõe a aumentar a visibilidade e o controle de dispositivos e usuários em redes locais. Como recomendações para a adoção da solução NAC é o fato que a implementação do NAC seja, minimamente, feita como parceira da infraestrutura de rede para possibilitar, minimamente, melhores respostas de segurança baseada na integração. Como definição os provedores comerciais de NAC se dividem em 2 (duas) categorias que contemplam fornecedores puros de NAC e fornecedores de infraestrutura de rede. Neste último o funcionamento se baseia em métodos de autenticação baseados em RADIUS e 802.1x. O Gartner traz nesse mesmo documento uma figura que demonstra a forma de operação do serviço de NAC, conforme abaixo:

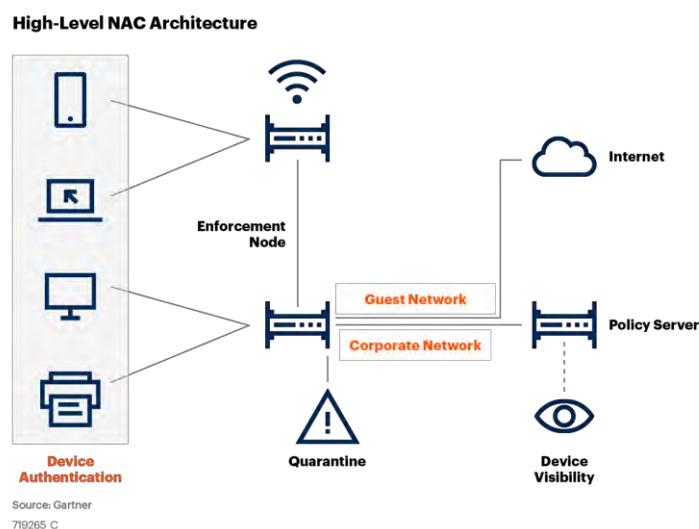


Figura 6: Arquitetura NAC (<https://www.gartner.com/document/4002144?ref=solrAll&refval=373758889&>)

12.12. Uma arquitetura NAC inclui a capacidade de visualizar dispositivos conectados à rede com técnicas de varredura passiva ou ativa. Ele também reforça a autenticação de dispositivos e usuários usando nós de imposição, como pontos de acesso sem fio e switches, ou métodos de autenticação fora de banda. Depois de autenticados, os produtos NAC autorizam o acesso e atribuem usuários e dispositivos a segmentos de rede ou dispositivos de quarentena com base em sua postura de segurança. Eles podem autenticar dispositivos corporativos e "dispositivos pessoais como é o caso da AGU" (BYOD) e atribuí-los à rede correta, seja corporativa ou apenas redes de acesso à Internet para convidados (conforme a Figura 6 acima). Explorando um pouco as possibilidades em cima do cenário acima vamos imaginar que um usuário conectou um notebook contaminado por um malware (ex. Ramsonware) na rede e passou a navegar tranquilamente. Em algum momento esse malware começa a se disseminar na rede e criar a sua cadeia de comprometimento. Com uma solução NAC em operação no ambiente será possível fazer uma análise de postura prévia e “separar” o segmento de rede que esse usuário irá navegar impossibilitando que ele alcance o perímetro de rede dos equipamentos, servidores e demais

componentes da AGU que possam ser comprometidos e mais ainda a solução é capaz de detectar comportamentos anômalos e simplesmente impedir que esse notebook (BYOD) se conecte na rede (depende das definições de escolha das políticas)

12.13. Para atendimento da solução de rede unificada (Unified Network) o quadrante mágico do Gartner assim distribui as soluções de networking unificado:



Figura 7: Quadrante Mágico do Gartner (<https://www.gartner.com/document/4022457?ref=gfaimage>)

12.14. De igual maneira, nesse mesmo documento, o Gartner traz uma forma de entrega da solução de redes de maneira integrada, baseada em solução, que ele nomeia de solução unificada ou de *Enterprise Wired and Wireless LAN Infrastructure* que envolve a entrega de hardware e software para compor a solução. O Gartner deixa claro que: a combinação de hardware de rede e software é essencial para abordar a agilidade da missão organizacional, a segurança generalizada e os níveis aumentados de desempenho exigidos pelos usuários finais em todas as categorias de aplicativos e dispositivos conectados. Adicionalmente essas ferramentas de software integradas aceleram o tempo para concluir implantações de rede corporativa, reduzem o tempo para identificar e resolver problemas de rede e aplicativos e fornecem ferramentas de automação abrangentes que reduzem as cargas de trabalho do administrador de rede.

12.15. Mas aprofundando um pouco mais no conceitual e nas possibilidades de entrega de soluções de rede cabeada e sem fio podemos perceber que o conceito de rede corporativa foi moldada por mais de 30 anos de fornecimento, principalmente, de conectividade e resiliência nas Camadas 2 e 3 do modelo de rede OSI. Como resultado, os compradores esperam recursos robustos de comutação de Camada 2

tradicionais, alimentação apropriada sobre Ethernet para suportar hardware VoIP e AP, qualidade de serviço (QoS) e velocidades de uplink suficientes para suportar vários requisitos de tráfego. Na camada de acesso sem fio da rede, os clientes esperam a **potência**, o **desempenho** e a **taxa de transferência** Wi-Fi necessários para suportar as densidades de conexão e os requisitos de largura de banda do cliente. Finalmente, as camadas de núcleo (datacenter principal) e distribuição (topo de rede/datacenter das unidades) da rede devem fornecer a redundância e a capacidade de roteamento e comutação de alta velocidade para suportar o aumento drástico do tráfego norte-sul, grande parte do qual é destinada à nuvem e a outros locais fora da rede.

12.16. Os fornecedores de redes corporativas oferecem ferramentas que utilizam vários graus de inteligência artificial, aprendizado de máquina, uma interface de linguagem natural, identificação automática de problemas e correção para reduzir a administração da rede e as cargas de trabalho operacionais. Essas ferramentas são unificadas para gerenciamento e segurança em todas as camadas da rede.

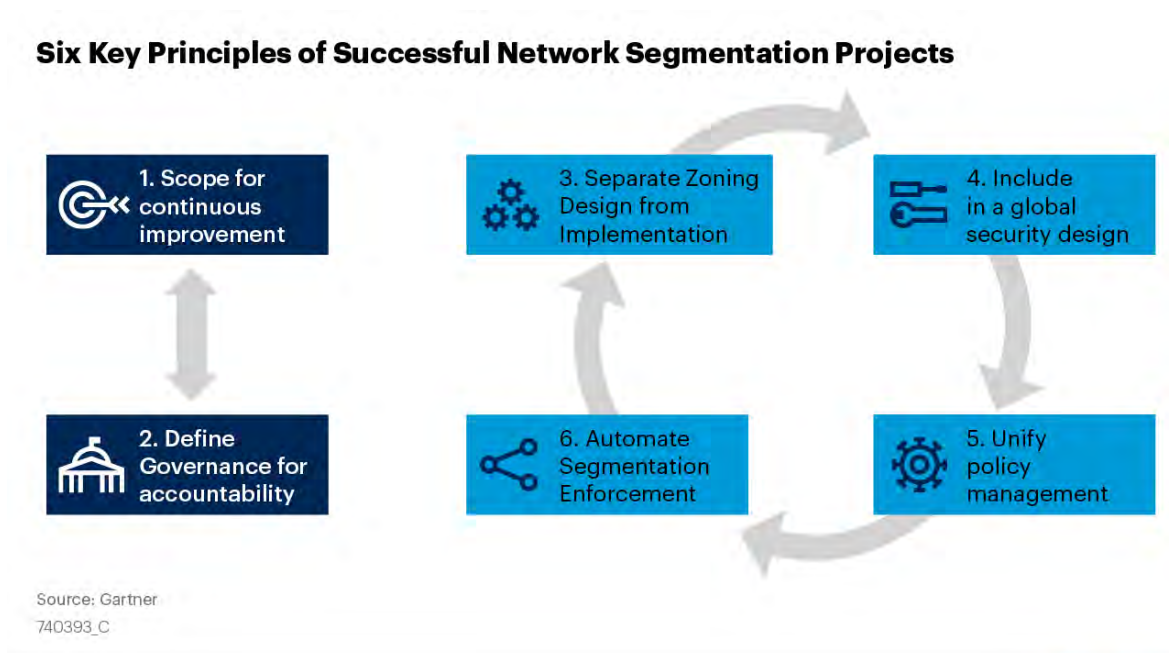
12.17. E como essas soluções podem ser entregues à AGU? O Gartner entende que os compradores geralmente obtêm sua infraestrutura de LAN com fio/sem fio por meio de um parceiro de canal de fornecedor autorizado, com relativamente poucas compras ocorrendo diretamente do fornecedor da rede. Os gastos com hardware geralmente são um custo único (capital/investimento), que inclui um contrato de licenciamento de usuário final de firmware (suporte e garantia). Esses custos iniciais incluem atualizações para resolver certos bugs de firmware que afetam negativamente o uso do hardware ou vulnerabilidades de segurança que exporiam o usuário final a danos significativos se não fossem corrigidos. Futuras atualizações do sistema operacional, atualizações de recursos ou patches de segurança são uma função de um contrato de manutenção de firmware que é adquirido separadamente, no momento da compra ou em uma data futura (suporte e garantia por 5 anos, por exemplo). Os fornecedores cobram por licenças de hardware e software como uma licença perpétua ou como uma licença de assinatura, a tendência do mercado é de afastamento do licenciamento perpétuo. No modelo proposta a aquisição seria por licenciamento subscrição e suporte/garantia por 5 (cinco) anos.

12.18. As plataformas de gerenciamento de rede se tornaram onipresentes, portanto, o acesso geralmente requer licenciamento de gerenciamento separado com várias funcionalidades atribuídas a níveis mais altos. Investir apenas em equipamentos (comodities) não é mais considerado uma opção inteligente de mercado devendo se voltar para a entrega de resultados.

12.19. Não custa ressaltar que alguns fatores estão sendo considerados nessa contratação. São elas:

- a) **Visibilidade:** A rede unificada deve fornecer uma visão abrangente de toda a rede, incluindo dispositivos, tráfego e políticas. Isso pode ajudar os administradores de rede a identificarem e corrigirem os problemas mais rapidamente.
- b) **Desempenho:** A rede unificada deve ser capaz de fornecer desempenho suficiente para atender às necessidades da organização. Isso pode exigir a utilização de switches de alta largura de banda e recursos avançados, como QoS e STP.
- c) **Segurança:** A rede unificada deve ser capaz de proteger a organização contra ataques de segurança.
- d) **Eficiência:** A rede unificada deve ser eficiente em termos de custo e recursos. Isso pode exigir a utilização de switches que possam ser gerenciados centralizadamente tendo seus recursos que possam ser compartilhados por vários dispositivos.

12.20. Como o projeto trata da gestão centralizada e seguindo os 6 (seis) princípios recomendados pelo Gartner em sua publicação The 6 Principles of Successful Network Segmentation Strategies (<https://www.gartner.com/document/4002289?ref=solrAll&refval=373757412&>). Nesse documento o Gartner recomenda que:



Gartner

Figura 10: 6 chaves para se obter sucesso na segmentação de rede (<https://www.gartner.com/document/4002289?ref=solrAll&refval=373757412&>)

12.21. Os 6 princípios estão assim descritos:

- a) Escopo para melhoria contínua (por exemplo, use “perímetros” como subprojetos individuais).
- b) Construir governança para responsabilidade (por exemplo, recalibrar as expectativas de “mais zonas” para “zoneamento mais integrado”).

- c) Incorporar no projeto de segurança de rede global (por exemplo, “gama de opções e controles compensatórios”).
- d) Separe o projeto de zoneamento da implementação (mantenha o projeto interno, misture os princípios de zoneamento conforme necessário).
- e) **Unifique o gerenciamento de políticas** (por exemplo, obtenha o fluxo de trabalho correto para descoberta de aplicativos e gerenciamento de alterações).
- f) **Automatize a aplicação da segmentação** (por exemplo, ofereça segmentação como um recurso de negócios empacotado).

12.22. É dessa maneira esse projeto se estrutura baseado em um ambiente totalmente integrado, que seja capaz de lidar com o improvável, baseado em uma análise eminentemente comportamental, com recursos e funcionalidades de IA (Inteligência Artificial) e que possa fornecer uma base sólida contra as ameaças existentes e as que estão por vir.

12.23. Com uma segmentação lógica inteligente e uma solução robusta de gerenciamento e segurança vislumbra-se a análise de postura dos equipamentos e a separação para uma rede quarentena caso não atenda a requisitos básicos definidos pelo administrador da rede. Essa solução deverá acompanhar o tempo de vida do usuário e seu dispositivo enquanto os acessos dele à rede permanecer e deverá tomar ações baseada em comportamentos com potencial de danos.

12.24. A justificativa para o parcelamento ou não do objeto

12.24.1. O art. 18, inciso 1º, item VIII da lei 14.133/2021, determina que:

§ 1º O estudo técnico preliminar a que se refere o inciso I do caput deste artigo deverá evidenciar o problema a ser resolvido e a sua melhor solução, de modo a permitir a avaliação da viabilidade técnica e econômica da contratação, e conterá os seguintes elementos:

...

VIII – justificativas para o parcelamento ou não da contratação;

12.24.2. O art. 40, item V, subitem b) da lei 14.133/2021, determina que:

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

...

V – atendimento aos princípios:

b) do parcelamento, quando for tecnicamente viável e economicamente vantajoso;

12.24.3. E conforme o inciso 3º do mesmo art. 40, da lei 14.133/2021, determina que:

§ 3º O parcelamento não será adotado quando:

I – a economia de escala, a redução de custos de gestão de contratos ou a maior vantagem na contratação recomendar a compra do item do mesmo fornecedor;

II - o objeto a ser contratado configurar sistema único e integrado e houver a possibilidade de risco ao conjunto do objeto pretendido; grifo

III - o processo de padronização ou de escolha de marca levar a fornecedor exclusivo.

§ 4º Em relação à informação de que trata o inciso III do § 1º deste artigo, desde que fundamentada em estudo técnico preliminar, a Administração poderá exigir que os serviços de manutenção e assistência técnica sejam prestados mediante deslocamento de técnico ou disponibilizados em unidade de prestação de serviços localizada em distância compatível com suas necessidades.

12.24.4. Nesse sentido, a Equipe de Planejamento da Contratação avaliou a viabilidade de realizar o parcelamento da solução de TIC a ser contratada, em tantos itens quanto se comprovasse técnica e economicamente viável, porém, verificou-se que o parcelamento dos itens descaracteriza a unicidade da solução e compromete seriamente a entrega dos resultados pretendidos podendo, inclusive aumentar os custos para atendimento da solução necessária.

12.24.5. Dessa forma a adjudicação do objeto deve ser menor preço GLOBAL, pois trata-se Contratação de solução de conectividade de Datacenter, Borda e Wireless para a AGU. No caso em apreço, a integração da prestação de serviços em único Grupo é a forma mais adequada de adjudicação. A divisão, com a possível ampliação da quantidade de contratos, revela-se administrativa e economicamente desinteressante, pelas seguintes razões:

12.24.6. **Sob o aspecto de gestão:** Centralização em único contratado, para execução dos serviços, racionaliza o acompanhamento, a fiscalização contratual, facilitando o controle detectivo de problemas e a proposição e o monitoramento de soluções.

12.24.7. **Sob o aspecto técnico:** O objeto da licitação apresenta elevadas especificidades, como uma solução completa que para se possa alcançar os seus objetivos deve operar em completa sinergia com todos os componentes de rede, fazendo-se uma comparação é como se se analisássemos uma orquestra sinfônica onde cada instrumento exerce seu papel para que o resultado final seja alcançado. Aspectos relacionados a funcionalidades e recursos, gestão, segurança e tomada de decisão de maneira autônoma é necessário para um ambiente tão vasto e sem uniformidade.

12.24.8. Desde já firmado que ampliação do número de potenciais licitantes é um instrumento desejável para que a Administração obtenha melhores ofertas em virtude do aumento da competitividade, compreendemos que este não é o objetivo imediato e primordial de um processo licitatório – que entendemos ter como direcionador maior a tutela do interesse público, aqui traduzido pelo atendimento à necessidade da Administração da forma mais tecnicamente adequada e economicamente viável. Logo, não seria justificável adotar um modelo de parcelamento que acarrete perda de benefícios e/ou em elevação de custos somente em função de que isso potencialmente beneficiaria a um número maior de particulares.

12.24.9. O agrupamento e adjudicação em Grupo é lícito, “desde que os lotes sejam integrados por itens de uma mesma natureza e que guardem relação entre si” (Acórdão TCU 5.260/2011-1ª Câmara). Também nessa linha, é certo que, conforme disserta o Acórdão TCU nº 861/2013, o “aumento da eficiência administrativa do setor público passa pela otimização do gerenciamento de seus contratos de fornecimento. Essa eficiência administrativa também é de estatura constitucional e deve ser buscada pela administração pública”.

12.24.10. Ao se admitir uma quantidade demasiada de fornecedores, além da **perda de uniformidade e padronização da solução**, haveria evidente risco de descompasso no fornecimento dos itens da solução, além da elevação da complexidade dos procedimentos de gestão contratual. Destarte, a admissão da adjudicação por item, desconfigura a caracterização da Solução de Tecnologia da Informação, vez que resultaria na **perda irreparável da capacidade de integração dos serviços e do potencial de compartilhamento de recursos** – condições que não podem ser asseguradas meramente mediante especificações técnicas.

12.24.11. Portanto, a estruturação proposta agrupa de forma lícita, segura, técnica e economicamente viável, serviços de uma mesma natureza, que guardam correlação entre si, seja por similaridade técnica ou de tecnologia, bem como de aplicabilidade e de configuração do modelo de contratação propriamente dito, sem causar qualquer prejuízo à ampla competitividade. Por fim encontra-se preservado os interesses públicos no modelo de agrupamento abaixo:

GRUPO	ITEM	DESCRIÇÃO	MÉT.	QTD.	VALOR UNITÁRIO	VALOR TOTAL
1	1	Switch Datacenter - Tipo 1 (Spine)	Und	4	R\$ 200.663,83	R\$ 802.655,32
	2	Switch Datacenter - Tipo 2 (Leaf)	Und	14	R\$ 147.067,75	R\$ 2.058.948,50
	3	Switch Acesso tipo 3 (24 portas PoE Base T)	Und	230	R\$ 15.681,91	R\$ 3.606.839,30
	4	Switch Acesso tipo 4 (48 portas PoE Base T)	Und	100	R\$ 21.390,86	R\$ 2.139.086,00
	5	Interface Ótica (transceiver) 100Gbe QSFP28 100GBase-SR4 MPO	Und	60	R\$ 8.799,31	R\$ 527.958,60
	6	Interface Ótica (transceiver) 40Gbe QSFP28+ 40GBase-SR4 MPO	Und	40	R\$ 5.827,38	R\$ 233.095,20

7	Interface Ótica (transceiver) 25Gbe SFP28+ 25GBase-SR	Und	240	R\$ 3.787,34	R\$ 908.961,60
8	Interface Ótica (transceiver) 10Gbe QSFP28	Und	60	R\$ 1.240,00	R\$ 74.400,00
9	Access Point Tipo 1 (4x4)	Und	160	R\$ 8.963,98	R\$ 1.434.236,80
10	Access Point Tipo 2 (2x2)	Und	550	R\$ 5.071,08	R\$ 2.789.094,00
11	Solução de Gerenciamento e Controladora	Und	1	R\$ 689.336,96	R\$ 689.336,96
12	Solução de NAC	Und	5000	R\$ 559,84	R\$ 2.799.200,00
13	Cabo DAC para Empilhamento (Switches Tipo 3 e 4) ou Fibra	Und	170	R\$ 509,00	R\$ 86.530,00
14	Cabo Ótico 100 Gbe QSFP28 15 mts – MPO	Und	60	R\$ 1.600,00	R\$ 96.000,00
15	Cabo Ótico 40 Gbe QSFP28 10 mts - MPO	Und	40	R\$ 1.400,00	R\$ 56.000,00
16	Cabo Ótico 25 Gbe SFP28 10 mts	Und	240	R\$ 163,11	R\$ 39.146,40
17	Cabo Ótico 10 Gbe SFP+ Base-SR MMF LC 10 mts	Und	40	R\$ 163,11	R\$ 6.524,40
18	Serviço de Instalação e Configuração dos Switches de Datacenter Tipos 1 e 2	Und	18	R\$ 28.272,36	R\$ 508.902,48
19	Serviço de Instalação e Configuração dos Switches de Acesso Tipos 3 e 4	Und	330	R\$ 993,00	R\$ 327.690,00
20	Serviço de Instalação e Configuração dos Access Point Tipos 1 e 2	Und	710	R\$ 975,00	R\$ 692.250,00
TOTAL GERAL					R\$ 19.876.855,56

12.24.12. Dessa maneira temos um único Lote/Grupo com 20 (vinte) itens. Como esse projeto trata-se de um Registro de Preços tem como característica a necessidade de ser implementado sob demanda, ou seja, por etapas.

13. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

13.1. 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 custos unitários apostos neste Estudo.

14. JUSTIFICATIVA TÉCNICA DA ESCOLHA DA SOLUÇÃO

14.1. Com relação aos requisitos técnicos, a solução foi especificada tanto para prover as funcionalidades mínimas para atendimento das necessidades do ambiente tecnológico da AGU. Após análise técnica das soluções levantadas a substituição da solução implantada da Advocacia-Geral da União se mostra a mais vantajosa do ponto de vista técnico.

14.2. A especificação do objeto também considerou os critérios de sustentabilidade ambiental contidos no Art. 5º da Instrução Normativa nº 01, de 19 de janeiro de 2010, da Secretaria de Governo Digital do Ministério da Economia e no Decreto nº 7.746, de 05 de junho de 2012, da Casa Civil da Presidência da República, no que couber.

14.3. A escolha pela contratação, foi baseada na análise com mais vantajosidade dos aspectos técnicos e econômicos da solução, se mostrando ser a mais viável, quer sob a perspectiva técnica, econômica e, especialmente, sob a ótica da segurança da informação.

14.4. Pelas razões acima delineadas e pelo já exposto tecnicamente no item 13 deste estudo técnico preliminar, o cenário escolhido, mostra-se incontestado, por esse motivo, esta equipe de planejamento declara viável a contratação Substituição completa da solução implantada de modo a atender todas as necessidades da AGU e ainda viabilizar a continuidade de sua operação, descartando-se desde já as demais opções.

14.5. Por fim, este estudo demonstrou as vantagens técnicas e econômicas de se proceder com a contratação de solução de TI que viabilize a substituição dos equipamentos danificados.

14.6. Características técnicas necessárias para ao atendimento da solução objeto desse estudo técnico seguem, de maneira detalhada, no Anexo II e justificadas no Anexo III desse Estudo Técnico.

15. JUSTIFICATIVA ECONÔMICA DA ESCOLHA DA SOLUÇÃO

15.1. Uma vez que se busca uma solução que, além de garantir a economicidade, reduza a indisponibilidade e garanta a eficiência do serviço público, a contratação de suporte e manutenção para solução implantada, **SOLUÇÃO A:** Contratação de suporte e manutenção para solução implantada e licenças adicionais de NAC, não se configura como uma escolha tecnicamente viável, tendo em vista os riscos apontados na análise da solução, bem como o fato de ser uma opção que usualmente é mais

onerosa para a Administração do que quando o bem é adquirido com garantia para toda sua vida útil, tal qual explicita o item 1.2, AQUISIÇÃO DE ATIVOS COM GARANTIA VERSUS CONTRATAÇÃO DE SERVIÇOS DE MANUTENÇÃO, do documento de BOAS PRÁTICAS, ORIENTAÇÕES E VEDAÇÕES PARA CONTRATAÇÃO DE ATIVOS DE TIC – Versão 4 (https://www.gov.br/governodigital/pt-br/contratacoes/orientacoes_ativos-de-tic-v-4.pdf), do MP/STI, anexo da à Portaria MP/STI nº 20/2016, conforme segue:

1.2.1. Os ativos de TI devem ser adquiridos com garantia de funcionamento provida pelo fornecedor durante sua vida útil, salvo quando justificado o contrário e com relação ao ativo em específico.

1.2.2. Tal procedimento se justifica pelo fato de que, de forma geral a contratação, a posteriori, de serviços de manutenção para ativos fora de garantia, usualmente é mais onerosa para a Administração do que quando o bem é adquirido com garantia para toda sua vida útil. Ainda, os contratos de manutenção têm seus custos elevados na medida em que os bens mantidos se tornam obsoletos. Ou seja, quanto mais antigo for o ativo de TI, menor seu valor comercial e maior será seu custo de manutenção, devido à dificuldade de provimento de peças de reposição e do maior risco de o fornecedor descumprir os níveis de serviço exigidos para reparo desses equipamentos.

1.2.3. Tem-se, portanto, que um dos fatores que para definição do posicionamento adequado da tecnologia (item 1.1) é o tempo de vida útil previsto para utilização do ativo e, por conseguinte, o tempo de garantia de funcionamento a ser contratado. (grifo nosso)

15.2. O referido documento tem força normativa legal, estando vinculado à Portaria MP/STI nº 20, de 14 de junho de 2016, na forma de anexo, tendo sido assinado, em sua última versão, pelo Secretário de Tecnologia da Informação do Ministério do Planejamento, Desenvolvimento e Gestão em 22/03/2017 e publicado em 23/03/2017.

15.3. Verificou-se ainda a existência de uma solução que se baseia na substituição da solução implantada, **SOLUÇÃO B**. Esta proposta, além de atender às recomendações legais, estabelece padrões de qualidade, com vistas ao ganho na eficiência e economicidade para a Administração Pública.

15.4. Em busca de se realizar o melhor atendimento às necessidades desta contratação, considerando a situação crítica da AGU, o Guia de Boas Práticas de Contratação de Ativos de TI, e que os seus equipamentos já se encontram fora da garantia e já com o fim da vida útil, observou-se, por meio desta análise, que diante das possíveis alternativas elencadas para se manter o parque tecnológico da AGU com garantia e disponibilidade, de modo a manter a continuidade do negócio, a que melhor que atenderá às necessidades da AGU será a **SOLUÇÃO B** – Substituição Completa da Solução Implantada.

15.5. Desta forma, todo o parque tecnológico está fora do tempo de vida útil e está obsoleto, a alternativa mais viável técnica e econômica é a aquisição de novos ativos de TI. Contudo, para garantir a economicidade na aquisição de bens de TI é essencial definir as especificações técnicas de modo que atendam à real necessidade da AGU e a garantia aderente ao tempo de vida útil do equipamento, também

é essencial estabelecer níveis mínimos de serviço para reparo e substituição dos ativos defeituosos com aplicação de glosas em caso de descumprimento dos níveis de serviço estabelecidos.

15.6. Portanto, a solução escolhida se baseia na aquisição de novos switches com garantia de 60 (sessenta) meses, considerando a vida útil mínima de 5 (cinco) anos para fins de posicionamento da tecnologia e de garantia de funcionamento, em conformidade com o item 1.4, ORIENTAÇÕES ESPECÍFICAS SOBRE CICLO DE VIDA, do documento de BOAS PRÁTICAS, ORIENTAÇÕES E VEDAÇÕES PARA CONTRATAÇÃO DE ATIVOS DE TIC – Versão 4 (https://www.gov.br/governodigital/pt-br/contratacoes/orientacoes_ativos-de-tic-v-4.pdf), do MP/STI, anexo a Portaria MP/STI nº 20/2016.

16. BENEFÍCIOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

16.1. Esta contratação objetiva substituir os equipamentos de rede da AGU (datacenter, acesso e Wifi) que, pelas razões já expostas, irá trazer além do ambiente sustentando, com suporte, atualização e garantia, recursos avançados de segurança e gestão (gerência). Como benefícios temos os seguintes:

- a) Manter a disponibilidade dos serviços de rede de dados;
- b) Atender às necessidades de negócio, garantindo infraestrutura de TI adequada para a execução das atividades da AGU;
- c) Mitigar possíveis riscos, danos ou indisponibilidade a prestação de serviços de TI, decorrentes de problemas técnicos identificados nos equipamentos;
- d) Permitir a criação de condições favoráveis para manter os níveis de desempenho e disponibilidade exigidos;
- e) Garantir a continuidade do funcionamento dos sistemas da AGU, dentre eles do SAPIENS;
- f) 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.

16.2. Dessa maneira, com a presente contratação, busca-se que a AGU continue exercendo com eficiência seus objetivos institucionais e que mantenha os serviços com disponibilidade e segurança.

17. PROVIDÊNCIAS A SEREM ADOTADAS

17.1. Todas as adequações necessárias, incluindo instalação e configuração da solução, serão de responsabilidade da CONTRATADA.

17.2. A prestação destes serviços deverá ocorrer, preferencialmente, nos dias e horários de expediente da unidade, nada impedindo, porém, que se realizem fora do expediente, desde que haja necessidade e haja comunicado prévio da CONTRATADA e anuência da AGU nas unidades onde o serviço será executado.

17.3. A equipe de planejamento da contratação foi instituída via portaria juntada aos autos e este

estudo deverá ser aprovado e assinado por seus integrantes e pela autoridade máxima da área de TI.

18. DECLARAÇÃO DE VIABILIDADE

18.1. Justificativa

18.1.1. Considerando os estudos realizados, a fundamentação aduzida aos autos relativamente às necessidades a serem atendidas, ao alinhamento com o planejamento institucional, ao levantamento de preços e considerando a previsão no orçamento de 2023 dos recursos financeiros necessários, a equipe manifesta-se pela viabilidade da presente proposta de contratação.

18.1.2. O presente ESTUDO TÉCNICO PRELIMINAR, elaborado pelos integrantes TÉCNICO e REQUISITANTE em harmonia com o disposto no art. 11 da Instrução Normativa SGD/ME Nº 94/2022, considerando a análise das alternativas de atendimento das necessidades elencadas pela área requisitante e os demais aspectos normativos, conclui pela VIABILIDADE DA CONTRATAÇÃO – uma vez considerados os seus potenciais benefícios em termos de eficácia, eficiência, efetividade e economicidade. Em complemento, os requisitos listados atendem adequadamente às demandas formuladas, os custos previstos são compatíveis e os riscos identificados são administráveis, pelo que recomendamos o prosseguimento da pretensão.

19. RESPONSÁVEIS

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

19.2. Conforme o § 2º do Art. 11 da IN SGD/ME nº 94, de 2022, o Estudo Técnico Preliminar deverá ser aprovado e assinado pelos Integrantes Técnicos e Requisitantes e pela autoridade máxima da área de TIC.

INTEGRANTE TÉCNICO	INTEGRANTE REQUISITANTE
(assinado eletronicamente) Thiago de Sousa Martins	(assinado eletronicamente) Uendel da Silva Tavares

20. APROVAÇÃO E DECLARAÇÃO DE CONFORMIDADE

20.1. Aprovo este Estudo Técnico Preliminar e atesto sua conformidade às disposições da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.

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

ANEXO I – UNIDADES DA AGU

1.1. Conforme já descrito neste Estudo Técnico, para o correto dimensionamento, o DTI levantou todos os equipamentos defasados, com problemas e necessários todos eles distribuídos pelas unidades abaixo.

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 Sarmiento, 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-	5 - Tipo 3

			338	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-	5 - Tipo 3

			140	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 - Uruguiana/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 - Agrônômica - 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-	5 - Tipo 3

			021	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 - Ribeirão 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

ANEXO II – REQUISITOS TÉCNICOS 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 Weighted Fair Queuing (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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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.

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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.
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 Mpps (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>).

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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	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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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: 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);

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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;
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);

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
D-47	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-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>);
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 - EEE</i>);
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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-79	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;
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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);

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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);
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);

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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.
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:

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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.

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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
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;
G-53	Realizar o backup das configurações para permitir o retorno de uma configuração salva;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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 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 sub-redes 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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
	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;
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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);

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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
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.

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
	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;
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:

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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
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

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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
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.

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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.

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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;
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
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 – TRANSCIVER 40G QSFP28 40GBASE-SR MPO
M-1	Ser do tipo QSFP28+ de 40GBASE-SR

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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 (TRANSCIVER) 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 (TRANSCIVER) 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.

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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 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.
	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.

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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
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.

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
	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.
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.

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
T-37	Deverá a contratada realizar alguns dos seguintes serviços:
T-38	Instalação Física
T-39	Configuração Logica
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.
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;

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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	
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.

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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 Lógica
T-82	Configuração Perfil de dispositivo
T-83	Configuração com a solução de Autenticação e Registro.

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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
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.
U-5	Planejamento da Topologia de Rede.
U-6	Verificação dos Requisitos de Energia e Refrigeração.

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
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 Logica
U-16	Configuração de Alta Disponibilidade e Redundância
U-17	Implementação logica 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
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
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.

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
	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 Lógica
V-16	Implementação lógica 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

ID	REQUISITOS TÉCNICOS DA SOLUÇÃO
	Contratante, com 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.

ANEXO III – FABRICANTES QUE ATENDEM ÀS ESPECIFICAÇÕES OBJETO DESTE ESTUDO TÉCNICO

	ARUBA	CISCO	JUNIPER	FORTINET	HUAWEI
SPINE	 HPE Aruba 9300-32D 32P Manual	 CISCO NEXUS 9364C - GX Manual	 QFX5130-32CD Manual	 FS-3032E Manual	 CloudEngine 8850-64CQ-EI Manual
LEAF	 HPE Aruba 8360-48Y6C Manual	 CISCO NEXUS 9340YC-FX2 Manual	 QFX5120 Manual	 FS-2048F Manual	 CloudEngine 8861-4C-EI Manual
SWITCH DE ACESSO 24P/48P	 HPE Aruba 3810m 24G/48G poe+ 1-slot switch Manual	 Switch Cisco Catalyst C9200L-24P/48P Manual	 EX4300-24P/EX4300-48P Manual	 FS-124F-FPOE/ FS-148F-FPOE Manual	 CloudEngine S5731-H24P4XC/ CloudEngine S5731-H48P4XC Manual
PONTO DE ACESSO Tipos 1 e 2	 HPE Aruba 510 / Aruba 530 Manual	 Cisco Catalyst 9105/9115 Manual	 AP24/45 Manual	 FAP-231F-N/FAP-431F-N Manual	 AirEngine 5761-21/ AirEngine 5760-51 Manual