Termo de Referência 227/2023

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
227/2023	154043-FUNDACAO UNIVERSIDADE FEDERAL DE UBERLANDIA	PAULO RODOLFO DA SILVA LEITE COELHO	05/02/2024 17:22 (v 4.0)

Status

ASSINADO

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação/Bens de TIC		23117.072054/2023-60

1. Definição do objeto

1.1 CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1.1. Registro de preços para aquisição de equipamentos de rede de Tecnologia da Informação e Comunicação (TIC), nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

GRUPO	ITEM	ESPECIFICAÇÃO	CATMAT	UNIDADE DE MEDIDA	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
-	**1**	Firewall de grande porte: Fortinet FG-600F + UTP (Unified Threat Protection) 5 anos, ou modelo superior da Fortinet, ou nas condições do item 4.1.10.11.1	481646	unidade	4	R$632.844,58	R$2.531.378,32
						Total para o Item 1:	**R$2.531.378,32**
1	**2**	Ponto de Acesso Indoor com garantia e suporte de 60 meses	603936	unidade	550	R$7.294,00	R$4.011.700,00
	3	Ponto de Acesso Outdoor com garantia e suporte de 60 meses	609339	unidade	50	R$10.687,05	R$534.352,50
	4	Controladora para pontos de acesso com garantia e suporte de 60 meses	486317	unidade	2	R$48.725,58	R$97.451,16
	5	Injetor PoE com garantia e suporte de 60 meses	426731	unidade	50	R$684,89	R$34.244,50

	Total para o Grupo 1:	**R$4.677.748,16**

1.1.2. Os bens objeto desta contratação são caracterizados como comuns, conforme justificativa constante do Estudo Técnico Preliminar.

1.1.3. Os objetos desta contratação não se enquadram como sendo de bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021, nem tampouco correspondem a itens presentes nos Catálogos de Soluções de TIC com Condições Padronizadas publicados pelo Órgão Central do SISP.

1.1.4. Os objetos desta contratação são considerados Ativos de Tecnologia da Informação, confirme Anexo I da IN SGD nº 94 /2022, cujas exigências são apresentadas na Seção 4 deste documento

1.1.5. De acordo com o art. 10 da Instrução Normativa Seges/ME nº 81, de 25 de novembro de 2022, este documento é classificado como não sigiloso, nos termos da Lei nº 12.527, de 18 de novembro de 2011.

2. Fundamentação da contratação

2.1. A Fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada em Tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

2.2. O objeto da contratação está previsto no Plano de Contratações Anual 2024, conforme detalhamento a seguir:

I) ID PCA no PNCP: 25648387000118-0-000001/2024

II) Data de publicação no PNCP: 19/05/2023

III) Id do item no PCA: 5060, 5061.

IV) Classe/Grupo: 7050 - EQUIPAMENTOS DE REDE DE TIC - LOCAL E REMOTA

V) Identificador da Futura Contratação: 154043-90223/2023

2.3. A utilização do Sistema de Registro de Preços na presente contratação justifica-se pela necessidade de instalação em etapas, com o intuito de minimizar a parada da infraestrutura de rede da UFU. Além deste aspecto, a abertura de processo com maior quantidade de itens possibilita economicidade pelo ganho em escala e garantia de aquisição do quantitativo total dos mesmos fabricantes, reduzindo, ainda, a possibilidade de aumento dos preços e a consequente inviabilidade de se contratar o quantitativo planejado. Assim sendo, justifica-se a utilização do SRP considerando o inc. I do art. 3º do Decreto 11.462/2023

3. Descrição da solução

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

3.1.1. Esta seção detalha a diferença entre um firewall tradicional e o de próxima geração, justificando a escolha do equipamento descrito nas seções anteriores. Com o aumento de ataques a redes de computadores, especialmente ataques com finalidade econômica no intuito de sequestrar a rede e serviços internos de companhias e solicitar pagamento de resgates para liberação de acesso (ransomware), empresas no mundo todo tem gastado milhões de dólares para aumentar a segurança de suas redes. Firewalls tem papel central na proteção da rede, pois servem de porta de entrada entre a rede externa (geralmente a internet) e a rede interna da empresa/instituição. Existem dois tipos principais de firewalls, os chamados firewalls tradicionais e os próxima geração, já citados acima. Os firewalls tradicionais foram introduzidos no final da década de 80, e são capazes de operar e oferecer proteção até a quarta camada do modelo OSI, isto é, conseguem monitorar e proteger nos níveis de endereço de acesso ao meio físico (como
endereços MAC, por exemplo), endereços IP e portas TCP/UDP. Isto é feito examinando individualmente cada pacote passando pela rede e verificando se o mesmo se enquadra em alguma regra previamente configurada, permitindo a passagem pela rede, ou descartando o pacote. Apesar de ser fácil de configurar, é altamente reativo e pode ser facilmente "enganado" por hackers bots. Na década seguinte, com o avanço da tecnologia, surgiram os firewalls de terceira geração, ou ainda NGFW, presentes na maiorias das empresas de médio e grande porte atualmente. Esses equipamentos possuem diversas funcionalidades adicionais, quando comparados a firewalls tradicionais, conforme elencado a seguir:

- Conseguem trabalhar com as camadas OSI de 2 até 7, ou seja, conseguem realizar detecções e filtragens na camada de aplicação.
- Realizam *Deep Packet Inspection* (DPI), ou seja, inspecionam também o conteúdo de cada pacote.
- Realizam inspeção *stateful* , isto é, examinam o contexto geral de cada conexão, e não apenas os pacotes individualmente.
- Tipicamente oferecem serviços de acesso seguro à rede interna via VPN (Virtual Private Network).
- Permite definição de regras específicas por aplicação.
- Fornecem *Intrusion Prevention System* (IPS) capazes de bloquearem tentativas de intrusão ativamente e impedir todo tráfego futuro a partir da fonte do ataque.
- Conseguem aprender e atualizar base de dados de ameaças e softwares maliciosos, muitas vezes aliadas a técnicas de inteligência artificial.
- Fornecem monitoramento de ameaças nos níveis de usuários, equipamentos, redes e dispositivos.
- Fornecem relatórios avançados com detalhamento em tempo real e diversas opções de filtragem.

3.1.1.1. Considerando o fim da garantia e suporte dos equipamentos FortiGate 1500D no campus Santa Mônica, bem como o fato de que o fabricante descontinou a venda e possibilidade de extensão da garantia do mesmo, e considerando ainda, a necessidade de manter alta disponibilidade (HA - *High Availability*) e não interromper toda a rede da UFU em caso de parada de um dos equipamentos, são necessários 2 firewalls de grande porte para o campus Santa Mônica. A necessidade de alta disponibilidade também se aplica ao campus Umuarama que, com a modernização da rede sem fio e o aumento dos links de internet para além dos limites suportados pelos equipamentos atualmente instalados, necessitará de 2 firewalls de grande porte. Deste modo, necessita-se de um total de 4 (quatro) firewalls de grande porte.

3.1.2. Com relação à solução de rede sem fio, o aspecto principal considerado foi a escolha de equipamentos que trabalhem com a tecnologia Wi-Fi 6, nome popular para o padrão IEEE 802.11ax. IEEE é o órgão que reúne todas as especificações de redes sem fio no padrão de conjuntos de redes Wi-Fi (802.11). O Wi-Fi 6 foi publicado oficialmente em 2021 com as seguintes especificações:

- Velocidade máxima de transferência de dados: até 9,6 Gb/s, dependendo do equipamento utilizado, número de fluxos espaciais e canal de operação;
- Largura de canal: até 160 MHz;
- Frequência de operação: 2,4 GHz e 5 GHz;
- Modulação: 1024QAM;
- MIMO: suporte para transmissões simultâneas em múltiplos dispositivos (MU-MIMO);
- Protocolo de segurança: WPA3;
- Outras tecnologias: OFDMA, BSS Coloring, TWT.

3.1.2.1. De acordo com a Wi-Fi Alliance, a velocidade máxima teórica do Wi-Fi 6 é de até 9,6 Gb/s, enquanto o Wi-Fi 5 (802.11 ac) atinge até 6,93 Gb/s. A experiência de uso é muito superior no padrão mais recente, uma vez que o Wi-Fi 6 funciona com a frequência de 2,4 GHz e entrega taxas de dados mais rápidas em uma área de cobertura maior. Além disso, tecnologias como o MU-MIMO (*Multi Users, Mutiple Input Multiple Output*) permitem que múltiplos dispositivos conectados façam conexões ao mesmo tempo, melhorando as velocidades de transmissão e experiência de uso da rede Wi-Fi.

3.1.2.2. Os pontos de acesso são configurados e monitorados pela controladora, de tal modo que a exigência de uma controladora é essencial. Caso a controladora fornecida ao final do processo licitatório seja virtual, isto é suficiente para garantir o funcionamento adequado da rede em casos de falha, pois a reinicialização da máquina virtual da controladora ou o restauro de uma versão anterior ao problema corrige o mesmo. No caso do equipamento ser físico, é recomendável a aquisição de uma segunda unidade, para aumentar a disponibilidade do serviço. Com relação aos quantitativos de pontos de acessos, temos atualmente cerca de 200 pontos de acesso indoor e apenas 10 pontos de acesso outdoor no campus Umuarama. Estes equipamentos possuem mais de 12 anos de uso ininterrupto, com tecnologia ultrapassada e potenciais falhas de segurança devido à incapacidade de atualização. Considerando que a cobertura atual do campus é inferior a 50%, realizou-se uma análise da cobertura atual para abranger os 44 blocos localizados neste campus, bem como suas áreas externas. A análise aponta a necessidade de ao menos 40 pontos de acesso externos e 500 pontos de acesso internos. Considerando uma margem de segurança neste quantitativo, estima-se que a quantidade de pontos de acesso necessária seja de 50 pontos de acesso externos e 550 pontos de acesso internos. Os 50 pontos de acesso externos demandam alimentação por meio de injetores de potência, ou seja, deve-se adquirir 50 unidades, uma para cada ponto de acesso.

3.1.3. Visando uma instalação escalonada, principalmente no sentido de interrupção mínima dos serviços e sistemas em operação e adequação das atividades à força de trabalho disponível no Centro de Tecnologia da Informação e Comunicação (CTIC), órgão responsável pela gerência de toda a infraestrutura de rede da Universidade, recomenda-se a aquisição dos equipamentos e sua instalação em quatro etapas.

3.1.3.1 A etapa inicial, com previsão de execução até março de 2024, compreende a instalação e configuração de 2 firewalls de grande porte no campus Santa Mônica, em substituição aos equipamentos com garantia e suporte do fabricante próximos de expirar.

3.1.3.2. A segunda etapa, com previsão de execução até outubro de 2024, compreende a melhoria da segurança na rede e início da modernização da rede sem fio do campus Umuarama, correspondendo à aquisição dos 2 firewalls de grande porte restantes, da controladora de rede sem fio, de 50 pontos de acesso externos com os respectivos injetores PoE, além de 100 pontos de acesso internos.

3.1.3.3. A terceira e quarta etapa, realizadas no primeiro e segundo semestres de 2025, correspondem à aquisição dos pontos de acesso internos restantes divididos em 225 por etapa.

4. Requisitos da contratação

4.1. REQUISITOS DA CONTRATAÇÃO

Sustentabilidade

4.1.1. Os critérios de sustentabilidade eventualmente inseridos na descrição do objeto, se baseiam no Guia Nacional de Contratações Sustentáveis, na Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, e na Portaria SGD/MGI nº 2.715, de 21 de junho de 2023.

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

> 4.1.2.1. Os eventuais materiais impressos utilizados e disponibilizados, devem ser passíveis de reciclagem, visando a preservação do meio ambiente e a sustentabilidade ambiental;
>
> 4.1.2.2. A empresa deverá cumprir, no que couber, o objetivo de promoção do “desenvolvimento nacional sustentável” contido no Decreto nº 7.746 de 05 de junho de 2012;
>
> 4.1.2.3 A empresa deverá prever e adotar, no que couber, as práticas de sustentabilidade, conforme IN 01 - SLTI/MPOG, de 19 de janeiro de 2010;
>
> 4.1.2.4. A empresa deverá cumprir, no que couber, os critérios de segurança, compatibilidade eletromagnética e eficiência energética previstos na Portaria 170/2012 do Inmetro;
>
> 4.1.2.4. Os equipamentos devem possuir Certificado de Rotulagem Ambiental por organismo acreditado pelo Cgcre (INMETRO) que assegure a conformidade com a Diretiva ROHS ou Autodeclaração de conformidade emitida pela empresa atestando a conformidade com a Diretiva ROHS (*Restriction of Certain Hazardous Substances RoHS*). Essa certificação garante que os equipamentos fornecidos, periféricos, acessórios e componentes da instalação não contém substâncias perigosas como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenilpolibromados (PBBs), éteres difenilpolibromados (PBDEs) em concentração acima da recomendada pela diretiva da Comunidade Econômica Européia.

Requisitos de Negócio

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

> 4.1.2.1 A padronização do controle de segurança por meio de equipamentos NGFW em todos os campi da UFU foi implantada ao longo do ano de 2023. Os firewalls no campus Santa Mônica (duas unidades do FortiGate 1500D), entretanto, necessitam de substituição em função do final da garantia e suporte em meados de 2024 e do próprio término definitivo do suporte pelo fabricante no início de 2025, o que impede a extensão da garantia, por exemplo
>
> 4.1.2.2 Outro aspecto importante a ser considerado é a ampliação recente da capacidade do link fornecido pela RNP no campus Umuarama, de 200Mbps para 1 Gbps, atingido o limite dos firewalls ali instalados, evitando utilização efetiva da banda na ocorrência de um novo aumento da velocidade. Deste modo, este estudo prevê também a aquisição de 2 firewalls para este campus.
>
> 4.1.2.3 Ainda no campus Umuarama, temos uma enorme deficiência de cobertura da rede sem fio, sendo que os lugares cobertos pela rede sem fio corresponde a pontos de acessos com mais de 12 anos de uso, com tecnologia e velocidade inadequadas para atender à demanda apresentada.
>
> 4.1.2.4 Uma modernização da rede sem fio neste campus é fundamental, sendo co-dependente da própria atualização dos firewalls no mesmo campus para suportar a expectativa de acesso em termos de banda e de quantidade de usuários e sessões concorrentes.

Requisitos de Capacitação

4.1.3 Não será necessário treinamento à equipe que atuará com a solução, exceto na situação tratada no **item 4.1.6.2**. As etapas serão executadas inteiramente pela equipe da Divisão de Rede, a qual já possui a capacitação adequada para instalação e configurações dos equipamentos objetos desta contratação.

Requisitos Legais

4.1.4 O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis.

Requisitos de Manutenção

4.1.5. Garantia e Suporte para Firewall de grande porte

4.1.5.1. Suporte

4.1.5.1.1. O serviço de suporte técnico deverá contemplar as manutenções corretivas e evolutivas para a solução contratada e não poderão acarretar custos adicionais além do contratado.

4.1.5.1.1.1 Entende-se por "manutenção corretiva" uma série de procedimentos destinados a recolocar a solução em pleno estado de funcionamento, removendo os defeitos apresentados.

4.1.5.1.1.2 Entende-se por "manutenção evolutiva" o fornecimento de novas versões e/ ou releases corretivas e/ou evolutivas de softwares que compõem a solução corporativa do software, lançadas durante a vigência deste contrato.

4.1.5.1.2. Durante o período de vigência do contrato a CONTRATANTE terá direito, sem ônus adicional, a todas as atualizações de versão e releases dos softwares e firmwares que fazem parte da solução ofertada.

4.1.5.1.3. A CONTRATADA deverá manter o serviço de suporte técnico, disponível para a abertura e acompanhamento de chamados em tempo integral, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, todos os dias do ano, inclusive sábados, domingos e feriados, com início de atendimento e prazo de solução de acordo com o nível de severidade exigido para o caso.

4.1.5.1.4. A CONTRATADA deve possuir uma estrutura nacional de suporte técnico, possibilitando que o atendimento seja realizado no idioma nativo da equipe técnica da CONTRATANTE (português brasileiro) se necessário.

4.1.5.1.4.1. O suporte técnico deverá ser prestado pela CONTRATADA, sendo facultado a esta escalar as questões para o respectivo fabricante.

4.1.5.1.5. A CONTRATADA deverá assegurar a disponibilidade da solução conforme os Níveis Mínimos de Serviço na forma abaixo e abaixo estabelecida:

4.1.5.1.5.1. No momento da abertura do chamado, será informada a prioridade para o atendimento de acordo com as seguintes definições:

4.1.5.1.5.1.1. Prioridade 1 (Crítica): Este Nível de severidade é aplicado em situações de emergência ou problema crítico, caracterizado pela existência de ambiente paralisado;

4.1.5.1.5.1.2. Prioridade 2 (Alta): Este nível de severidade é aplicado em situações de alto impacto, incluindo os casos de degradação severa de desempenho da solução. Esse nível representa uma interrupção parcial que está ocorrendo como resultado de uma falha técnica identificada em alguma funcionalidade da solução.

4.1.5.1.5.1.3. Prioridade 3 (Média): Este nível de severidade é aplicado em situações de baixo impacto ou de problemas que se apresentam de forma intermitente;

4.1.5.1.5.1.4. Prioridade 4 (Baixa): Este nível de severidade é aplicado em situações não críticas e de caráter mais generalista; pode representar uma necessidade de apoio relacionada ao registro de um dispositivo, à mudança de propriedade de um dispositivo, correção de dados incorretos no portal de suporte ou outras necessidades gerenciais.

4.1.5.1.5.2 O tempo de resposta após a abertura dos chamados deve ser de até 1 hora, em caso de problema crítico, ou no próximo dia útil, para o caso de questões não criticas.

4.1.5.1.5.3 Caso seja comprovada a existência de um dispositivo ou componente defeituoso na solução, a CONTRATADA deve realizar o envio de um dispositivo de substituição no máximo até o próximo dia útil.

4.1.5.1.6 Os serviços de reparo dos equipamentos especificados serão executados preferencialmente onde se encontram (ONSITE);

4.1.5.2 Garantia

4.1.5.2.1 Todos os equipamentos/softwares fornecidos deverão ser novos, de primeiro uso e estarem na linha de produção atual do fabricante;

4.1.5.2.2 Todos os componentes de hardware da solução de firewall deverão ser de um único fabricante ou em regime de OEM, não sendo permitida a integração de itens não homologados (ex.: memórias e discos rígido) de terceiros que venha a ocasionar perda parcial ou total da garantia ou qualquer ônus financeiro adicional durante a vigência da garantia;

4.1.5.2.3 Todos os equipamentos objetos deste Termo de Referência deverão possuir no mínimo 60 (sessenta) meses de garantia e suporte, incluindo a troca de peças defeituosas sem qualquer ônus adicional para a contratante;

4.1.5.2.3.1 Em caso de troca, as peças ou o equipamento deverão ser novos, do mesmo fabricante e iguais ou equivalentes aos equipamentos substituídos.

4.1.5.2.4 A garantia e suporte deverão ser prestados em regime de 24 (vinte e quatro) horas, 07 (sete) dias por semana com tempo de atendimento no próximo dia útil (NBD);

4.1.5.2.5 O fabricante deve possuir central de atendimento por meio de atendimento telefônico, sistema web de help-desk (sistema de chamados) e e-mail, com disponibilidade de 24 horas por dia, 7 dias por semana e 365 dias por ano, para abertura dos chamados de garantia, comprometendo-se a manter registros dos mesmos constando a descrição do problema e permitindo consulta em tempo real aos registros;

4.1.5.2.6 Durante todo o período de garantia, a assistência técnica será prestada pelo fabricante com atendimento por mão de obra treinada e especializada;

4.1.5.2.7 Todos os equipamentos e suas funcionalidades descritas neste documento deverão ser fornecidos em pleno funcionamento e sem restrições de licenciamento;

4.1.5.2.8 A garantia deverá incluir a disponibilização de todas as atualizações de softwares e firmwares dos equipamentos, sem qualquer ônus adicional para a contratante;

4.1.5.2.8.1 As atualizações devem ser do tipo “minor release” e “major release”, permitindo a correção de vícios e para manter os softwares e firmwares de equipamentos atualizados em sua última versão;

4.1.5.2.9 Deverá ser garantido o acesso a drivers, manuais e softwares, obrigatoriamente durante o período de garantia e até que o fabricante descontinue o suporte ao equipamento;

4.1.5.2.9.1 Tal acesso deve ser realizado via site dos fabricantes dos equipamentos e softwares, devendo permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto.

4.1.6 Garantia, suporte e treinamento para Solução para rede sem fio (Wi-Fi)

4.1.6.1 Garantia e Suporte Técnico

4.1.6.1.1 Todos os equipamentos/softwares fornecidos deverão ser novos, de primeiro uso e estarem na linha de produção atual do fabricante;

4.1.6.1.2 Todos os componentes de hardware da solução de rede deverão ser de um único fabricante ou em regime de OEM, não sendo permitida a integração de itens não homologados (ex.: memórias e discos rígidos) de terceiros que venha a ocasionar perda parcial ou total da garantia ou qualquer ônus financeiro adicional durante a vigência da garantia;

4.1.6.1.3 Todo equipamento ofertado deverá possuir no mínimo 60 (sessenta) meses de garantia e suporte, incluindo a troca de peças defeituosas sem qualquer ônus adicional para a contratante;

4.1.6.1.4 Em caso de troca, as peças ou o equipamento deverão ser novos, do mesmo fabricante e iguais ou equivalentes aos equipamentos substituídos.

4.1.6.1.5 A garantia e suporte deverão ser prestados em regime de 24 (vinte e quatro) horas, 07 (sete) dias por semana com tempo de atendimento no próximo dia útil (NBD);

4.1.6.1.6 Os serviços de reparo dos equipamentos especificados serão executados preferencialmente onde se encontram (ONSITE);

4.1.6.1.7 O fabricante deve possuir central de atendimento por meio de atendimento telefônico, sistema web de help-desk (sistema de chamados) e e-mail, com disponibilidade de 24 horas por dia, 7 dias por semana e 365 dias por ano, para abertura dos chamados de garantia, comprometendo-se a manter registros dos mesmos constando a descrição do problema e permitindo consulta em tempo real aos registros;

4.1.6.1.8 O suporte técnico deverá ser prestado pela contratada, sendo facultado a esta escalar as questões para o respectivo fabricante. Deverá ser disponibilizada, cumulativamente, estrutura de suporte técnico por meio de atendimento telefônico, sistema web de help-desk (sistema de chamados) e e-mail, com disponibilidade de 24 horas por dia, 7 dias por semana e 365 dias por ano, para registro e acompanhamento de solicitações;

4.1.6.1.9 Em caso de controladora física, o prazo para troca de peças ou mesmo de todo o equipamento deve ser até o próximo dia útil à abertura do chamado técnico (NBD - Next Business Day), para os demais itens, o prazo é de 10 dias úteis;

4.1.6.1.10 Durante todo o período de garantia, a assistência técnica será prestada pelo fabricante e/ou contratada com atendimento por mão de obra treinada e especializada;

4.1.6.1.11 Todos os equipamentos e suas funcionalidades descritas neste documento deverão ser fornecidos em pleno funcionamento e sem restrições de licenciamento;

4.1.6.1.12 A garantia deverá incluir a disponibilização de todas as atualizações de softwares e firmwares dos equipamentos, sem qualquer ônus adicional para a contratante;

4.1.6.1.13 As atualizações devem ser do tipo “minor release” e “major release”, permitindo a correção de vícios e para manter os softwares e firmwares de equipamentos atualizados em sua última versão;

4.1.6.1.14 Deverá ser garantido o acesso a drivers, manuais e softwares, obrigatoriamente durante o período de garantia e até que o fabricante descontinue o suporte ao equipamento;

4.1.6.1.15 Tal acesso deve ser realizado via site dos fabricantes dos equipamentos e softwares, devendo permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto.

4.1.6.2 Treinamento

4.1.6.2.1. Considerando que a infraestrutura atual da UFU contempla equipamentos dos fabricantes Ruckus e Aruba, caso a empresa vencedora **para os items do Grupo 1** seja de fabricante diferente, deverá ser ofertado treinamento presencial nas dependências da Universidade para 4 pessoas, com duração mínima de 20 horas e emissão de certificado.

4.1.6.2.2. O treinamento deve ser realizado em até 15 dias após o recebimento definitivo dos bens da **primeira entrega**.

4.1.6.2.3. As despesas com deslocamento, diárias e passagens dos profissionais que realizarão o treinamento ficam a cargo da CONTRATADA.

Requisitos Temporais

4.1.7. A Entrega dos equipamentos deverá ser efetivada no prazo máximo de 30 (trinta) dias corridos, a contar do recebimento da Ordem de Fornecimento de Bens (OFB), emitida pela Contratante, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pelo Contratado e autorizado pela Contratante;

> 4.1.7.1 Na contagem dos prazos estabelecidos neste Termo de Referência, quando não expressados de forma contrária, excluir-se-á o dia do início e incluir-se-á o do vencimento.

Requisitos de segurança e Privacidade

4.1.8 As formas de acesso e critérios de Segurança da Informação obedecerão à Política de Segurança da Informação da contratante. A contratada deverá tratar como informações sigilosas e privadas da contratante quaisquer dados ou informações disponíveis em componentes dos equipamentos ou softwares, os quais venham a ter acesso em função da prestação de serviços, não podendo revelá-los ou facilitar seu acesso a terceiros.

Requisitos Sociais, Ambientais e Culturais

4.1.9 Os equipamentos devem estar aderentes às seguintes diretrizes sociais, ambientais e culturais:

4.1.9.1 Observar, no que couber, às exigências de sustentabilidade ambiental estabelecidas na Instrução Normativa no 01 /2010 da SLTI/MPOG, de 19 de janeiro de 2010, bem como o Decreto no 7.746/2012 que estabelece critérios, práticas e diretrizes para a promoção do desenvolvimento nacional sustentável;

4.1.9.2 Cumprir, no que couber, as exigências do inciso XI, art. 7o da Lei 12.305, de 2010, que institui a Política Nacional de Resíduos Sólidos – PNRS. 20.3

Requisitos da Arquitetura Tecnológica

4.1.10. Firewall de grande porte

4.1.10.1. Descrições básicas

4.1.10.1.1. Throughput de, no mínimo, 10.5Gbps com a funcionalidade de Threat Prevention, ou seja, com funcionalidades de Firewall, IPS, Controle de Aplicação e Antivírus habilitadas;

4.1.10.1.2. Sessões TCP concorrentes, no mínimo, 8.000.000 (oito milhões);

4.1.10.1.3. Novas sessões TCP por segundo, no mínimo, 550.000 (quinhentos e cinquenta mil);

4.1.10.1.4. Suportar no mínimo 9Gbps de throughput de Inspeção SSL;

4.1.10.1.5. Suportar no mínimo 32 Gbps de controle de aplicações;

4.1.10.1.6. Suportar no mínimo 55 Gbps de throughput de VPN IPsec;

4.1.10.1.7. Suportar no mínimo 4 Gbps de throughput de VPN SSL;

4.1.10.1.8. Suportar no mínimo throughput de 105 Mpps (milhões de pacotes por segundo);

4.1.10.1.9. Possuir ao menos 16 interfaces 1 GE RJ45;

4.1.10.1.10. Possuir ao menos 8 interfaces 1 GE SFP;

4.1.10.1.11. Possuir ao menos 4 interfaces 10 GE SFP+;

4.1.10.1.12. Possuir ao menos 4 interfaces 25 GE SPF28 com 8 transceivers inclusos, os quais devem ser do tipo 25GBASE-SR com comprimento de onda de 850nm e conector LC;

4.1.10.1.13. Suportar a criação de no mínimo 10 instâncias virtuais;

4.1.10.1.14. Possuir fontes de alimentação internas, redundantes.

4.1.10.1.15. Atender ao padrões FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB.

4.1.10.2. Funcionalidades de SD-WAN

4.1.10.2.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para umaaplicação;

4.1.10.2.2.Deve ser possível criar políticas para modelagem do tráfego definido pelo menos os parâmetros:

4.1.10.2.2.1. IP de origem;

4.1.10.2.2.3. VLAN de origem;

4.1.10.2.2.4. IP de destino;

4.1.10.2.2.5. Porta TCP/UDP de destino;

4.1.10.2.2.6. Domínio e URL de destino;

4.1.10.2.2.7. Aplicação de camada 7 utilizada (O365 Exchange, AWS, Dropbox e etc);

4.1.10.2.3. A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por ping, http, tcp/udp echo, dns, tcp-connecte twamp;

4.1.10.2.4. O SD-WAN deverá balancear o tráfego das aplicações entre múltiplos links simultaneamente;

4.1.10.2.5. O SD-WAN deverá analisar o tráfego em tempo real e realizar o balanceamento dos pacotes de um mesmo fluxo entre múltiplos links simultaneamente em uma extremidade e realizar a reordenação dos pacotes desse mesmo fluxo no outro extremo;

4.1.10.2.6. Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo;

4.1.10.2.7. A solução deve permitir a definição do roteamento para cada aplicação;

4.1.10.2.8. Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação;

4.1.10.2.9. Deve possibilitar a definição do link de saída para uma aplicação específica;

4.1.10.2.10. Deve implementar balanceamento de link por hash do IP de origem;

4.1.10.2.11. Deve implementar balanceamento de link por hash do IP de origem e destino;

4.1.10.2.12. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, dois links;

4.1.10.2.13. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;

4.1.10.2.14. A solução de SD-WAN deve possuir suporte a Policy based routing ou policy based forwarding;

4.1.10.2.15. Para IPv4, deve suportar roteamento estático e dinâmico (BGP e OSPF);

4.1.10.2.16. Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;

4.1.10.2.17. Deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões;

4.1.10.2.18. Deve permitir a customização dos timers para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecido;

4.1.10.2.19. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, Facebook, etc), impactando no bom uso das aplicações de negócio, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de shaping. Dentre as tratativas possíveis, a solução deve suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem, endereço de destino, usuário e grupo de usuários, aplicações e porta;

4.1.10.2.20. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;

4.1.10.2.21. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como Youtube, Facebook etc;

4.1.10.2.22. Deve ainda possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda;

4.1.10.2.23. O QoS deve possibilitar a definição de fila de prioridade;

4.1.10.2.24. Além de possibilitar a definição de banda máxima e garantida por aplicação, o QoS deve também suportar o match em categorias de URL, IPs de origem e destino, logins e portas;

4.1.10.2.25. A capacidade de agendar intervalos de tempo onde as políticas de shaping/QoS serão válidas é mandatória. Ex: regra de controle de banda mais permissivas durante o horário de almoço;

4.1.10.2.26. O QoS deve possibilitar a definição de bandas distintas para download e upload;

4.1.10.2.27. A solução de SD-WAN deve prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do health check (packet loss, jitter e latência);

4.1.10.2.28. A solução de SD-WAN deve suportar IPv6;

4.1.10.2.29. Deve possibilitar roteamento distinto a depender do grupo de usuário selecionado na regra de SD-WAN;

4.1.10.2.30. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

4.1.10.2.31. OSD-WAN deverá possuir serviço de Firewall Stateful;

4.1.10.2.32. A solução SD-WAN deverá fornecer criptografia AES de 128 bits ou AES de 256 bits em sua VPN;

4.1.10.2.33. A solução SD-WAN deverá simplificar a implantação de túneis criptografados de site para site;

4.1.10.2.34. Deve ser capaz de bloquear acesso às aplicações;

4.1.10.2.35. Deve suportar NAT dinâmico bem como NAT de saída;

4.1.10.2.36. Deve suportar balanceamento de tráfego por sessão e pacote;

4.1.10.2.37. A solução SD-WAN deve prover capacidade de inspeção SSL para a inspeção de tráfego https nas filiais, no contexto de bloqueio de malwares e reconhecimento em camada 7 de aplicações;

4.1.10.2.38. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link principal recuperado seja X% (com X variando de 10 à 50) do seu valor de Saúde melhor que o link atual;

4.1.10.2.39. A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, em que X é configurável pelo administrador do sistema.

4.1.10.3. Políticas

4.1.10.3.1. Deverá suportar controles por zonas de segurança;

4.1.10.3.2. Deverá suportar controles de políticas por porta e protocolo;

4.1.10.3.3. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

4.1.10.3.4. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

4.1.10.3.5. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);

4.1.10.3.6. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);

4.1.10.3.7. Deve descriptografar tráfego outbound em conexões negociadas com TLS 1.2e TLS 1.3;

4.1.10.3.8. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

4.1.10.3.9. Suporte a objetos e regras IPV6;

4.1.10.3.10. Suporte a objetos e regras multicast;

4.1.10.3.11. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

4.1.10.4. Controle de Aplicações:

4.1.10.4.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

4.1.10.4.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

4.1.10.4.3. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

4.1.10.4.4. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

4.1.10.4.5. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

4.1.10.4.6. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;

4.1.10.4.7. Para tráfego criptografado SSL, deve descriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

4.1.10.4.8. Deve realizar decodificação de protocolos com o objetivo dedetectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação;

4.1.10.4.9. Identificar o uso de táticas evasivas via comunicações criptografadas;

4.1.10.4.10. Atualizar a base de assinaturas de aplicações automaticamente;

4.1.10.4.11. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory;

4.1.10.4.12. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

4.1.10.4.13. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

4.1.10.4.14. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

4.1.10.4.15. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

4.1.10.4.16. Deve alertar o usuário quando uma aplicação for bloqueada;

4.1.10.4.17. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle /políticas para os mesmos;

4.1.10.4.18. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

4.1.10.4.19. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts e bloquear a chamada de vídeo;

4.1.10.4.20. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle /políticas para os mesmos;

4.1.10.4.21. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);

4.1.10.4.22. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação e categoria da aplicação;

4.1.10.4.23. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação.

4.1.10.5. Prevenção de ameaças

4.1.10.4.1.10. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

4.1.10.4.1.11. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

4.1.10.5.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

4.1.10.5.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;

4.1.10.5.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

4.1.10.5.6. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

4.1.10.5.7. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

4.1.10.5.8. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

4.1.10.5.9. Deve permitir obloqueio de vulnerabilidades;

4.1.10.5.10. Deve permitir o bloqueio de exploits conhecidos;

4.1.10.5.11. Deve incluir proteção contra-ataques de negação de serviços;

4.1.10.5.12. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

4.1.10.5.13. Detectar e bloquear a origem de portscans;

4.1.10.5.14. Bloquear ataques efetuados por worms conhecidos;

4.1.10.5.15. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

4.1.10.5.16. Possuir assinaturas para bloqueio de ataques de buffer overflow;

4.1.10.5.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

4.1.10.5.18. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

4.1.10.5.19. Permitir o bloqueio devírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

4.1.10.5.20. Identificar e bloquear comunicação com botnets;

4.1.10.5.21. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

4.1.10.5.22. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

4.1.10.5.23. Os eventos devem identificar o país de onde partiu a ameaça;

4.1.10.5.24. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

4.1.10.5.25. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

4.1.10.5.26. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;

4.1.10.5.27. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;

4.1.10.5.28. Dentre as análises efetuadas, a solução deve suportar antivírus, query na nuvem, emulação de código, sandboxing e verificação de call-back;

4.1.10.5.29. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado;

4.1.10.6. Filtro de URLs

4.1.10.6.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

4.1.10.6.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

4.1.10.6.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

4.1.10.6.4. A identificação pela base do Active Directory deve permitir SSO, de forma que os usuários não precisem logar novamente na rede para navegar pelo firewall;

4.1.10.6.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

4.1.10.6.6. Possuir categorias de URLs previamente definidas pelo fabricante e atualizáveis a qualquer tempo;

4.1.10.6.7. Possuir pelo menos 70 categorias de URLs;

4.1.10.6.8. Deve possuir a função de exclusão de URLs do bloqueio;

4.1.10.6.9. Permitir a customização de página de bloqueio;

4.1.10.6.10. Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;

4.1.10.6.11. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;

4.1.10.7. Identificação de usuários

4.1.10.7.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;

4.1.10.7.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

4.1.10.7.3. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2016;

4.1.10.7.4. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;

4.1.10.7.5. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle /políticas baseadas em usuários e grupos de usuários;

4.1.10.7.6. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle /políticas baseadas em Usuários e Grupos de usuários;

4.1.10.7.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

4.1.10.7.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

4.1.10.7.9. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

4.1.10.7.10. A solução deve permitir que usuários que não possuam uma conta local ou em mídias sociais se autentiquem através de um rápido cadastro, que garanta o mínimo de rastreabilidade, através da validação de endereços de e-mail ou número de telefone;

4.1.10.7.11. A solução deve permitir o login automático de usuários visitantes depois de se registrarem com sucesso;

4.1.10.7.12. Deve suportar Security Assertion Markup Language (SAML), agindo como um Provedor de Identidade (Indentity Provider -IDP) estabelecendo um relacionamento de confiança para autenticação segura de usuários tentando acessar um Provedor de Serviços (Service Provider -SP);

4.1.10.8. Filtro de dados

4.1.10.8.1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);

4.1.10.8.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

4.1.10.8.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

4.1.10.8.4. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

4.1.10.9. Geolocalização

4.1.10.9.1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

4.1.10.9.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

4.1.10.10. VPN

4.1.10.10.1. Suportar VPN IPSec Site-to-Site;

4.1.10.10.2. A VPN IPSEC deve suportar criptografia 3DES, AES128, AES192 e AES256 (Advanced Encryption Standard);

4.1.10.10.3. A VPN IPSEc deve suportar Autenticação MD5, SHA1, SHA256, SHA384 e SHA512;

4.1.10.10.4. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2,Group 5 e Group 14, Group 15 até 21 e Group 27 até 32;

4.1.10.10.5. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

4.1.10.10.6. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI;

4.1.10.10.7. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

4.1.10.10.8. Deverá possuir suporte a VPN SSL;

4.1.10.10.9. Deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais;

4.1.10.10.10. A VPN SSL deverá possibilitar o acesso a toda infraestrutura, de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java;

4.1.10.10.11. A VPN SSL deverá suportar cliente para plataforma Windows, Linux e Mac OS X;

4.1.10.11. Equipamento *Fortinet* que atende especificações

Nesta seção apresentamos o equipamento do fabricante **Fortinet** que atende a configuração mínima detalhada nas subseções 4.1.10.1 a 4.1.10.10.

- Firewall de grande porte: **FG-600F + UTP (Unified Threat Protection) 5 anos**.

4.1.10.11.1. Soluções alternativas

Considerando que os equipamentos já adquiridos e atualmente em operação são do fabricante **Fortinet**, é essencial que os equipamentos adquiridos neste processo licitatório sejam do mesmo fabricante. Atém disso, do ponto de vista técnico, o equipamento de gerência centralizada e o analisador de logs atualmente em produção em nossa infraestrutura (FortiManager 200F, FortiAnalizer FAZ-800G) não é capaz de operar firewalls de outro fabricante. Por fim, este requisito também é necessário para compatibilidade e operação junto à solução para análise de tráfego.

Caso algum fornecedor queira ofertar produtos de outro fabricante, o mesmo deverá substituir, sem custo, a base atual da instituição, composta de 11 equipamentos FortiGates 101F (com licenciamento de software e hardware completo), 12 equipamentos FortiGate 40F (com licenciamento de software e hardware completo), 1 equipamento FortiGate 201E, 1 equipamento FortiManager 200F (com licenciamento de software e hardware completo) e 1 equipamento FortiAnalizer FAZ-800G (com licenciamento de software e hardware completo). Os modelos ofertados devem possuir capacidade igual ou superior aos equipamentos citados e serem todos do mesmo fabricante. Além disso, o fornecedor deverá ofertar, sem custo, treinamento oficial do fabricante com duração mínima de 80 horas para 13 pessoas da Divisão de Redes (DR) do CTIC, além da emissão de certificado de conclusão emitido pelo fabricante dos equipamentos para cada um.

4.1.11. Solução para rede sem fio (Wi-Fi)

4.1.11.1. Ponto de acesso sem fio interno (Indoor)

PONTO DE ACESSO INDOOR 802.11ax DUAL-BAND 4x4 5GHz e 2x2 2.4GHz

4.1.11.1.1. Especificações gerais

4.1.11.1.1.1. Deverá ser do mesmo fabricante do controlador WLAN para fins de compatibilidade.

4.1.11.1.1.2. Deverá possuir estrutura que permita a utilização do equipamento em locais internos, com fixação em teto e parede.

4.1.11.1.1.3. Deverá ser apresentado o certificado dentro do prazo de validade referente à homologação da Agência Nacional de Telecomunicações (ANATEL) para o produto, com data anterior à publicação do edital, conforme a resolução 242. Não serão aceitos protocolos de entrada ou outros documentos diferentes do certificado, uma vez que os mesmos não garantem o fornecimento de equipamentos homologados e em conformidade com as leis brasileiras.

4.1.11.1.1.4. Visando a plena compatibilidade do ponto de acesso com o padrão WiFi 6 e suas respectivas funcionalidades, a citar, de forma não-exaustiva, DL OFDMA, UL OFDMA, DL MU-MIMO e se faz necessário que o equipamento ofertado esteja listado como Wi-Fi CERTIFIED 6 no programa da WiFi Alliance na data do pregão.

4.1.11.1.1.5. Desejável possuir a certificação IEC 61373 ou IEC 60950

4.1.11.1.1.6. Deve ser compatível com o padrão UL 2043, o qual regula os componentes dos materiais com o intuito de proteger contra danos causados por fogo, bem como pela fumaça.

4.1.11.1.1.7. Suportar, no mínimo, 500 (quinhentos) usuários wireless simultâneos, sem nenhum tipo de licença adicional.

4.1.11.1.1.8. Possuir suporte a pelo menos 16 (dezesseis) SSIDs por ponto de acesso.

4.1.11.1.1.9. Possibilitar alimentação elétrica local via fonte de alimentação com seleção automática de tensão (100-240V) e via padrão PoE (IEEE 802.3at ou 802.3bt). Ademais, para PoE, a alimentação elétrica deve ocorrer através de uma única interface de rede, sem perda de funcionalidade e de desempenho.

4.1.11.1.1.10. Deve suportar temperatura de operação entre 0°C a 40°C.

4.1.11.1.1.11. O equipamento ofertado não deverá possuir antenas aparentes externas ao ponto de acesso, evitando desta forma que as mesmas sejam removidas, o que ocasionaria na degradação do desempenho da rede sem fio.

4.1.11.1.1.12. Deverá possuir 2 (duas) interfaces ethernet, sendo 1 (uma) 10/100/1000 Mbps e 1 (uma) 1/2.5 Gbps, utilizando conector RJ-45, para conexão à rede local.

4.1.11.1.1.13. Deverá possuir, no mínimo, um rádio embarcado para IoT, o qual deve ser compatível com BLE ou ZigBee.

4.1.11.1.1.14. Deverá dispor de uma porta USB para inserção de módulo IoT compatível com BLE e ZigBee.

4.1.11.1.1.15. Deverá possuir LEDs para a indicação do status da alimentação do ponto de acesso, status das interfaces e dos rádios de 2.4 GHz e 5 GHz.

4.1.11.1.1.16. Deverá ser fornecido com todas as funcionalidades de segurança, incluindo WIPS/WIDS, e Wi-Fi Mesh habilitadas, incluindo autocura via Mesh.

4.1.11.1.1.17. Deve ser compatível com IPv4, IPv6 e dual-stack.

4.1.11.1.1.18. Deve acompanhar suporte e garantia do fabricante por um período de no mínimo 05 (cinco) anos

4.1.11.1.2. Características dos rádios

4.1.11.1.2.1. O ponto de acesso deverá atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax, com operação nas frequências de 2.4 GHz e 5 GHz de forma simultânea.

4.1.11.1.2.2. Implementar as seguintes taxas de transmissão com fallback automático: IEEE 802.11b: 1 Mbps a 11 Mbps, IEEE 802.11a e IEEE 802.11g: 6 Mbps a 54 Mbps, IEEE 802.11n: 6.5 Mbps a 600 Mbps, IEEE 802.11ac: 6.5 Mbps a 1732 Mbps e IEEE 802.11ax: 4 Mbps a 2400 Mbps.

4.1.11.1.2.3. Deverá possuir antenas internas e integradas com padrão de irradiação omnidirecional compatíveis com as frequências de rádio dos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax, com ganhos de, no mínimo, 2 dBi para 2.4GHz e 2 dBi para 5GHz.

4.1.11.1.2.4. Deverá suportar potência agregada de saída, considerando todas as cadeias MIMO, de, no mínimo, 24 dBm na frequência de 5 GHz e 21 dBm na frequência de 2.4 GHz.

4.1.11.1.2.5. Deverá suportar canalização de 20 MHz, 40 MHz, 80 MHz e 160 MHz.

4.1.11.1.2.6. Deverá possuir mecanismo de rádio com suporte a 6 (seis) fluxos espaciais, sendo 4x4:4 em 5 GHz e 2x2:2 em 2.4 GHz para MU-MIMO e/ou SU-MIMO.

4.1.11.1.2.7. Deve possuir sensibilidade mínima de recepção de -90dBm considerando MCS0 HE20 (802.11ax) em 5GHz e -90 dBm considerando MCS0 HE20 (802.11ax) em 2.4GHz.

4.1.11.1.2.8. Deve permitir ajustes dinâmicos do sinal de rádio frequência para otimizar o tamanho da célula de abrangência do ponto de acesso.

4.1.11.1.2.9. Deve possuir capacidade de selecionar automaticamente o canal de transmissão.

4.1.11.1.2.10. Deve suportar os padrões IEEE 802.11r, IEEE 802.11k e IEEE 802.11v.

4.1.11.1.3. Serviços, segurança e gerenciamento

4.1.11.1.3.1. Deve permitir controle e gerenciamento pelo controlador WLAN através de Camada 2 ou 3 do modelo OSI.

4.1.11.1.3.2. Deve ser capaz de operar no modo Mesh sem adição de novo hardware ou alteração do sistema operacional, sendo que a comunicação até o controlador pode ser feita via wireless ou pela rede local.

4.1.11.1.3.3. Deve suportar autocura por meio de Mesh em caso de falha da conexão cabeada de dados, bem como permitir que os pontos de acesso gerenciados estabeleçam automaticamente uma rede mesh sem fio.

4.1.11.1.3.4. Em caso de falha de comunicação entre os pontos de acesso e o controlador WLAN, os usuários associados à rede sem fio devem continuar conectados com acesso à rede. Além disso, deve ser possível que novos usuários se associem à rede sem fio utilizando autenticação do tipo IEEE 802.1x mesmo que os pontos de acesso estejam sem comunicação com a controladora.

4.1.11.1.3.5. Deve suportar, somente por meio do ponto de acesso em conjunto com o controlador de rede sem fio, a identificação e controle de aplicações dos dispositivos clientes conectados ao ponto de acesso, levando em consideração a camada 7 do modelo OSI.

4.1.11.1.3.6. Deve suportar a configuração de limite de banda por usuário ou por SSID.

4.1.11.1.3.7. Deve oferecer suporte a mecanismo de localização e rastreamento de usuários (Location Based Services).

4.1.11.1.3.8. Implementar cliente DHCP, para configuração automática de seu endereço IP e implementar também suporte a endereçamento IP estático.

4.1.11.1.3.9. Deve suportar VLANs conforme o padrão IEEE 802.1Q.

4.1.11.1.3.10. Deve suportar atribuição dinâmica de VLAN por usuário.

4.1.11.1.3.11. Deve implementar balanceamento de usuários por ponto de acesso.

4.1.11.1.3.12. Deve suportar mecanismo que identifique e associe clientes preferencialmente na banda de 5GHz, deixando a banda de 2.4 GHz livre para dispositivos que trabalhem somente nesta frequência.

4.1.11.1.3.13. Deve implementar mecanismo para otimização de roaming entre pontos de acesso.

4.1.11.1.3.14. Deve suportar HotSpot 2.0, Captive Portal e WISPr.

4.1.11.1.3.15. Implementar, pelo menos, os seguintes padrões de segurança wireless: (WPA) Wi-Fi Protected Access, (WPA2) Wi-Fi Protected Access 2, (WPA3) Wi-Fi Protected Access 3, (AES) Advanced Encryption Standard, (TKIP) Temporal Key Integrity Protocol, IEEE 802.1X e IEEE 802.11i.

4.1.11.1.3.16. Deverá permitir a criação de filtros de endereços MAC de forma a restringir o acesso à rede sem fio.

4.1.11.1.3.17. Deverá permitir a criação de listas de controle de acesso de Camada 3 e 4 do modelo OSI.

4.1.11.1.3.18. Deverá ser possível criar políticas de controle com base no tipo ou sistema operacional do dispositivo.

4.1.11.1.3.19. Deve permitir habilitar e desabilitar a divulgação do SSID.

4.1.11.1.3.20. Deverá implementar autenticação de usuários usando portal de captura;

4.1.11.1.3.21. Deve implementar autenticação de usuários usando WISPr e Hotspot 2.0.

4.1.11.1.3.22. Deverá suportar funções para análise de espectro.

4.1.11.1.3.23. Deve disponibilizar uma página local acessível pelo cliente conectado ao ponto de acesso para visualização de estatísticas de conexão e informações do respectivo ponto de acesso.

4.1.11.1.3.24. Deve suportar conversão de tráfego multicast para unicast.

4.1.11.1.3.25. Permitir a configuração e gerenciamento direto através de navegador padrão (HTTPS), SSH, SNMPv2c, SNMPv3 ou através do controlador, a fim de se garantir a segurança dos dados.

4.1.11.1.3.26. Permitir que sua configuração seja realizada automaticamente quando este for conectado ao controlador WLAN do mesmo fabricante.

4.1.11.1.3.27. Implementar funcionamento em modo gerenciado por controlador WLAN, para configuração de seus parâmetros wireless, das políticas de segurança, QoS, autenticação e monitoramento de RF.

4.1.11.1.3.28. Permitir que o processo de atualização de software seja realizado manualmente através de interface Web, FTP ou TFTP e automaticamente através de controlador WLAN do mesmo fabricante.

4.1.11.1.4. Licença de ponto de acesso para controlador

4.1.11.1.4.1. Deve adicionar licença de uso de ponto de acesso gerenciado no Item Controlador de Rede Virtual ou físico.

4.1.11.1.4.2. Deve permitir licenciamento em pacotes, de, no mínimo 10 unidades, permitindo a este órgão adquirir o quantitativo que desejar, respeitando o limite suportado pelo equipamento Controlador de Rede Virtual ou Físico.

4.1.11.1.4.3. Deve ser obrigatoriamente do mesmo fabricante dos pontos de acesso e controlador.

4.1.11.1.4.4. Deve atender na íntegra os requisitos especificados no item Controlador de Rede Virtual ou Físico.

4.1.11.1.4.5. Deve acompanhar suporte do fabricante por um período de 05 (cinco) anos, porém, mesmo após este prazo, todas as funcionalidades devem permanecer ativas, sem prejuízos ou interrupções no funcionamento da rede Wi-Fi em operação.

4.1.11.2. Ponto de acesso sem fio externo (Outdoor)

PONTO DE ACESSO 802.11ax DUAL-BAND OUTDOOR

4.1.11.2.1. Especificações Gerais

4.1.11.2.1.1. Equipamento de ponto de acesso para rede local sem fio deverá atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax com operação nas frequências de 2.4 GHz e 5 GHz de forma simultânea

4.1.11.2.1.2. Deverá ser do mesmo fabricante do Controlador WLAN

4.1.11.2.1.3. Deverá ser apresentado o certificado dentro do prazo de validade referente à homologação da Agência Nacional de Telecomunicações (ANATEL) para o produto, com data anterior à publicação do edital, conforme a resolução 242. Não serão aceitos protocolos de entrada ou outros documentos diferentes do certificado, uma vez que os mesmos não garantem o fornecimento de equipamentos homologados e em conformidade com as leis brasileira

4.1.11.2.1.4. Possuir antenas internas e integradas, compatíveis com as frequências de rádio dos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax.

4.1.11.2.1.5. Não serão aceitos equipamentos com antenas aparentes (externas ao ponto de acesso) que sejam rosqueáveis, permitindo a remoção das antenas

4.1.11.2.1.6. Deve suportar potência de saída de no mínimo 22 dBm com operação na frequência 5GHz e de no mínimo 22 dBm com operação na frequência 2.4GHz

4.1.11.2.1.7. Deve suportar ganho de antena de no mínimo 2 dBi para 2.4GHz e 3dBi para 5GHz

4.1.11.2.1.8. Deve atender aos padrões IEEE 802.11h, sendo desejável atender aos padrões IEEE 802.11d

4.1.11.2.1.9. Deverá suportar canalização de 20 MHz, 40 MHz e 80MHz

4.1.11.2.1.10. Deverá possuir mecanismo de rádio com suporte à MIMO 2x2 com 2 Spatial Streams

4.1.11.2.1.11. Deverá suportar Multi User MIMO (MU-MIMO)

4.1.11.2.1.12. Deverá, em conjunto com o controlador de rede sem fio, permitir a análise de espectro do ambiente em modo dedicado ou simultâneo ao fornecimento de serviço aos dispositivos clientes.

4.1.11.2.1.13. Deverá suportar meio de direcionamento de sinal para ganho de desempenho

4.1.11.2.1.14. Deve suportar mecanismo que identifique e associe clientes preferencialmente na banda de 5GHz, deixando a banda de 2,4 GHz livre para dispositivos que trabalhem somente nesta frequência.

4.1.11.2.1.15. Deve suportar, em conjunto com o controlador de rede sem fio, a identificação e controle de aplicações dos dispositivos clientes conectados ao ponto de acesso.

4.1.11.2.1.16. Deve suportar, em conjunto com o controlador de rede sem fio, a configuração de limite de banda (rate limit) por usuário e por SSID.

4.1.11.2.1.17. Deve oferecer suporte ao mecanismo de localização e rastreamento de usuários (Location Based Service)

4.1.11.2.1.18. Deverá possuir, no mínimo, 01 (uma) interface IEEE 802.3 10/100/1000 Mbps Base-T Ethernet, auto-sensing, com conector RJ-45, para conexão à rede local fixa.

4.1.11.2.1.19. É desejável possuir LEDs para a indicação do status: portas ethernets, rede wireless e atividades do equipamento

4.1.11.2.1.20. Deverá possuir o padrão de alimentação IEEE 802.3af (PoE) ou IEEE 802.3at (PoE).

4.1.11.2.1.21. Deve suportar temperatura de operação entre -20°C a mínimo de 60°C com PoE ativado

4.1.11.2.1.22. Deverá possuir certificação IP67

4.1.11.2.1.23. Deverá possuir estrutura que permita a utilização do equipamento em locais internos e externos, com fixação em teto, parede e também em poste e fornecer acessórios para que possa ser feita a fixação

4.1.11.2.1.24. Deverá ser fornecido com todas as funcionalidades de segurança instaladas. Não deve haver licença restringindo itens de segurança do equipamento e nem a quantidade de usuários conectados

4.1.11.2.1.25. Funcionar via configuração do controlador no modo de MESH (WiFi Mesh) sem adição de novo hardware ou alteração do sistema operacional, sendo a comunicação até o controlador efetuada via wireless ou por pelo menos 02 pontos ethernet conectados ao controlador ou a uma rede local

4.1.11.2.1.26. Deverá ser fornecido com todas as licenças para funcionamento em MESH (WiFi Mesh)

4.1.11.2.1.27. Deve acompanhar suporte e garantia do fabricante por um período de no mínimo 05 (cinco) anos

4.1.11.2.2. Gerenciamento

4.1.11.2.2.1. Permitir a configuração e gerenciamento direto através de browser padrão (HTTPS), SSH, SNMPv2c e SNMPv3, ou através do controlador, a fim de garantir a segurança dos dados

4.1.11.2.2.2. Permitir gerenciamento através de plataformas de software que sigam padrões SNMPv2c e SNMPv3

4.1.11.2.2.3. Implementar funcionamento em modo gerenciado por controlador WLAN, para configuração de seus parâmetros wireless, das políticas de segurança, QoS, autenticação e monitoramento de RF

4.1.11.2.2.4. Permitir que sua configuração seja automaticamente realizada quando este for conectado no ambiente de rede do Controlador WLAN.

4.1.11.2.2.5. O ponto de acesso poderá estar diretamente ou remotamente conectado ao controlador WLAN, inclusive via roteamento da camada 3 de rede OSI

4.1.11.2.2.6. O ponto de acesso deverá conectar-se ao controlador WLAN através de túnel seguro padrão ou através de protocolo de comunicação seguro que ofereça controle total do equipamento

4.1.11.2.2.7. Permitir ajustes dinâmicos de RF modo a otimizar o tamanho da célula de abrangência de RF

4.1.11.2.2.8. Permitir que o processo de atualização de versão seja realizado manualmente através da WEB ou FTP ou TFTP e automaticamente através do Controlador WLAN descrito neste documento

4.1.11.2.3. Rede

4.1.11.2.3.1. Implementar cliente DHCP, para configuração automática do seu endereço IP e implementar também endereçamento IP estático

4.1.11.2.3.2. Deve suportar VLAN seguindo a norma IEEE 802.1q

4.1.11.2.3.3. Possuir suporte a pelo menos 16 SSIDs por ponto de acesso

4.1.11.2.3.4. Permitir habilitar e desabilitar a divulgação do SSID

4.1.11.2.3.5. Possuir capacidade de selecionar automaticamente o canal de transmissão

4.1.11.2.3.6. Suportar, no mínimo, 300 (trezentos) usuários wireless simultâneos

4.1.11.2.3.7. Deve suportar limitação de banda por grupo de usuário ou SSID

4.1.11.2.3.8. Implementar, pelo menos, os seguintes padrões de segurança wireless:

4.1.11.2.3.8.1. (WPA) Wi-Fi Protected Access

4.1.11.2.3.8.2. (WPA2) Wi-Fi Protected Access 2

4.1.11.2.3.8.3. (WPA3) Wi-Fi Protected Access 3

4.1.11.2.3.8.4. (AES) Advanced Encryption Standard

4.1.11.2.3.8.5. (TKIP) Temporal Key Integrity Protocol

4.1.11.2.3.8.6. IEEE 802.1x

4.1.11.2.3.8.7. IEEE 802.11i

4.1.11.2.3.9. Implementar as seguintes taxas de transmissão e com fallback automático:

4.1.11.2.3.9.1. IEEE 802.11b: 11 Mbps

4.1.11.2.3.9.2. IEEE 802.11a e IEEE 802.11g: 54 Mbps

4.1.11.2.3.9.3. IEEE 802.11n: 300Mbps

4.1.11.2.3.9.4. IEEE 802.11ac: 867Mbps

4.1.11.2.3.9.5. IEEE 802.11ax: 1200Mbps

4.1.11.2.3.10. Deverá permitir a criação de filtros de MAC address de forma a restringir o acesso à rede wireless

4.1.11.2.4. Licença de ponto de acesso para controlador

4.1.11.2.4.1. Deve adicionar licença de uso de ponto de acesso gerenciado no Item Controlador de Rede Virtual ou físico.

4.1.11.2.4.2. Deve permitir licenciamento em pacotes, de no mínimo 10 unidades, permitindo a este órgão adquirir o quantitativo que desejar, respeitando o limite suportado pelo equipamento Controlador de Rede Virtual ou Físico.

4.1.11.2.4.3. Deve ser obrigatoriamente do mesmo fabricante dos pontos de acesso e controlador.

4.1.11.2.4.4. Deve atender na íntegra os requisitos especificados no item Controlador de Rede Virtual ou Físico.

4.1.11.2.4.5. Deve acompanhar suporte do fabricante por um período de 05 (cinco) anos, porém, mesmo após este prazo, todas as funcionalidades devem permanecer ativas, sem prejuízos ou interrupções no funcionamento da rede Wi-Fi em operação.

4.1.11.3. Controladora

4.1.11.3.1. Especificações gerais

4.1.11.3.1.1. O controlador WLAN deverá ser preferencialmente do tipo virtual e compatível com os ambientes VMWare 6.7 e superiores, Hyper-V Windows 2019, KVM CentOS 7.5 e superiores, AWS, MS Azure ou GCE. O ambiente virtualizado deverá ser disponibilizado em servidor ou servidores da CONTRATANTE com as especificações recomendadas pelo fabricante da solução; Caso seja controlador físico, deverá ser um appliance dedicado, e deve atender a todas as especificações técnicas descritas a seguir.

4.1.11.3.1.2. Não serão aceitas soluções baseadas nas premissas de computação em nuvem ou pontos de acesso autônomos. Todas as funcionalidades exigidas deverão ser fornecidas por componentes físicos ou virtualizados do mesmo fabricante, dedicados para a solução de WLAN, instalados nas dependências da Contratante na modalidade perpétua.

4.1.11.3.1.3. Não serão aceitos sistemas implementados em virtualizadores de desktop, tais como Oracle VM VirtualBox ou VMware Workspace;

4.1.11.3.1.4. Se a solução for baseada em Hardware Appliance deve possuir no mínimo 2 (duas) portas 40Gbps QSFP+ e 8 (oito) portas 10Gbps SFP+. Essas portas devem operar simultaneamente e não devem ser do tipo combo.

4.1.11.3.1.5. Se a solução for baseada em Hardware Appliance deve possuir fontes redundantes 100-240vac, hot swappable.

4.1.11.3.1.6. Deverá ser do mesmo fabricante dos pontos de acesso fornecidos pela CONTRATADA, para fins de compatibilidade e gerenciamento;

4.1.11.3.1.7. Deverá suportar operação como um cluster (N+1) para prover resiliência e desempenho, podendo o mesmo ser composto por, no mínimo, 2 (dois) controladores;

4.1.11.3.1.8. Deve vir acompanhado de todos os acessórios necessários para operacionalização da solução, tais como softwares, documentações técnicas e manuais que contenham informações suficientes, que possibilitem a instalação, configuração e operacionalização da solução;

4.1.11.3.1.9. Deve permitir gestão centralizada, mas com acesso independente e isolado para cada domínio ou site por meio de grupos de Access Points com SSIDs e permissões dedicadas para cada administrador, sendo desejável o suporte a multi-tenant.

4.1.11.3.1.10. Deverá suportar pontos de acesso internos e externos nos padrões 802.11a/b/g/n/ac/ax;

4.1.11.3.1.11. Deverá possuir suporte a RESTful API compatível com JSON e disponibilizar suporte às funções GET, POST, DELETE, PUT e PATCH;

4.1.11.3.1.12. Deve acompanhar suporte e garantia do fabricante por um período de 05 (cinco) anos porém, mesmo após o encerramento deste prazo, todas as funcionalidades da controladora devem permanecer ativas, sem prejuízos ou interrupções no funcionamento do gerenciamento da rede wi-fi em operação

4.1.11.3.2. Gerenciamento

4.1.11.3.2.1. Capacidade para gerenciar, no mínimo, 600 Pontos de Acesso, podendo chegar através de adição de licenças de software a até 4000 Pontos de Acesso simultâneos por controlador;

4.1.11.3.2.2. Suportar, no mínimo, 100.000 dispositivos simultâneos por controlador;

4.1.11.3.2.3. Prover o gerenciamento centralizado dos Pontos de Acesso, suportando versões de firmware diferentes;

4.1.11.3.2.4. Deverá permitir gerenciamento através de Endereço IP, Range de IPs e Sub-Redes pré-configuradas;

4.1.11.3.2.5. Permitir a configuração total dos pontos de acesso, assim como os aspectos de segurança da rede wireless (WLAN) e Rádio Frequência (RF);

4.1.11.3.2.6. O controlador WLAN poderá estar diretamente e/ou remotamente conectado aos Pontos de Acesso por ele gerenciados, inclusive via roteamento em camada 3 do modelo OSI;

4.1.11.3.2.7. Possibilitar a configuração de envio dos eventos do Controlador WLAN para um servidor de Syslog remoto;

4.1.11.3.2.8. Implementar, pelo menos, os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps SNMP;

4.1.11.3.2.9. Permitir a visualização de alertas da rede em tempo real;

4.1.11.3.2.10. Implementar, no mínimo, 3 (três) níveis de acesso administrativo ao equipamento (apenas leitura, leitura/escrita e administrador da senha de visitante) protegidos por senhas independentes;

4.1.11.3.2.11. Permitir a customização do acesso administrativo através de atribuição de grupo de função do usuário administrador;

4.1.11.3.2.12. Permitir a configuração de servidores AAA para autenticação dos usuários administrativos;

4.1.11.3.2.13. Permitir a configuração e gerenciamento através de navegador padrão por meio de HTTPS;

4.1.11.3.2.14. Gerenciar de forma centralizada a autenticação de usuários administradores e clientes da rede sem fio;

4.1.11.3.2.15. Permitir o envio de alertas ou alarmes através do protocolo SMTP, sendo que a comunicação com o servidor deverá ser autenticada e cifrada (SMTP/TLS);

4.1.11.3.2.16. Permitir que o processo de atualização de versão seja realizado através de navegador padrão (HTTPS) ou SSH;

4.1.11.3.2.17. Permitir o agendamento da atualização de firmware dos pontos de acesso gerenciais por zona ou por grupo;

4.1.11.3.2.18. Deverá possuir a capacidade de importação de certificados digitais emitidos por uma autoridade certificadora externa.;

4.1.11.3.2.19. A disponibilidade da rede sem fio deve ser passível de agendamento para, no mínimo, as opções a seguir:

4.1.11.3.2.19.1. 24 horas por dia, 7 dias na semana;

4.1.11.3.2.19.2. Agendamento customizado permitindo escolher os dias da semana e horários;

4.1.11.3.2.20. Possuir ferramentas de diagnóstico e log de eventos para depuração e gerenciamento em primeiro nível;

4.1.11.3.2.21. Possuir ferramenta que permite o monitoramento em tempo real de informações de utilização de CPU, memória e estatísticas de rede;

4.1.11.3.2.22. Possibilitar cópia “backup” da configuração, bem como a funcionalidade de restauração da configuração através de navegador padrão (HTTPS) ou FTP ou TFTP;

4.1.11.3.2.23. Possuir a capacidade de armazenar múltiplos arquivos de configuração do controlador pertencente à rede sem fio;

4.1.11.3.2.24. Monitorar o desempenho da rede sem fio, permitindo a visualização de informações gerais e de cada ponto de acesso;

4.1.11.3.2.25. Suportar cluster de controladores WLAN no modo ativo/ativo ou ativo/standby, com sincronismo automático das configurações entre controladores para suporte a redundância em alta disponibilidade (HA - high availability);

4.1.11.3.2.24.1.10. Deverá suportar compartilhamento de recursos e licenças de pontos de acesso entre os controladores participantes do cluster;

4.1.11.3.2.24.1.11. Deverá, em caso de falha, suportar a redundância de forma automática e sem nenhuma necessidade de intervenção do administrador de rede;

4.1.11.3.2.26. Deverá possuir a capacidade de geração de informações ou relatórios de, no mínimo, os seguintes tipos: Listagem de clientes Wireless, Listagem de Pontos de Acesso, utilização da rede;

4.1.11.3.2.27. Deverá suportar, somente por meio do controlador e do ponto de acesso, a identificação de aplicações dos dispositivos clientes conectados aos pontos de acesso com base na camada 7 do modelo OSI, permitindo o controle de acesso, de banda (uplink e/ou downlink) e definição de regra de QoS para estas aplicações;

4.1.11.3.2.27.1. Deve permitir a atualização do pacote de assinaturas para identificação das aplicações utilizadas pelos dispositivos clientes conectados aos pontos de acesso durante todo o período de garantia;

4.1.11.3.2.28. Deve ser possível especificar regras de usuários baseadas em tempo, permitindo determinar em quais dias e horários a regra estará ativa, ou seja, deve ser possível escolher das 08:00 às 18:00, por exemplo;

4.1.11.3.2.29. Permitir visualizar a localização dos pontos de acesso e através desta obter o seu estado de funcionamento;

4.1.11.3.2.30. Deverá possibilitar a importação de plantas baixas nos formatos dwg ou jpg ou png, devendo permitir a visualização dos Pontos de Acesso instalados com seu estado de funcionamento, bem como disponibilizar uma visualização da cobertura do sinal em 2.4GHz ou 5GHz;

4.1.11.3.2.31. Deve ser possível localizar o dispositivo cliente e o Access Points que está conectado

4.1.11.3.2.32. Implementar funcionalidade de análise espectral em tempo real e por frequência, 2.4GHz ou 5GHz permitindo a detecção de interferências e geração de gráficos de uso do ambiente de rede sem fio;

4.1.11.3.2.33. Implementar análise de tráfego por WLAN, Ponto de acesso e dispositivos cliente, apresentando os 10 itens mais usados;

4.1.11.3.2.34. A solução deve suportar a adição de um serviço de SMS externo;

4.1.11.3.2.35. Deve suportar integração com tags da Ekahau e / ou AeroScout/Stanley para Real-Time Location Service (RTLS);

4.1.11.3.3. Rede

4.1.11.3.3.1. Deverá implementar suporte aos protocolos IPv4 e IPv6;

4.1.11.3.3.2. Deverá suportar tagging de VLANs;

4.1.11.3.3.3. Implementar associação dinâmica de usuário a VLAN com base nos parâmetros da etapa de autenticação via IEEE 802.1X;

4.1.11.3.3.4. Suportar associação dinâmica de ACL e de QoS por usuário, com base nos parâmetros da etapa de autenticação;

4.1.11.3.3.5. Deverá suportar, no mínimo, 1024 (mil e vinte e quatro) SSIDs simultâneos;

4.1.11.3.3.6. Desejável possuir funcionalidade de balanceamento de carga entre VLANs e permitir que clientes sejam designados para diferentes VLANs dentro de um mesmo SSID, com suporte a até 50 VLANs por pool;

4.1.11.3.3.7. Em caso de falha de comunicação entre os pontos de acesso e a controladora, os usuários associados à rede sem fio devem continuar conectados e com acesso à rede. Também deve permitir que novos usuários se associem à rede sem fio utilizando autenticação do tipo 802.1X mesmo que os pontos de acesso estejam sem comunicação com a controladora;

4.1.11.3.3.8. Deve ser possível desabilitar o suporte ao padrão IEEE 802.11b visando aprimorar o desempenho da rede sem fio;

4.1.11.3.3.9. Deve suportar 802.11k, além de ser desejável suportar 802.11d

4.1.11.3.3.10. Deve suportar captura de pacotes por ponto de acesso para resolução de problemas, sendo possível definir a captura nos rádios de 2.4 GHz e 5 GHz, bem como na interface LAN. A operação de captura deve ser realizada via interface Web com a possibilidade de exportação do arquivo de captura para análise local em software específico para análise de pacotes;

4.1.11.3.3.11. Deve ser possível monitorar o processo de conexão de um dispositivo cliente em tempo real com a finalidade de identificar problemas de conectividade e determinar em qual estágio o problema aconteceu;

4.1.11.3.3.12. Deve ser possível estabelecer um limite para o nível de sinal visando permitir que o cliente se junte à rede sem fio, o qual deve ser estabelecido em dBm e variar entre -60dBm e -90dBm;

4.1.11.3.3.13. Deverá suportar de forma centralizada a configuração de agregação de portas (LACP) ethernet dos pontos de acesso que possuírem suporte a essa funcionalidade;

4.1.11.3.3.14. Deve suportar autoconfiguração e autocorreção para redes do tipo mesh;

4.1.11.3.4. Segurança

4.1.11.3.4.1. Os itens a seguir devem estar integrados a solução ofertada, não serão aceitos equipamentos externos a solução para seu atendimento. Caso sejam necessárias licenças ou softwares de controle, os mesmos devem ser fornecidos de forma que a solução esteja operacional e sem nenhuma restrição no ato de sua implementação (hardware e softwares necessários para implementação);

4.1.11.3.4.2. Implementar, pelo menos, os seguintes padrões de segurança wireless:

4.1.11.3.4.2.1. (WPA) Wi-Fi Protected Access;

4.1.11.3.4.2.2. (WPA2) Wi-Fi Protected Access 2;

4.1.11.3.4.2.3. (WPA3) Wi-Fi Protected Access 3;

4.1.11.3.4.2.4. (TKIP) Temporal Key Integrity Protocol;

4.1.11.3.4.2.5. (AES) Advanced Encryption Standard;

4.1.11.3.4.2.6. PSK (Pre-Shared Key) única por dispositivo cliente em um mesmo SSID;

4.1.11.3.4.2.7. IEEE 802.1X;

4.1.11.3.4.2.8. IEEE 802.11i;

4.1.11.3.4.2.9. IEEE 802.11w;

4.1.11.3.4.3. Implementar, pelo menos, os seguintes controles/filtros:

4.1.11.3.4.3.1. Baseado em endereço MAC e isolamento de cliente na camada 2 do modelo OSI;

4.1.11.3.4.3.2. Baseado em endereço IP;

4.1.11.3.4.3.3. Baseado em protocolo, tais como TCP, UDP, ICMP e IGMP;

4.1.11.3.4.3.4. Baseado em porta de origem e/ou destino;

4.1.11.3.4.4. Permitir a autenticação para acesso dos usuários conectados nas redes WLAN (Wireless) através:

4.1.11.3.4.4.1. Endereço MAC;

4.1.11.3.4.4.2. Autenticação Local;

4.1.11.3.4.4.3. Captive Portal;

4.1.11.3.4.4.4. Active Directory;

4.1.11.3.4.4.5. RADIUS;

4.1.11.3.4.4.6. IEEE 802.1X;

4.1.11.3.4.4.7. LDAP;

4.1.11.3.4.5. Deverá permitir a seleção/uso de servidor RADIUS específico com base no SSID;

4.1.11.3.4.6. Deverá suportar servidor de autenticação RADIUS redundante. Isto é na falha de comunicação com o servidor RADIUS principal, o sistema deverá buscar um servidor RADIUS secundário;

4.1.11.3.4.7. A solução deverá suportar a criação de uma zona de visitantes, que terá seu acesso controlado através de senha cadastrada internamente, sendo que esta deverá possuir a configuração de tempo pré-determinado de acesso à rede sem fio;

4.1.11.3.4.8. O controlador deverá permitir a criação de múltiplos usuários visitantes (guests) de uma única vez (em lote);

4.1.11.3.4.9. Deve ser possível definir o período de validade da senha de visitantes em quantidade de horas, dias e semanas;

4.1.11.3.4.10. Deve permitir que após o processo de autenticação de usuários visitantes (guests), os mesmos sejam redirecionados para uma página de navegação específica e configurável;

4.1.11.3.4.11. Deve permitir que múltiplos usuários visitantes (guests) compartilhem a mesma senha de acesso à rede;

4.1.11.3.4.12. Deverá dispor de opção para enviar a senha de usuários visitantes (guests) por e-mail ou por SMS;

4.1.11.3.4.13. Deverá permitir que um usuário visitante se cadastre automaticamente através de funcionalidade do tipo “self registration”;

4.1.11.3.4.14. Deve disponibilizar autenticação dos usuários por meio de Redes Sociais suportando, no mínimo, 4 (quatro) redes sociais diferentes dentro de uma mesma WLAN;

4.1.11.3.4.15. Deverá permitir o isolamento do tráfego unicast, multicast ou ambos entre usuários visitantes (guests) em uma mesma VLAN/Subrede, sendo possível adicionar exceções com base em endereços MAC e IP;

4.1.11.3.4.16. Deverá permitir o encaminhamento do tráfego de saída de usuários visitantes (guests) diretamente para a Internet, de forma totalmente separada do tráfego da rede corporativa através de VLAN definida na WLAN visitante;

4.1.11.3.4.17. Deverá ser possível permitir que o ponto de acesso filtre todo o tráfego IPv4 e IPv6 dos tipos multicast e broadcast dos clientes sem fio associados, com exceção de alguns tráfegos pertencentes a uma lista de exclusões, tais como ARP, DHCPv4 e DHCPv6, MLD, IGMP, IPv6 NS, IPv6 NA, IPv6 RS e todos os pacotes do tipo unicast;

4.1.11.3.4.18. Deverá ser possível especificar o tipo de serviço Bonjour que será permitido entre VLANs por meio de execução de gateway bonjour nos pontos de acesso;

4.1.11.3.4.19. Deve suportar mecanismo de acesso de acordo com o padrão Hotspot 2.0;

4.1.11.3.4.20. Deve implementar mecanismos de segurança e proteção da rede sem fio contemplando, no mínimo, os recursos abaixo:

4.1.11.3.4.20.1. SSID Spoofing – Detectar APs não pertencentes ao controlador propagando o mesmo SSID;

4.1.11.3.4.20.2. MAC Spoofing – Detectar APs que não pertencem ao controlador e que estejam propagando o mesmo MAC de um AP válido;

4.1.11.3.4.20.3. Rogue APs – Detectar APs não pertencentes ao controlador;

4.1.11.3.4.20.4. Same Network – Detectar APs não pertencentes ao controlador exibindo qualquer SSID pertencentes ao mesmo segmento de rede LAN.;

4.1.11.3.4.20.5. Ad Hoc – Possibilidade de detectar rede Ad Hoc como rogue AP;

4.1.11.3.4.20.6. Flood de Deauthentication – Detectar quando há um número excessivo de frames de desautenticação oriundos de um mesmo transmissor;

4.1.11.3.4.20.7. Flood de Disassociation – Detectar quando há um número excessivo de frames de desassociação oriundos de um mesmo transmissor;

4.1.11.3.4.21. Deve implementar varredura de rádio frequência para identificação de ataques e Pontos de Acesso intrusos não autorizados (rogue AP);

4.1.11.3.4.22. Deve fazer a varredura no canal de operação do Ponto de Acesso sem impacto na performance da rede WLAN;

4.1.11.3.4.23. Deve utilizar os Pontos de Acesso para fazer a monitoração do ambiente Wireless procurando por pontos de acesso do tipo rogue de forma automática;

4.1.11.3.4.24. Deve ser possível especificar um ponto de acesso ou grupo de pontos de acesso para atuarem somente com a função de monitoramento visando detectar ataques e analisar o ambiente de rádio frequência;

4.1.11.3.4.25. Deverá ser capaz de localizar Pontos de Acesso do tipo rogue com informações de, no mínimo:

4.1.11.3.4.25.1. Pontos de Acesso que detectam;

4.1.11.3.4.25.2. Tipo de Rogue;

4.1.11.3.4.25.3. Nome da Rede;

4.1.11.3.4.25.4. Nível de sinal de detecção;

4.1.11.3.5. Recursos de gerenciamento automático de rádio frequência (RF)

4.1.11.3.4.1.10. Na ocorrência de inoperância de um Ponto de Acesso, o controlador sem fio deverá ajustar automaticamente a potência dos Pontos de Acesso adjacentes, de modo a prover a cobertura da área não assistida;

4.1.11.3.4.1.11. Ajustar automaticamente a utilização de canais de modo a otimizar a cobertura de rede e mudar as condições de rádio frequência baseado em desempenho;

4.1.11.3.5.3. Detectar interferência e ajustar parâmetros de rádio frequência, evitando problemas de cobertura de RF de forma automática;

4.1.11.3.5.4. Implementar sistema automático de balanceamento de carga para associação de clientes entre Pontos de Acesso próximos para otimizar o desempenho;

4.1.11.3.5.5. Implementar funcionalidade de balanceamento de carga entre os rádios de um mesmo Ponto de Acesso;

4.1.11.3.5.6. Permitir que o serviço wireless seja desabilitado de determinado ponto de acesso. Também deve ser possível selecionar o serviço de qual rádio (banda) de determinado ponto de acesso deve ser desabilitado;

4.1.11.3.6. Recursos de convergência e multimídia

4.1.11.3.6.1. Deverá Suportar 802.11e;

4.1.11.3.6.2. Deverá possuir funcionalidade de configuração do limite de banda disponível por usuário ou através de SSID /BSSID;

4.1.11.3.6.3. Deverá permitir a configuração de prioridade de um determinado SSID sobre outros SSIDs existentes na controladora;

4.1.11.3.6.4. Deve suportar WiFi Calling;

4.1.11.3.7. Solução de análise e visibilidade da rede

4.1.11.3.7.1. A solução poderá ser baseada nas premissas de computação em nuvem ofertado como serviço pelo fabricante, devendo ser compatível com a plataforma de gerenciamento, e os pontos de acesso propostos nesse certame;

4.1.11.3.7.2. A solução deverá ser baseada em algoritmos de inteligência artificial e nos conceitos de machine learning (aprendizagem de máquina) ou analíticos de aprendizagem conforme histórico de uso da rede;

4.1.11.3.7.3. A solução deverá atuar em conjunto com as funcionalidades do controlador WLAN virtual ou físico desde que seja do mesmo fabricante dos controladores e pontos de acesso utilizados na solução;

4.1.11.3.7.4. Deve possuir interface gráfica para visualização das informações, dashboards e relatórios;

4.1.11.3.7.5. Deve permitir seu acesso e gerenciamento através de navegador web padrão (HTTPS);

4.1.11.3.7.6. Deve apresentar estatisticas de rede identificadas por pelo menos as seguintes categorias: conexão, desempenho e infraestrutura;

4.1.11.3.7.7. Para incidentes da categoria de conexão, deve identificar pelo menos problemas relacionados a:

4.1.11.3.7.7.1 Associação e autenticação;

4.1.11.3.7.7.2. Roaming;

4.1.11.3.7.7.3. DHCP;

4.1.11.3.7.7.4. EAP;

4.1.11.3.7.7.5. RADIUS;

4.1.11.3.7.7.6. Tempo para conectar, bem como correlacionar os incidentes com o tipo de rádio 2,4GHz ou 5GHz, fabricantes dos dispositivos clientes e SSID;

4.1.11.3.7.8. Para incidentes da categoria de desempenho, deve identificar pelo menos problemas relacionado a:

4.1.11.3.7.8.1. Cobertura devido a baixo nível de sinal (RSSI), bem como correlacionar a incidência com tipo de rádio 2,4 GHz ou 5GHz, tipo de S.O. dos dispositivos clientes, SSID, modelo e firmware de AP;

4.1.11.3.7.9. Para incidentes da categoria de infraestrutura, deve identificar pelo menos problemas relacionados a:

4.1.11.3.7.9.1. NTP;

4.1.11.3.7.9.2. PoE;

4.1.11.3.7.9.3. Incompatibilidade de vlan id;

4.1.11.3.7.9.4. Comunicação entre AP e controladora;

4.1.11.3.7.10. Para cada incidente identificado, a solução deve trazer as seguintes informações, que devem ser armazenadas na plataforma ofertada por pelo menos 3 (três) meses:

4.1.11.3.7.10.1. Possíveis causas raízes e ações recomendadas para a sua mitigação;

4.1.11.3.7.10.2. Quantidade e a porcentagem de clientes impactados, quando aplicável;

4.1.11.3.7.10.3. Quantidade e a porcentagem de APs impactados, quando aplicável;

4.1.11.3.7.10.4. Dia e horário que ocorreu a incidência e sua duração;

4.1.11.3.7.11. Deve identificar insuficiência de potência PoE para alimentar os dispositivos PDs;

4.1.11.3.7.12. Deve identificar se a solução de rede wi-fi atende aos parâmetros de SLA para pelo menos:

4.1.11.3.7.12.1. Conexões realizadas com sucesso;

4.1.11.3.7.12.2. Tempo para se conectar;

4.1.11.3.7.12.3. Desempenho dos clientes;

4.1.11.3.7.13. Deve permitir a comparação de informações de dois períodos de 24 horas cada e listar todas as alterações que foram realizadas na configuração da solução wi-fi entre esses dois períodos;

4.1.11.3.7.14. Deve permitir realizar o troubleshooting de um cliente mostrando todos os eventos do processo de conexão desse cliente (autenticação, associação, EAP, RADIUS, DHCP, client connect, client disconnect, client timeout, bem como roaming e qualidade da conexão;

4.1.11.3.7.15. Deve permitir que o AP faça o papel de um cliente para validar um serviço criado de ponta-a-ponta, como autenticação 802.11, associação, DHCP, DNS, Ping, traceroute, upload e download de tráfego;

4.1.11.3.7.16. Desejável realizar testes para avaliar a qualidade de uma vídeo-chamada, como calculos de métricas de delay, jitter e MOS

4.1.11.3.7.17. Deve implementar a visualização ou geração de relatórios dos seguintes tipos:

4.1.11.3.7.17.1. Informações e detalhes de clientes wireless;

4.1.11.3.7.17.2. Informações das WLAN;

4.1.11.3.7.17.3. Listagem e detalhes de APs e controladores;

4.1.11.3.7.17.4. Informação de “airtime utilization”

4.1.11.3.7.17.5. Listagem das principais aplicações em uso;

4.1.11.3.7.17.6. Informações e detalhes de switches;

4.1.11.3.7.18. Deve suportar a criação de relatórios customizados.

4.1.11.3.7.19. Deve possuir retenção de dados de pelo menos 12 (doze) meses para gerar relatórios;

4.1.11.3.7.20. Permitir que os relatórios sejam convertidos em arquivos pdf ou csv;

4.1.11.3.7.21. A solução ofertada deve suportar a capacidade de monitorar simultaneamente, no mínimo, 600 (seiscentos) pontos de acesso e 02 (dois) controladores de rede; caso sejam necessárias licenças ou assinatura de serviço para esse fim, essas licenças precisam ser ofertadas juntamente com as LICENÇAS DE PONTO DE ACESSO PARA CONTROLADOR.

4.1.11.3.7.22. Deverá ser possível expansão de ativos monitorados em incrementos de uma unidade, mediante adição de licença de uso de ponto de acesso monitorado;

4.1.11.3.7.23. A licença ou Serviço de Assinatura de Ponto de Acesso deve ter validade de no mínimo 5 (cinco) anos incluindo o suporte do fabricante.

4.1.11.4. Injetores de energia (Power injector)

4.1.11.4.1 Dispositivo Injetor PoE para alimentação de equipamentos com suporte a PoE;

4.1.11.4.2. O injetor PoE deverá ser fornecido pelo mesmo fabricante das controladoras e pontos de acesso. Não serão aceitos injetores genéricos ou fornecidos por outros fabricantes;

4.1.11.4.3. Deve possuir potência de até 24W (vinte e quatro watts);

4.1.11.4.4. Deve possuir 2 portas RJ-45 fêmea, uma para conectar ao switch não PoE e outra para fornecer energia e dados para o Ponto de Acesso. Ambas as portas devem operar em 10/100/1000 Mbps;

4.1.11.4.5. Deve acompanhar cabos e acessórios para o seu perfeito funcionamento;

4.1.11.4.6. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V ou 220V com comutação automática e frequência de 60Hz;

4.1.11.4.7. Deve possuir 5 (cinco) anos de garantia do fabricante.

Requisitos de Implantação

4.1.12. Os equipamentos deverão observar integralmente os requisitos de implantação, instalação e fornecimento descritos a seguir:

4.1.12.1. No caso dos firewalls, exceto na situação descrita no item **4.1.10.11.1**, a instalação será feita integralmente pela CONTRATANTE.

4.1.12.2. No caso da solução de rede sem fio, a instalação e configuração da controladora será realizada nas dependências da CONTRATANTE pela CONTRATADA, preferencialmente de modo presencial. A instalação dos pontos de acesso será realizada pela CONTRATANTE>

5. Modelo de execução do objeto

Rotinas de Execução

Do Encaminhamento Formal de Demandas

5.1 O gestor do contrato emitirá a Ordem de fornecimento de bens (OFB) para a entrega dos bens desejados.

5.1.1. A empresa terá 30 dias para entrega após a emissão da Ordem de Empenho.

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

5.3 O recebimento provisório e definitivo dos bens é disciplinado em tópico próprio deste TR.

Forma de execução e acompanhamento do contrato

Condições de Entrega

5.4 A previsão de entrega das parcelas são apresentadas a seguir**:**

Etapa	Data	Firewall de Grande Porte	Ponto de Acesso Indoor	Ponto de Acesso Outdoor	Controladora	Injetor PoE
1	até março/2024	2	-	-	-	-
2	até outubro/2024	2	100	50	2	50
3	até junho/2025	-	225	-	-	-
4	até dezembro/2025	-	225	-	-	-

5.5 Os bens deverão ser entregues no seguinte endereço: Av. Amazonas, nº 2210, bairro Umuarama, Uberlândia/MG, CEP 38405-302.

Garantia, manutenção e assistência técnica

5.6. O prazo de garantia contratual dos bens, complementar à garantia legal, será de, no mínimo, 60 (sessenta) meses, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

5.6.1. Mesmo após o encerramento deste prazo, todas as funcionalidades da controladora (Grupo 1, item 4) devem permanecer ativas, sem prejuízos ou interrupções no funcionamento do gerenciamento da rede sem fio em operação.

5.6.2. O contratado deve fornecer termo de garantia para os itens deste processo, com data de início e fim conforme prazos estabelecidos acima.

5.7 Caso o prazo da garantia oferecida pelo fabricante seja inferior ao estabelecido nesta cláusula, o fornecedor deverá complementar a garantia do bem ofertado pelo período restante.

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

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

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

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

5.12 Uma vez notificado, o Contratado realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo de até 2 (dois) dias úteis para o firewall de grande porte e controladora de ponto de acesso (caso não seja virtualizada) e até 10 (dez) dias úteis para pontos de acesso e injetores, contados a partir da data de retirada do equipamento das dependências da Administração pelo Contratado ou pela assistência técnica autorizada.

5.13 O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada do Contratado, aceita pelo Contratante.

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

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

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

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

PAPÉIS E RESPONSABILIDADES

5.18 São obrigações da CONTRATANTE:

5.18.1 nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

5.18.2 encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;

5.18.3 receber o objeto fornecido pelo Contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

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

5.18.5 liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

5.18.6 comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

5.18.7 definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do Contratado, com base em pesquisas de mercado, quando aplicável;

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

5.19 São obrigações do CONTRATADO:

5.19.1 indicar formalmente preposto apto a representá-la junto à Contratante, que deverá responder pela fiel execução do contrato;

5.19.2 atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

5.19.3 reparar quaisquer danos diretamente causados à Contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução do contrato pela Contratante;

5.19.4 propiciar todos os meios necessários à fiscalização do contrato pela Contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

5.19.5 manter, durante toda a execução do contrato, as mesmas condições da habilitação;

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

5.19.7 quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

5.19.8 ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração;

5.19.9 fazer a transição contratual, com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos do contratante ou da nova empresa que continuará a execução do contrato, quando for o caso;

5.19.10 A fim de obter comprometimento formal sobre o sigilo dos dados e informações de uso da contratante, bem como suas normas e políticas de segurança, a contratada deverá concordar e assinar, por meio de representante legal, o Termo de Compromisso de Manutenção de Sigilo, conforme modelo no **Anexo 1 do Termo de Referência**.

5.20 São obrigações do órgão gerenciador do registro de preços:

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

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

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

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

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

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

5.20.4.1 a definição da produtividade ou da capacidade mínima de fornecimento da solução de TIC;

5.20.4.2 as regras para gerenciamento da fila de fornecimento da solução de TIC aos órgãos participantes e não participantes, contendo prazos e formas de negociação e redistribuição da demanda, quando esta ultrapassar a produtividade definida ou a capacidade mínima de fornecimento e for requerida pelo Contratado; e

5.20.4.3 as regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a verificação de Amostra do Objeto, observado o disposto no inciso III, alínea "c", item 2 deste artigo, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica.

Mecanismos formais de comunicação

5.21 São definidos como mecanismos formais de Comunicação, entre a Contratante e o Contratado, os seguintes:

5.21.1 Ordem de Fornecimento de Bens;

5.21.2 Ata de Reunião;

5.21.3 Ofício;

5.21.4 Sistema de abertura de chamados;

5.21.5 E-mails e Cartas;

Formas de Pagamento

5.22 Os critérios de medição e pagamento serão tratados em tópico próprio do Modelo de Gestão do Contrato.

6. Modelo de gestão do contrato

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

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

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

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

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

6.6 A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em até 10(dez) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.

6.7 A pauta desta reunião observará, pelo menos:

6.7.1 Presença do representante legal da contratada, que apresentará o seu preposto;

6.7.2 Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;

6.7.3 Esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

6.7.4 A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à Contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

6.7.5 Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

Fiscalização

6.6. A execução do contrato deverá ser acompanhada e fiscalizada pelo fiscal do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput).

Fiscalização Técnica

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

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

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

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

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

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

Fiscalização Administrativa

6.8. O fiscal administrativo do contrato verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as multas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

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

Gestor do Contrato

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

6.10 O gestor do contrato acompanhará a manutenção das condições de habilitação do Contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.

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

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

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

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

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

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

Critérios de Aceitação

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

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

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

6.20 Todos os componentes internos dos equipamento(s) deverão estar instalados de forma organizada e livres de pressões ocasionados por outros componentes ou cabos, que possam causar desconexões, instabilidade, ou funcionamento inadequado.

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

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

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

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

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

6.26 Só haverá o recebimento definitivo, após a análise da qualidade dos bens e/ou serviços, em face da aplicação dos critérios de aceitação, resguardando-se ao Contratante o direito de não receber o OBJETO cuja qualidade seja comprovadamente baixa ou em desacordo com as especificações definidas neste Termo de Referência – situação em que poderão ser aplicadas à CONTRATADA as penalidades previstas em lei, neste Termo de Referência e no CONTRATO. Quando for o caso, a empresa será convocada a refazer todos os serviços rejeitados, sem custo adicional.

Níveis Mínimos de Serviço Exigidos

6.27 Os níveis mínimos de serviço são indicadores mensuráveis estabelecidos pelo Contratante para aferir objetivamente os resultados pretendidos com a contratação. São considerados para a presente contratação os seguintes indicadores:

IAE – INDICADOR DE ATRASO NO FORNECIMENTO DO EQUIPAMENTO	
Tópico	**Descrição**
Finalidade	Medir o tempo de atraso na entrega dos produtos e serviços constantes na Ordem de Fornecimento de Bens
Meta a cumprir	(IAE < = 0) A meta definida visa garantir a entrega dos produtos e serviços constantes nas Ordens de Fornecimento de Bens dentro do prazo previsto.
Instrumento de medição	OFB, Termo de Recebimento Provisório (TRP)
Forma de acompanhamento	A avaliação será feita conforme linha de base do cronograma registrada na OFB. Será subtraída a data de entrega dos produtos da OFB (desde que o fiscal técnico reconheça aquela data, com registro em Termo de Recebimento Provisório) pela data de início da execução da OFB.
Periodicidade	Para cada Ordem de Fornecimento de Bens encerrada e com Termo de Recebimento Definitivo.
Mecanismo de Cálculo (métrica)	IAE = TEX - TEST Onde: IAE – Indicador de Atraso de Entrega da OFB; TEX – Tempo de Execução – corresponde ao período de execução da OFB, da sua data de início até a data de entrega dos produtos da OFB. A data de início será aquela constante na OFB; caso não esteja explícita, será o primeiro dia útil após a emissão da OFB. A data de entrega da OFB deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes neste Termo de Referência. Para os casos em que o fiscal técnico rejeita a entrega,

	o prazo de execução da OFB continua a correr, findando-se apenas quanto o Contratado entrega os produtos da OFB e haja aceitação por parte do fiscal técnico. TEST – Tempo Estimado para a execução da OFB – constante na OFB, conforme estipulado no Termo de Referência.
Observações	Obs1: Serão utilizados dias corridos na medição. Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias corridos no cômputo do indicador.
Início de Vigência	A partir da emissão da OFB
Faixas de ajuste no pagamento e Sanções	Para valores do indicador IAE: Menor ou igual a 0 – Pagamento integral da OFB; De 1 a 60 - aplicar-se-á multa de 0,1666% por dia de atraso sobre o valor da OFB ou fração em atraso. Acima de 60 - aplicar-se-á multa de 10% bem como multa de 2% sobre o valor OFB ou fração em atraso.

Sanções Administrativas e Procedimentos para retenção ou multa no pagamento

6.28 Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela Contratante, conforme a tabela abaixo:

Id	Ocorrência	multa/Sanção
1	Não prestar os esclarecimentos imediatamente, referente à execução do contrato, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 4 (quatro) horas úteis.	Multa de 0,5% sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela Contratante, até o limite de 10 (dez) dias úteis. _____ Após o limite de 10 (dez) dias úteis, aplicar-se-á multa de 10% do valor total do Contrato.
2	Não atender ao indicador de nível de serviço IAE (Indicador de Atraso de Entrega de OS).	Para valores do indicador IAE de 1 a 60 - aplicar-se-á multa de 0,1666% por dia de atraso sobre o valor da OFB ou fração em atraso. _____ Para valores do indicador IAE acima de 60 - aplicar-se-á multa de 10% bem como multa de 2% sobre o valor OFB ou fração em atraso.
3	Recusa em assinar a Ata, o Contrato, ou retirar a Nota de Empenho, no prazo máximo de 5 (cinco) dias úteis, após a regular convocação.	Multa no percentual de 5% (cinco por cento), calculada sobre o valor total estimado do Contrato. Por valor total estimado do contrato entenda valor homologado ao fornecedor.
4	Deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não manter a proposta, falhar ou fraudar na execução do Contrato, comportar-se de modo inidôneo ou cometer fraude fiscal.	A Contratada ficará impedida de licitar e contratar com a União, pelo prazo de até 5 (cinco) anos, sem prejuízo das demais cominações legais, e multa de 5% do valor da contratação.
5	Demonstrar não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.	Suspensão temporária de 6 (seis) meses para licitar e contratar com a Administração, sem prejuízo da Rescisão Contratual.
6	Não executar total ou parcialmente o objeto da contratação.	Multa de até 3% sobre o valor total do Contrato.

7	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, o funcionamento ou funcionalidades do objeto da contratação, por prazo superior a 2 dias, sem comunicação formal ao gestor do Contrato.	Multa de até 3% sobre o valor total do Contrato.
8	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	Advertência. Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplicar-seámulta de 0,5% do valor total do Contrato.

7. Critérios de medição e pagamento

Recebimento

7.1. Os bens serão recebidos provisoriamente, de forma sumária, no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

7.2. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 10 (dez) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

7.3. O recebimento definitivo ocorrerá no prazo de 10(dez) dias úteis, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.

7.4 O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

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

7.6. O prazo para a solução, pelo contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

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

Liquidação

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

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

7.9.1. o prazo de validade;

7.9.2. a data da emissão;

7.9.3. os dados do contrato e do órgão contratante;

7.9.4. o período respectivo de execução do contrato;

7.9.5. o valor a pagar; e

7.9.6. eventual destaque do valor de retenções tributárias cabíveis.

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

7.11. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

7.12. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018).

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

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

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

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

Prazo de pagamento

7.17. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

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

Forma de pagamento

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

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

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

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

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

Cessão de crédito

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

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

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

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

7.26. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração. (INSTRUÇÃO NORMATIVA Nº 53, DE 8 DE JULHO DE 2020 e Anexos)

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

8. Critérios de seleção do fornecedor

Forma de seleção e critério de julgamento da proposta

8.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO por Grupo e por Item.

8.1.1. Justifica-se o agrupamento dos itens no Grupo 1 pelo fato de que os pontos de acesso sem fio e a controladora devem ser do mesmo fabricante, uma vez que a controladora deve ser capaz de gerenciar todos os pontos de acesso adquiridos neste processo. Os injetores PoE, por sua vez, devem ser do mesmo fabricante dos pontos de acesso para padronização de conectores e potência de alimentação.

Forma de fornecimento

8.2. O fornecimento do objeto será parcelado. Visando uma instalação escalonada, principalmente no sentido de interrupção mínima dos serviços e sistemas em operação e adequação das atividades à força de trabalho disponível no Centro de Tecnologia da Informação e Comunicação (CTIC), órgão responsável pela gerência de toda a infraestrutura de rede da Universidade, a aquisição dos equipamentos e sua instalação ocorrerá em quatro etapas, detalhadas no ETP.

Da Aplicação da Margem de Preferência

8.3 Não será aplicada margem de preferência na presente contratação.

Exigências de habilitação

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

Habilitação jurídica

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

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

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

8.8. **Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI**: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

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

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

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

8.12. Não serão aceitas sociedades cooperativas.

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

Habilitação fiscal, social e trabalhista

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

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

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

8.17. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

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

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

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

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

Qualificação Econômico-Financeira

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

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

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

8.26.1. índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);

8.26.2. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura.

8.26.3. Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos;

8.26.4. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.

8.27. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação patrimônio líquido mínimo de 10% (dez por cento) do valor total estimado da contratação

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

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

Qualificação Técnica

8.30 A exigência de Qualificação Técnica justifica-se pela criticidade dos itens contratados para o funcionamento da rede de dados da Universidade. Especificamente, a solução de firewall é crítica pra proteger a rede da UFU de tentativas de acesso indevido, extravio e sequestro de dados críticos, entre outros. No caso da solução de rede sem fio, a questão da segurança e do funcionamento adequado é fundamental, visto que a digitalização de diversos serviços (compra de tickets para restaurante universitário, realização de chamadas e lançamento de notas, registro de ponto de funcionários, etc.) criam uma dependência muito forte entre a rede sem fio e o dia-a-dia dos diversos campi. Por estas razões, deve-se garantir que as empresas contratadas possuam capacidade de responder em tempo adequado e conhecimento técnico para prestar o suporte necessário.

8.32. Para efeito de qualificação técnica, a LICITANTE deve demonstrar sua aptidão e capacidade técnico-operacional para a execução do OBJETO mediante comprovação de prestação bem-sucedida de fornecimento de bens e de serviços em características e quantidades compatíveis com a presente licitação, mediante apresentação de um ou mais ATESTADO(S) DE CAPACIDADE TÉCNICA que deverão comprovar o fornecimento de, no mínimo, 30% (trinta por cento) do volume estimado de equipamentos para o item em disputa e com características compatíveis com o objeto da presente pretensão contratual, podendo considerar contratos já executados e/ou em execução.

8.33. A comprovação de capacidade técnica será realizada para cada item/grupo, devendo a Licitante apresentar:

a) atestado(s) que se refiram a contratos já concluídos ou já decorrido no mínimo um ano do início de sua execução, exceto se houver sido firmado para ser executado em prazo inferior; ou

b) atestado(s) que se refiram a serviços prestados ou fornecimentos realizados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

8.34. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.

8.35. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor. Não serão aceitos atestados de empresas subcontratadas.

8.36. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.

8.37. Não será admitida subcontratação de outra empresa para fornecimento dos itens deste certame, nem prestação do suporte e /ou garantia, exceto do próprio fabricante, quando pertinente.

9. Estimativas do Valor da Contratação

Valor (R$): 7.209.126,48

9.1. O custo estimado total da contratação é de **R$7.209.126,48** (sete milhões, duzentos e nove mil, cento e vinte e seis reais e quarenta e oito centavos) conforme custos unitários descritos abaixo:

9.1.1 **Item 1:** Firewall de grande porte: R$2.531.378,32 (dois milhões, quinhentos e trinta e um mil, trezentos e setenta e oito reais e trinta e dois centavos);

9.1.2 **Grupo 1:** Solução de rede sem fio: R$4.677.748,16 (quatro milhões, seiscentos e setenta e sete mil, setecentos e quarenta e oito reais e dezesseis centavos).

9.2. A estimativa de custo levou em consideração o risco envolvido na contratação e sua alocação entre contratante e contratado, conforme especificado na matriz de risco constante do Contrato.

9.3. Em caso de licitação para Registro de Preços, os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, nas seguintes situações (art. 25 do Decreto nº 11.462/2023):

9.3.1. em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata tal como pactuada, nos termos do disposto na alínea “d” do inciso II do caput do art. 124 da Lei nº 14.133, de 2021;

9.3.2. em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;

9.3.3. serão reajustados os preços registrados, respeitada a contagem da anualidade e o índice previsto para a contratação; ou

9.3.4. poderão ser repactuados, a pedido do interessado, conforme critérios definidos para a contratação.

10. Adequação orçamentária

10.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União.

10.2. Em se tratando de contratação via Sistema de Registro de preços a dotação orçamentária será informada previamente à formalização do contrato ou de outro instrumento hábil, conforme estabelecido pelo art. 17 do Decreto nº 11.462, de 31 de março de 2023.

11. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

PAULO RODOLFO DA SILVA LEITE COELHO

Membro da comissão de contratação

Assinou eletronicamente em 05/02/2024 às 17:14:15.

AMANDA FILSNER DIAS STRACK

Membro da comissão de contratação

Assinou eletronicamente em 05/02/2024 às 17:17:01.

JOAO EURIPEDES PEREIRA JUNIOR

Membro da comissão de contratação

Assinou eletronicamente em 05/02/2024 às 17:22:08.