



HOSPITAL UNIVERSITÁRIO DA UNIVERSIDADE DE BRASÍLIA
SGAN, Quadra 605, L2 Norte - Bairro Asa Norte
Brasília-DF, CEP 70830-200
- <https://hub-unb.hubbrasil.gov.br>

Termo de Referência - TI - SEI

TERMO DE REFERÊNCIA

Referência: Arts. 12 a 24 IN SGD/ME Nº 94/2022

1. OBJETO DA CONTRATAÇÃO (IN 94/2022 SGD/ME - ART. 12, INCISO I)

1.1. O objeto desta licitação é a aquisição de Solução de Rede sem fio WLAN - Wi-Fi, com fornecimento de equipamentos, sistema de gerenciamento integrado, sistema de controle de acesso - NAC, serviço de instalação, configuração e treinamento, garantia e suporte técnico *on-site* por 60 meses para atender o HUB-UnB e serviço de *site survey*, conforme condições, quantidades e exigências estabelecidas neste Termo de Referência, seus encartes e anexos.

1.2. A licitação será composta pelos itens indicados neste tópico, divididos em Grupo 1 e Item Avulso conforme Tabela 1.

1.3. Cada serviço ou produto do item deverá estar discriminado em subitens, separados nas propostas de preços, de modo a permitir a identificação do seu preço individual na composição do preço global e a eventual incidência sobre cada item das margens de preferência para produtos e serviços que atendam às Normas Técnicas Brasileiras - NTB.

GRUPO	ITEM	DESCRIÇÃO	CATMAT/CATSER	QUANTIDADE
1	1	Solução de Controladora WI-FI	486317	01
	2	Solução de Gerência, Monitoramento e Controle de Acesso (NAC)	27464	01
	3	Ponto de Acesso (Access Point) indoor 802.11ax - TIPO 1	393277	445
	4	Ponto de Acesso (Access Point) indoor 802.11ax - TIPO 2	603936	15
	5	Injetor de Potência (Power Injector)	426731	300
	6	Instalação e configuração da solução	27111	01
	7	Treinamento e capacitação da solução	16837	01
Item Avulso	8	Site Survey	620	01

Tabela 1 - Descrição do Objeto.

2. DESCRIÇÃO DA SOLUÇÃO DE TIC (IN 94/2022 SGD/ME - ART. 12, INCISO III)

2.1. Descrição detalhada do objeto:

GRUPO	ITEM	DESCRIÇÃO	CATMAT/CATSER	UNIDADE	TOTAL
1	1	Solução de Controladora WI-FI	486317	Unid.	01
	2	Solução de Gerência, Monitoramento e Controle de Acesso (NAC)	27464	Unid.	01
	3	Ponto de Acesso (Access Point) indoor 802.11ax - TIPO 1	393277	Unid.	445
	4	Ponto de Acesso (Access Point) indoor 802.11ax - TIPO 2	603936	Unid.	15
	5	Injetor de Potência (Power Injector)	426731	Unid.	300
	6	Instalação e configuração da			

	6	solução	27111	Unid.	01
	7	Treinamento e capacitação da solução	16837	Unid.	01
Item Avulso	8	Site Survey	620	Unid.	01

Tabela 2 - Itens previstos para a Solução de Rede Wi-Fi.

2.2. Informa-se que a estimativa constante da Tabela 2, corresponde à quantidade mínima de produtos/serviços necessários para composição da solução, não se limitando a estes, sendo necessário o proponente especificar todos os subitens que compõem os itens, se for o caso, haja visto que uma Solução de Rede sem fio WLAN - Wi-Fi pode variar a depender do fabricante, sem que isso comprometa os requisitos mínimos estabelecidos neste Termo de Referência e não restrinja a competitividade.

3. BENS E SERVIÇOS QUE COMPÕEM A SOLUÇÃO

3.1. A solução de rede Wi-Fi pretendida, será composta por:

- I - Controladora (as) Wi-Fi.
- II - Sistema de Gerência integrado.
- III - Sistema de Monitoramento da Solução.
- IV - Sistema de Controle de Acesso (NAC).
- V - Ponto de Acesso (*Access Point*) indoor 802.11ax - TIPO 1 (moderado).
- VI - Ponto de Acesso (*Access Point*) indoor 802.11ax - TIPO 2 (robusto).
- VII - Injetor de Potência (*Power Injector*).
- VIII - Garantia por 60 meses, com suporte técnico em garantia.
- IX - Serviço de Instalação e configuração.
- X - Treinamento para repasse de conhecimento.
- XI - Todo licenciamento necessário para habilitação das funcionalidades descritas neste Termo de Referência.
- XII - Todos os componentes necessários para implantação e interconexão da solução, a saber: *transceivers*, cabos, cordões óticos, parafusos etc.
- XIII - Serviço de *Site Survey* prático.

4. VISTORIA FACULTATIVA

4.1. A avaliação prévia do local de execução dos serviços é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, sendo assegurado ao interessado o direito de realização de vistoria prévia, acompanhado por servidor designado para esse fim.

4.2. A vistoria deverá ser agendada previamente junto ao e-mail cau.hub-unb@hubrasil.gov.br, podendo as visitas serem realizadas entre a publicação do edital e o dia anterior à licitação.

4.3. A vistoria prévia permitirá ao proponente um melhor dimensionamento para elaboração da sua proposta, sendo possível verificar as condições físicas para a acomodação e instalação dos equipamentos, tais como: espaço nos racks, ponto de rede elétrica e lógica, etc.

4.4. A vistoria deve ser efetuada por representante legal da empresa licitante.

4.5. O representante deverá identificar-se, exibindo documento oficial de identificação e a documentação que comprove os poderes que lhe foram outorgados para realização da vistoria.

4.6. A vistoria não é obrigatória, porém, sua não realização não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo o contratado assumir os ônus dos serviços decorrentes."

4.7. A vistoria não é obrigatória, porém o licitante deverá apresentar declaração de que tem pleno conhecimento das condições e peculiaridades inerentes à natureza do objeto, assumindo total responsabilidade pelo fornecimento dos bens e pela prestação dos serviços, e que não haverá quaisquer questionamentos futuros que ensejem avenças técnicas ou financeiras ao HUB-UnB.

4.8. Ressalta-se que após apresentação das propostas, não serão admitidas alegações de inviabilidade de execução em decorrência de desconhecimento dos serviços e/ou dificuldades técnicas não previstas.

4.9. A vistoria é recomendada ao licitante interessado, com a finalidade de melhor conhecimento da infraestrutura e suas condições, podendo ofertar preço dos serviços com maior confiabilidade e exatidão.

4.10. Deverá abster-se, qualquer que seja a hipótese, de veicular publicidade ou qualquer outra informação acerca dos serviços, objeto do Termo de Referência, sem prévia autorização do HUB-UnB.

4.11. Os requisitos especificados neste Termo de Referência e seus anexos e encartes, são consideradas condições mínimas ao atendimento das necessidades do HUB-UnB e devem ser iguais ou superados pela CONTRATADA.

5. JUSTIFICATIVA PARA A CONTRATAÇÃO (IN 94/2022 SGD/ME - ART. 12, INCISO IV)

5.1. O HUB-UnB tem como missão ampliar os cenários de prática em diferentes áreas do conhecimento, de forma interprofissional, para atuação no SUS, além de fornecer um cenário de prática adequado ao ensino e pesquisa para docentes e discentes. Nesse sentido, as áreas de negócio utilizam os serviços de Tecnologia da Informação e Comunicações, providos pelo Setor de Tecnologia da Informação e Saúde Digital para consecução de suas metas e objetivos da gestão hospitalar.

5.2. Nesse contexto, o uso de tecnologias digitais tornou-se um meio cada vez mais presente na área da saúde e na transformação digital dos setores, abrangendo as ações de telemedicina, telessaúde, de áreas tradicionais da informática em saúde, como gestão hospitalar e prontuário eletrônico - uma esfera de intervenções tecnológicas denominada "Saúde Digital" pela Organização Mundial da Saúde - OMS

5.3. As áreas administrativas e assistenciais dependem do uso e das facilidades dos recursos proporcionados pela tecnologia da informação, cada vez mais essenciais ao desenvolvimento de suas atividades laborais de forma segura, incluindo a necessidade de estarem sempre conectados de forma segura e com mobilidade por meio das redes WIFI. Atualmente, tal solução tecnológica é imprescindível e proporciona:

- a) **Produtividade e Flexibilidade:** O Wi-Fi permite que os funcionários trabalhem de qualquer lugar dentro do hospital, aumentando a flexibilidade e a produtividade.
- b) **Colaboração:** Facilita a comunicação e a colaboração entre equipes, especialmente em ambientes de trabalho híbridos e distantes.
- c) **Acesso a Informações:** Proporciona acesso rápido e fácil a informações e recursos online, essenciais para a tomada de decisões em tempo real.
- d) **Segurança:** Redes Wi-Fi corporativas bem configuradas podem oferecer segurança robusta, protegendo dados sensíveis contra acessos não autorizados.
- e) **Monitoramento de Pacientes:** Permite o uso de dispositivos móveis para acessar equipamentos médicos conectados que permitam a monitoração dos pacientes, melhorando a qualidade do atendimento.
- f) **Acesso a Prontuários:** Facilita o acesso rápido a prontuários eletrônicos e resultados de exames, podendo agilizar o diagnóstico e o tratamento.
- g) **Comunicação:** Melhora a comunicação entre a equipe médica e assistencial, permitindo uma coordenação mais eficiente e respostas rápidas em situações de emergência.
- h) **Conforto dos Pacientes:** Oferece aos pacientes e seus familiares acesso à internet, o que pode ajudar a aliviar o estresse durante a estadia no hospital, atendendo à Lei nº 14.198, de 2 de setembro de 2021, que dispõe sobre videochamadas entre pacientes internados em serviços de saúde impossibilitados de receberem visitas e seus familiares.
- i) **Acesso a Informação para Professores, Alunos e Pesquisadores:** Prover acesso à rede sem fio é essencial para apoiar o processo de formação de profissionais, pesquisa e inovação. No ambiente de um hospital universitário como o HUB-UnB, a conectividade estável e segura permite que docentes, discentes e pesquisadores acessem recursos educacionais, plataformas de ensino à distância e bases de dados científicas, potencializando o aprendizado e a produção acadêmica. Além disso, facilita a condução de projetos de pesquisa interdisciplinares e a troca de conhecimento em tempo real, promovendo a inovação e a melhoria contínua na área da saúde, e garantindo a disseminação e aplicação do conhecimento em práticas que beneficiem diretamente os pacientes e a comunidade.
- j) **Compatibilidade com Rede Eduroam:** A solução de rede Wi-Fi deve ser compatível com a implementação da rede Eduroam, proporcionando acesso seguro e global aos docentes, discentes e pesquisadores facilitando a mobilidade acadêmica e a colaboração entre diferentes instituições nacionais e internacionais.
- k) **Conectividade de Dispositivos IoT (internet das coisas):** Com o aumento do uso de dispositivos IoT, como sensores, dispositivos de controle de acesso e câmeras, as redes sem fio são essenciais para suportar a conectividade desses dispositivos.

5.4. Atualmente, a solução de rede Wi-Fi disponível no HUB-UnB, encontra-se com mais de 07 (sete) anos de uso, já sem garantia e suporte técnico especializado, sujeita a eventuais indisponibilidades que venham causar a perda ou interrupção de conectividade móvel, além disso, a cobertura da rede sem fio atual não alcança todas as áreas do hospital.

5.5. A implementação de uma solução de rede Wi-Fi no Hospital Universitário de Brasília (HUB-UnB) deve atender aos requisitos de segurança da informação estabelecidos na Política de Segurança da Informação da Rede HU Brasil, que visa assegurar a confidencialidade, integridade e disponibilidade dos dados institucionais e de seus usuários. É fundamental que a rede sem fio seja projetada para mitigar riscos e ameaças cibernéticas, protegendo informações sensíveis e garantindo um ambiente seguro para a execução das atividades assistenciais, administrativas, de ensino e pesquisa. Dessa forma, a nova infraestrutura deve contemplar mecanismos robustos de autenticação e controle de acesso, criptografia de dados e monitoramento contínuo, em alinhamento com as diretrizes da HU Brasil para a proteção do patrimônio informacional e a conformidade com as legislações aplicáveis, conforme critérios apresentados abaixo:

- **Autenticação Segura:** A rede Wi-Fi deve utilizar mecanismos de autenticação robustos, integrando-se com o Active Directory ou LDAP para autenticação de usuários. A implementação deve suportar o uso de certificados digitais para garantir a identidade dos dispositivos e usuários.
- **Controle de Acesso Granular:** Deve ser possível configurar políticas de acesso segmentadas, garantindo que cada perfil de usuário (administrativo, assistencial, docente, discente, visitante, etc.) tenha acesso apenas aos recursos necessários para suas atividades. Implementar segmentação de rede (VLANs) para isolar tráfegos de diferentes áreas e dispositivos.
- **Criptografia de Dados:** Todo o tráfego da rede Wi-Fi deve ser criptografado usando padrões de segurança fortes (AES-256) para proteger a integridade e confidencialidade das informações transmitidas, incluindo comunicações de dados sensíveis, como prontuários eletrônicos e informações administrativas.
- **Gerenciamento e Monitoramento Contínuo:** A solução deve incluir funcionalidades de gerenciamento centralizado para monitoramento em tempo real do uso da rede, comportamento anômalo e possíveis tentativas de acesso não autorizado. Implementar alertas automáticos para detecção e resposta a incidentes de segurança.
- **Segurança em Redes de Visitantes:** As redes destinadas a visitantes e dispositivos não gerenciados devem ser separadas da rede corporativa e assistencial, com políticas de acesso restritivas que limitem a conectividade a serviços públicos, como internet, sem acesso aos sistemas internos do hospital.
- **Atualizações e Patches de Segurança:** Todos os equipamentos da rede Wi-Fi devem ser mantidos com firmware e patches de segurança atualizados, conforme as recomendações do fabricante, para evitar vulnerabilidades conhecidas.
- **Registros de Atividade (Logs):** A solução deve registrar logs detalhados de acesso, atividade e tentativas de violação, permitindo auditorias regulares e investigação em caso de incidentes de segurança. Os registros devem ser armazenados de forma segura e com retenção adequada para conformidade com normas e políticas internas.
- **Segmentação e Isolamento de Dispositivos IoT:** Dispositivos IoT conectados à rede Wi-Fi devem ser isolados em segmentos de rede dedicados, com políticas de segurança específicas para limitar seu acesso e minimizar o impacto em caso de comprometimento.
- **Conformidade com Normas e Regulamentos:** A solução deve estar em conformidade com as normas e regulamentos de segurança da informação aplicáveis, incluindo a LGPD (Lei Geral de Proteção de Dados), e as diretrizes de segurança da HU Brasil, garantindo a proteção dos dados pessoais e sensíveis dos usuários do HUB-UnB.

5.6. Portanto, com as necessidades perenes do HUB-UnB, no que compete à garantia e melhora dos recursos de Telecomunicações, neste caso especificamente no que tange à necessidade de modernizar e ampliar a rede WIFI, é imprescindível que se adotem ações de forma a garantir a disponibilidade destes recursos para execução das atividades cotidianas dos usuários do HUB-UnB.

5.7. Além do exposto, são requisitos de negócio que motivam esta solicitação:

- Prover ao HUB-UnB de bens de TI necessários ao atendimento institucional;
- Prover recursos para melhor rendimento, eficiência e segurança na realização das atividades;
- Prover condições tecnológicas necessárias para que o HUB-UnB preste atendimento com qualidade aos usuários finais;
- Prover recursos que garantam a disponibilidade dos serviços de TI demandados pelos usuários do HUB-UnB;
- Prover recursos que visem melhorar o padrão de atendimento aos usuários, o que permitirá maior eficiência nas atividades dos colaboradores que dependam de recursos de TI;
- Prover recursos que visem a melhoria da conectividade de dados, informações e sistemas que atendam ao HUB-UnB e à Rede HU Brasil;
- Suprir a perspectiva de crescimento da quantidade de usuários de TIC, oriundas das contratações realizadas a curto/médio prazo, visando o atendimento aos princípios do planejamento e eficiência, garantindo a padronização e a conformidade dessa expansão aos colaboradores do HUB-UnB.

5.8. Atualmente, a principal solução de Wi-Fi que atende ao HUB-UnB dispõe de equipamentos que cobrem cerca de 20% da área total do hospital, além disso, foram adquiridos em 2014, então destaca-se que o parque tecnológico de equipamentos da rede Wi-Fi do HUB-UnB tem cerca de 11 (onze) anos de utilização. No entanto, não possuem mais suporte e nem garantia para seu pleno funcionamento, sujeitos a eventuais indisponibilidades que venham causar a perda ou interrupção da conectividade.

5.9. Deste modo, a presente aquisição se justifica em face a necessidade de atualização e expansão da atual capacidade da rede Wi-Fi, considerando a expectativa de crescimento nos próximos 5 anos.

6. **ALINHAMENTO COM O PLANEJAMENTO DA CONTRATAÇÃO (IN 94/2022 SGD/ME - ART. 15, INCISO I)**

6.1. A contratação encontra-se prevista no PDTI 2020/2022, prorrogado até a finalização do PDTIC 2025/2028 conforme Ata - SEI 1 (49706271) e que atualmente encontra-se em vigor, por deliberação e aprovação do Comitê Gestor de Tecnologia da Informação e Comunicação do HUB-UnB. A prorrogação inclui a necessidade de aquisição de solução de rede Wi-Fi, conforme planejamento abaixo:

OBJETIVOS ESTRATÉGICOS DO REQUISITANTE
OETIC1 - Garantir e melhorar as condições de uso dos sistemas institucionais
NECESSIDADE PREVISTA NO PDTI
NTIC74 - Adquirir solução de WiFi
AÇÃO DO PDTI
ACTIC73 - Publicar Artefatos da Contratação

Tabela 3 - Planejamento da Contratação

6.2. **RELAÇÃO ENTRE A NECESSIDADE DA CONTRATAÇÃO DA SOLUÇÃO DE TIC E OS RESPECTIVOS VOLUMES E CARACTERÍSTICAS DO OBJETO (IN 94/2022 SGD/ME - Art. 15, inciso II)**

- 6.2.1. A relação entre a necessidade da contratação da Solução de rede Wi-Fi e as características do objeto encontram-se detalhados no Estudo Técnico Preliminar - ETP desta contratação, neste mesmo processo SEI.
- 6.2.2. O Estudo Técnico Preliminar foi elaborado no Sistema ETP Digital, que faz parte de uma ampla reformulação do Sistema de Compras do Governo Federal (ComprasNet) e representa uma importante entrega aos órgãos e entidades, que passam a contar com um sistema para guiar a elaboração dos estudos técnicos preliminares da contratação, de forma digital e integrada ao ComprasNet.

6.3. **FORMA DE CÁLCULO UTILIZADA PARA A DEFINIÇÃO DO QUANTITATIVO DE BENS E SERVIÇOS QUE COMPÕEM A SOLUÇÃO (IN 94/2022 SGD/ME - Art. 15, inciso III)**

6.3.1. A forma de cálculo utilizada para definição dos quantitativos de bens e serviços, levou em consideração outros certames da administração pública, assim como a análise das soluções de rede Wi-Fi existentes no HUB-UnB que necessitam serem substituídas, com a perspectiva de crescimento para os próximos 5 anos. Informações em um nível maior de detalhe encontram-se no Estudo Técnico Preliminar desta contratação.

6.4. **RESULTADOS E BENEFÍCIOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO (IN 94/2022 SGD/ME - Art. 15, inciso IV)**

- 6.4.1. Os principais resultados que se pretendem alcançar com a aquisição da solução de rede Wi-Fi no âmbito do HUB-UnB são:
- a) Melhoria na experiência do usuário final: A nova rede aumentará a performance dos equipamentos e proporcionará maior disponibilidade, velocidade e estabilidade, atendendo às demandas assistenciais, de ensino, pesquisa e serviços administrativos.
 - b) Menor risco de interrupções: A infraestrutura renovada com suporte especializado reduz riscos de paradas não planejadas, impactando positivamente a continuidade dos serviços essenciais do HUB-UnB.
 - c) Suporte a novas tecnologias: A solução adquirida permitirá a adoção de serviços baseados em IoT, integração com sistemas de controle de acesso, dispositivos *bluetooth* BLE e outras inovações tecnológicas futuras.
 - d) Adequação à estratégia institucional: A decisão está alinhada ao Objetivo Estratégico **OETIC1 - Garantir e melhorar as condições de uso dos sistemas institucionais**, garantindo um ambiente

mais seguro, gerenciável e preparado para expansão.

e) A atualização do parque tecnológico do HUB-UnB: A solução adquirida manterá os recursos essenciais de conectividade e mobilidade de dados para os sistemas informatizados e soluções tecnológicas mantidos pelo HUB-UnB, tais como equipamentos médicos transportáveis, além da integridade dos recursos com o serviço de suporte técnico especializado e garantia do fabricante para casos de necessidade de assistência técnica ou reposição de peças.

f) Aumentar a performance: Os equipamentos e soluções tecnológicas conectados via rede Wi-Fi mantidas pelo HUB-UnB, terão significativa melhora de segurança e performance, reduzindo o tempo de resposta dos dados.

g) Capacitação: Os profissionais de TI do HUB-UnB serão capacitados para operar a solução de rede Wi-Fi a ser adquirida.

6.5. ATA DE REGISTRO DE PREÇO

6.5.1. Essa contratação formará Ata de Registro de Preços.

6.5.2. O prazo de vigência da Ata de Registro de Preços será de 12 (doze) meses, contado a partir do primeiro dia útil subsequente à data de divulgação no PNCP, podendo ser prorrogado por igual período, mediante a anuência do fornecedor, desde que comprovado o preço vantajoso.

6.5.3. *A prorrogação da validade da Ata de Registro de Preços renova os quantitativos a serem adquiridos.*

6.5.4. Motivação para permitir adesões por parte de órgãos ou entidades não participantes (IN 94/2022 SGD/MB - art. 15, inciso IV).

6.5.4.1. Não será permitido adesões por órgãos ou entidades não participantes, em observância ao disposto nos arts. 31 e 66 da Lei nº 13.303/2016, considerando o princípio do planejamento e a economicidade que orientaram a presente contratação.

6.5.5. Serão admitidos reajustes e repactuações quando da renovação da Ata de Registro de preços, conforme termos da Ata.

7. ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO (IN 94/2022 SGD/ME - ART. 12, INCISO V)

7.1. REQUISITOS DE NEGÓCIO (IN 94/2022 SGD/ME - Art. 16, inciso I, alínea a)

7.1.1. Considerando a necessidade de acompanhar o crescimento contínuo da base de usuários de tecnologia da informação no HUB-UnB, manter a performance adequada no acesso a dados e sistemas, otimizar operações por meio da informatização de processos, fomentar a inovação e garantir a disseminação das melhores práticas institucionais, identificam-se os seguintes requisitos de negócio relacionados à conectividade e à modernização da rede Wi-Fi:

a) Disponibilizar os bens e serviços de TIC necessários ao atendimento das demandas institucionais do HUB-UnB, assegurando alinhamento com os objetivos estratégicos da organização.

b) Prover recursos tecnológicos que promovam maior eficiência, desempenho e segurança na execução das atividades assistenciais, administrativas, de ensino e pesquisa.

c) Assegurar condições tecnológicas adequadas para a prestação de serviços com qualidade aos usuários finais, internos e externos, do HUB-UnB. Garantir a disponibilidade e continuidade dos serviços de TIC acessados por meio da infraestrutura de rede sem fio, minimizando riscos de indisponibilidade.

d) Oferecer desempenho compatível com a crescente demanda por acesso a dados, aplicações e informações institucionais, suportando tráfego simultâneo e ambientes de alta densidade de usuários.

e) Permitir a segregação lógica de redes Wi-Fi, de forma a assegurar a confidencialidade, integridade e segurança das informações trafegadas.

7.1.2. Dessa forma, com vistas a contribuir para o atingimento dos objetivos institucionais e atender às exigências operacionais de forma eficiente e segura, torna-se imprescindível que o HUB-UnB mantenha e amplie sua solução de rede Wi-Fi, assegurando que os recursos tecnológicos estejam dimensionados e atualizados para suportar a crescente complexidade e volume dos serviços ofertados.

7.2. REQUISITOS DE CAPACITAÇÃO (IN 94/2022 SGD/ME - Art. 16, inciso I, alínea b)

7.2.1. Com o objetivo de assegurar a correta utilização, administração e manutenção da solução de rede Wi-Fi e sistema de controle de acesso a serem implantados, a CONTRATADA deverá realizar repasse de conhecimento técnico-operacional, conforme os critérios abaixo:

7.2.2. Deverá ser iniciado em até 5 (cinco) dias úteis, após a conclusão da implantação da solução, previamente acordado conforme disponibilidade da CONTRATANTE, sendo executado nos horários da manhã e/ou da tarde, em turnos diários de no máximo 04h /dia, com carga total de no mínimo 20 (vinte) horas, para uma turma de até 5 alunos e até 5 ouvintes.

7.2.3. Deverá ser fornecido pela CONTRATADA todo o material audiovisual, didático e eletrônico para a realização dos treinamentos, além de impressos e quaisquer outras despesas diretas ou indiretas.

7.2.4. Deverá ser ministrado em idioma português do Brasil, em dias úteis, durante o horário comercial, contemplando no mínimo de 04 (quatro) horas, no modelo "operação assistida" (*hands-on*), realizado no ambiente implantado no HUB-UnB.

7.2.5. O planejamento do treinamento deverá considerar o menor impacto possível às atividades operacionais da equipe a ser capacitada.

7.2.6. Ao final da capacitação, os participantes deverão estar aptos a administrar a solução ofertada.

7.2.7. Deverá ser fornecido certificado de participação a cada um dos integrantes que participar da capacitação, com presença mínima de 60%, contendo ao menos: nome do participante, período, carga horária, conteúdo programático, a identificação da empresa CONTRATADA, do instrutor e da solução ofertada.

7.2.8. Ao final da capacitação, os participantes deverão estar aptos a administrar a solução ofertada e a CONTRATADA deverá disponibilizar:

- O conteúdo programático apresentado; e
- A gravação integral das sessões de treinamento.

7.3. **REQUISITOS LEGAIS (IN 94/2022 SGD/ME - Art. 16, inciso I, alínea c)**

7.3.1. No âmbito deste processo devem ser observados os respectivos requisitos legais:

7.3.2. Lei nº 13.303, de 30 de junho de 2016 - Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios.

7.3.3. Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022 - Estabelece diretrizes e procedimentos para o processo de contratação de soluções de Tecnologia da Informação e Comunicação (TIC) pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

7.3.4. Regulamento de Compras e Contratos (RCC 3.0) - estabelece normas e procedimentos de aquisição de bens, contratação de serviços e obras, e de alienação de bens no âmbito da Empresa Brasileira de Serviços Hospitalares (HU Brasil).

7.3.5. Norma Operacional SEI nº 3/2024/SCCEN/CAD/DAI-EBSERH - Dispõe sobre o procedimento administrativo para a realização de pesquisa de preços e alterações contratuais no âmbito da HU Brasil.

7.3.6. Decreto nº 11.462, de 31 de março de 2023 - Dispõe sobre o sistema de registro de preços para a contratação de bens e serviços, inclusive obras e serviços de engenharia, no âmbito da Administração Pública federal direta, autárquica e fundacional.

7.3.7. Política de Segurança da Informação da Rede HU Brasil - Estabelece princípios, diretrizes e responsabilidades para a proteção da informação no ambiente da HU Brasil. [Link: <https://www.gov.br/ebserh/pt-br/governanca/governanca-de-tecnologia-da-informacao/PoliticaSegurancadainformacaodaebserhverso2.pdf>]

7.3.8. Política de Proteção de Dados Pessoais da HU Brasil- Define as diretrizes e práticas para o tratamento de dados pessoais em conformidade com a LGPD. [Link: https://www.gov.br/ebserh/pt-br/governanca/governanca-corporativa/politica-de-protecao-de-dados-pessoais/politica_de_protecao_de_dados_pessoais_da_rede_ebserh.pdf]

7.3.9. Decreto-Lei nº 200, de 25 de fevereiro de 1967 - Dispõe sobre a organização da Administração Pública Federal e estabelece diretrizes para a Reforma Administrativa.

7.3.10. Decreto nº 7.174, de 12 de maio de 2010 - Regulamenta a contratação de bens e serviços de informática e automação pela Administração Pública Federal, direta e indireta.

7.3.11. Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD) - Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e desenvolvimento da personalidade da pessoa natural.

7.3.12. Decreto nº 9.373, de 11 de maio de 2018 - Dispõe sobre a destinação ambientalmente adequada de bens móveis no âmbito da Administração Pública Federal direta, autárquica e fundacional.

7.3.13. Instrução Normativa SLTI/MP nº 1, de 19 de janeiro de 2010 - Estabelece critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal.

7.3.14. Lei nº 12.305, de 2 de agosto de 2010 - Institui a Política Nacional de Resíduos Sólidos e estabelece diretrizes para a gestão integrada e o gerenciamento de resíduos no país.

7.3.15. Decreto nº 10.779, de 25 de agosto de 2021 - Estabelece medidas para a eficiência energética e a redução do consumo de energia elétrica no âmbito da Administração Pública Federal.

7.4. REQUISITOS DE MANUTENÇÃO (IN 94/2022 SGD/ME - Art. 16, inciso I, alínea d)

7.4.1. Todos os produtos que compõem a solução de rede Wi-Fi e sistema de controle de acesso deverão contar, durante toda a vigência do contrato e/ou período de garantia, com suporte técnico especializado e garantia fornecida pelos fabricantes, assegurando, no mínimo, os seguintes serviços:

- Reposição de peças com defeito;
- Disponibilização de atualizações de segurança e melhorias sistêmicas;
- Correção de falhas (*bugs*) identificadas na solução;
- Assistência técnica para esclarecimento de dúvidas, resolução de incidentes e tratamento de eventuais indisponibilidades da solução.

7.4.2. Deverão ser disponibilizados canais diretos de atendimento ao fornecedor ou aos fabricantes para abertura, acompanhamento e resolução de chamados técnicos sempre que necessário.

7.4.3. A CONTRATADA deverá fornecer documentação técnica completa, atualizada e em língua portuguesa, que permita o diagnóstico, a operação e a administração adequada da solução de rede Wi-Fi e do sistema de controle de acesso.

7.4.4. Durante todo o período de suporte técnico e garantia, deverão estar assegurados serviços de atendimento que possibilitem:

- Solicitação de informações técnicas e de operação;
- Registro e acompanhamento de incidentes;
- Esclarecimento de dúvidas operacionais relacionadas ao uso dos equipamentos e sistemas da solução ofertada.

7.4.5. O suporte técnico deverá ser prestado de forma que não comprometa a validade da garantia fornecida pelo fabricante.

7.4.6. Deverão ser estabelecidos Níveis Mínimo de Serviço (NMS) contendo prazos máximos de resposta e resolução, canais de atendimento, níveis de prioridade, horários de atendimento, responsabilidades das partes e penalidades por descumprimento.

7.4.7. Deverá ser prevista solução de contingência ou de contorno nos casos em que houver acionamento da garantia, de forma a mitigar impactos e minimizar o tempo de indisponibilidade da solução.

7.4.8. A adição de novos equipamentos à infraestrutura da solução de rede Wi-Fi, devidamente compatíveis, não deverá implicar perda ou limitação das garantias ofertadas.

7.4.9. Deverão ser previstas sanções administrativas à CONTRATADA em caso de prejuízos causados ao HUB-UnB por imperícia, falhas técnicas, negligência ou uso inadequado durante intervenções de manutenção.

7.4.10. Nos casos em que for necessária a substituição de qualquer equipamento, peça ou componente defeituoso, o item deverá ser repostado por outro equivalente ou de especificações superiores, sem prejuízo da garantia e mantendo todas as condições técnicas, funcionais e contratuais originalmente estabelecidas.

7.5. REQUISITOS TEMPORAIS (IN 94/2022 SGD/ME - Art. 16, inciso I, alínea e)

7.5.1. Todos os equipamentos que fazem parte da solução de rede Wi-Fi e sistema de controle de acesso deverão ser entregues no local indicado em até 60 (sessenta) dias corridos, a contar da data de abertura da Ordem de Serviço.

7.5.2. Local de entrega e instalação:

7.5.3. HUB-UnB - Hospital Universitário de Brasília Endereço: Setor de Grandes Áreas Norte, nº 605 Asa Norte, Brasília - Distrito Federal CEP: 70840-90 Telefone: (61)2028-5346.

7.5.4. A entrega dos equipamentos pela transportadora deverá ser previamente comunicada ao HUB-UnB com no mínimo 2 (dois) dias úteis de antecedência.

7.6. REQUISITOS DE SEGURANÇA E PRIVACIDADE (IN 94/2022 SGD/ME - Art. 16, inciso I, alínea f)

7.6.1. A execução dos serviços deverá obedecer integralmente às diretrizes estabelecidas na Política de Segurança da Informação (PSI) da HU Brasil, bem como às suas normas complementares e demais regulamentos internos aplicáveis.

7.6.2. A CONTRATADA deverá formalizar, por meio de um representante legal, o Termo de Compromisso, emitido pela CONTRATANTE.

7.6.3. Todos os profissionais da CONTRATADA envolvidos na prestação dos serviços deverão:

- a) Assinar o Termo de Ciência, fornecido pela CONTRATANTE, atestando conhecimento e Termo de Compromisso com os procedimentos e normas de segurança vigentes;

b) Estar devidamente identificados, utilizando crachá ou outro meio de identificação oficial da empresa, sempre que estiverem nas dependências do HUB-UnB, sejam representantes do fornecedor ou do fabricante da solução contratada.

7.6.4. A CONTRATADA deverá assegurar a confidencialidade, integridade e disponibilidade das informações tratadas no escopo do projeto, comprometendo-se a não divulgar, compartilhar ou disponibilizar a terceiros quaisquer dados ou informações obtidas no curso da execução contratual, salvo mediante autorização prévia, formal e expressa da CONTRATANTE.

7.6.5. A CONTRATADA e seus representantes deverão, ainda, respeitar rigorosamente todas as normas, políticas e procedimentos de segurança da informação em vigor no ambiente de Tecnologia da Informação do HUB-UnB, responsabilizando-se por eventuais infrações ou danos decorrentes do descumprimento dessas obrigações.

7.7. REQUISITOS SOCIAIS, AMBIENTAIS E CULTURAIS (IN 94/2022 SGD/ME - Art. 16, inciso I, alínea g)

7.7.1. A execução do objeto contratual deverá observar os critérios de sustentabilidade ambiental estabelecidos no art. 5º da Instrução Normativa SLTI/MPOG nº 01, de 19 de janeiro de 2010, e no Decreto nº 7.746, de 5 de junho de 2012, no que for aplicável.

7.7.2. Deverão ser adotados recursos tecnológicos que promovam o menor consumo de energia elétrica, visando à eficiência energética e à redução dos impactos ambientais.

7.7.3. Deverá disponibilizar sistema de chamados para atendimento técnico e de encaminhamento de demandas, preferencialmente, de interface eletrônica, de forma a evitar o uso de papel, promovendo práticas sustentáveis e reduzindo a geração de resíduos sólidos.

7.7.4. As configurações dos equipamentos de *hardware* e *software* deverão ser planejadas e executadas com foco em alto desempenho e no uso racional de energia, sem prejuízo da funcionalidade da solução ofertada.

7.7.5. Os equipamentos fornecidos deverão ser acondicionados, preferencialmente, em embalagens individuais compactas e adequadas, compostas por materiais recicláveis e que garantam a devida proteção durante o transporte e o armazenamento.

7.7.6. Os bens que compõem a solução deverão ser constituídos, no todo ou em parte, por materiais reciclados, atóxicos e biodegradáveis, conforme as normas técnicas da ABNT NBR 15448-1 e 15448-2.

7.7.7. O fornecedor deverá observar integralmente as normas, procedimentos e boas práticas referentes à prestação de serviços, abstendo-se de propor soluções inadequadas, danosas ou em desacordo com o mercado. Será de responsabilidade da CONTRATADA, o descarte ambientalmente adequado de resíduos decorrentes da substituição ou reposição de peças, quando necessário.

7.7.8. O fornecedor deverá respeitar todas as normas técnicas brasileiras aplicáveis, especialmente aquelas publicadas pela Associação Brasileira de Normas Técnicas (ABNT) relacionadas à gestão e ao descarte de resíduos sólidos.

7.8. REQUISITOS GERAIS DA SOLUÇÃO

7.8.1. Em conformidade com os art. 156 e art.162 da Lei Geral de Telecomunicações (Lei nº 9.472/1997), com a Resolução ANATEL nº 715/2019 e por serem equipamentos de telecomunicação com radiofrequência, os Access Points deverão possuir homologação vigente da Agência Nacional de Telecomunicações (ANATEL), sendo obrigatória a apresentação de cópia do Certificado de Homologação anexa à proposta técnica, para comprovação da regularidade de operação no Brasil, nos termos da legislação vigente.

7.8.2. Deverão ser compatíveis com, no mínimo, o padrão Wi-Fi 6 (IEEE 802.11ax) ou superior.

7.8.3. A solução deverá suportar, no mínimo, 500 (quinhentos) *Access Points* simultâneos

7.8.4. Deverá permitir a conexão simultânea de, no mínimo, 10.000 (dez mil) clientes (dispositivos) *wireless*, mesmo em caso de indisponibilidade de uma das controladoras (no caso de ser física). Cabe ressaltar que os acessos simultâneos envolvem não só usuários, mas também equipamentos que podem ser conectados, tais como celulares, impressoras, notebooks, IoT, sensores, dentre outros.

7.8.5. Deverá permitir a criação de portal Web personalizável (*captive portal*), com mecanismo de autenticação para clientes externos, incluindo autenticação via plataforma GOV.BR, Google e Facebook e outros logins sociais, com armazenamento dos registros de autenticação.

7.8.6. Deverá permitir a criação de, no mínimo, 2.000 (dois mil) usuários visitantes diretamente na solução de rede Wi-Fi.

7.8.7. Deverá permitir a criação de contas de visitantes com validade de acesso temporária.

7.8.8. Deverá ser compatível com a rede de dados local do CONTRATANTE, apresentando compatibilidade de protocolos, configurações, energização elétrica e demais funcionalidades necessárias à integração com a infraestrutura

de rede do HUB-UnB.

7.8.9. Deverá ser disponibilizada toda a documentação técnica original e atualizada da solução, contendo manuais, guias e mídias de instalação em meio eletrônico, se for o caso. Essa documentação poderá ser acessada por meio do site oficial do fabricante, desde que livre para *download* e sem exigência de senha, podendo estar em português (PT-BR) ou inglês.

7.8.10. Com o objetivo de assegurar a continuidade do suporte do fabricante, a disponibilidade de atualizações de segurança, a manutenção da interoperabilidade tecnológica e a economicidade do investimento ao longo do ciclo de vida da solução, os componentes da rede Wi-Fi ofertada não poderão estar classificados pelo fabricante como *End of Sale (EoS)* ou *End of Life (EoL)* na data de abertura da licitação. Caso essa condição ocorra durante a vigência contratual, a CONTRATADA deverá garantir o suporte, atualizações e pleno funcionamento da solução, promovendo, quando necessário, a substituição por equipamentos equivalentes ou superiores, sem ônus e sem prejuízo à CONTRATANTE.

7.8.11. A solução deverá operar em modo de alta disponibilidade, podendo ser configurada em ativo/passivo ou ativo/ativo, com transição automática e sem impactos ao ambiente em caso de falha do componente controlador.

7.8.12. Deverá permitir a sincronização automática das configurações entre os componentes da solução para operar em alta disponibilidade.

7.8.13. Os equipamentos deverão estar devidamente acondicionados e protegidos contra danos provenientes de transporte ou manuseio.

7.8.14. Deverá permitir o gerenciamento centralizado de todos os *Access Points*, por meio de interface web, com funcionalidades de monitoramento, provisionamento, configuração em lote e geração de relatórios detalhados.

7.8.15. Deverá permitir o gerenciamento centralizado do sistema de controle de acesso, por meio de interface web, com funcionalidades de monitoramento, provisionamento, configuração em lote e geração de relatórios detalhados.

7.8.16. Deverá permitir atualizações de firmware de forma centralizada, com possibilidade de agendamento e mecanismo de *fallback* automático em caso de falhas na atualização.

7.8.17. Deverá ser compatível com os protocolos IPv4 e IPv6, em conformidade com diretrizes de evolução tecnológica da infraestrutura do CONTRATANTE.

7.8.18. Deverá suportar a configuração de VLANs, segmentação de tráfego e aplicação de QoS, visando priorização de tráfego sensível como voz e vídeo.

7.8.19. Deverá contar com recursos de segurança integrados, incluindo detecção e mitigação de ataques, proteção contra *Access Points* não autorizados (*rogue APs*), isolamento de clientes e suporte à autenticação 802.1X.

7.8.20. Os requisitos estabelecidos neste documento devem ser considerados como condições mínimas para atendimento às necessidades do HUB-UnB, podendo ser superados pela CONTRATADA.

7.9. REQUISITOS DE LICENCIAMENTO DA SOLUÇÃO

7.9.1. Deverá possuir todo o licenciamento necessário para que a solução continue operacional e configurável, em todas as funcionalidades contratadas, mesmo após o término da garantia, sem a obrigatoriedade de aquisição de novas atualizações ou renovações por parte do fabricante.

7.9.2. Deverá incluir todas as licenças necessárias que permitam a expansão modular ou gradual da solução, contemplando o aumento do número de *Access Points*, sem necessidade de recontração de licenças básicas.

7.9.3. Deverá vir licenciada de forma a permitir o cadastro de todos os *Access Points* adquiridos, assegurando o pleno funcionamento da solução com todas as suas funcionalidades, mesmo após o encerramento do período de garantia.

7.9.4. Deverá vir licenciada de forma a permitir o gerenciamento de usuários e visitantes, assegurando o pleno funcionamento da do sistema de controle de acesso com todas as suas funcionalidades, mesmo após o encerramento do período de garantia.

7.9.5. Deverá ser fornecidas licenças suficientes para garantir o funcionamento completo e simultâneo de toda a infraestrutura da rede Wi-Fi e sistema de controle de acesso, assegurando resiliência operacional.

7.9.6. Deverá incluir todas as licenças necessárias para que a plataforma de gerenciamento atenda plenamente aos requisitos técnicos desta contratação, inclusive quanto ao número mínimo de conexões simultâneas especificadas.

7.9.7. Todas as licenças deverão ser entregues, instaladas e ativadas pela CONTRATADA, de forma que a solução esteja plenamente operacional durante todo o período de suporte e garantia, sendo obrigatória a comprovação documental e técnica desta ativação como condição para o aceite definitivo dos produtos.

7.9.8. Deverá ser fornecido documento oficial do fabricante ou acesso a portal público, vinculados à CONTRATANTE, contendo a identificação clara de cada licença, seus quantitativos e validade, permitindo a verificação do correto licenciamento da solução.

- 7.9.9. As licenças ofertadas deverão corresponder a versões atualizadas, estáveis e suportadas pelo fabricante, sem a necessidade de aquisição adicional de hardware ou software para seu funcionamento completo.
- 7.9.10. Deverá ser garantida a possibilidade de atualização da solução durante todo o período de garantia, assegurando suporte contínuo do fabricante sempre que necessário.
- 7.9.11. Após o término do período de garantia, deverá ser assegurada a permanência de todas as funcionalidades habilitadas durante a vigência contratual, sem descontinuidade de operação.
- 7.9.12. As licenças deverão contemplar de forma abrangente todos os serviços descritos nesta contratação, garantindo suporte ao número mínimo de acessos simultâneos estabelecido.
- 7.9.13. Deverá ser disponibilizada, juntamente a cada *Access Point* fornecido, a respectiva licença necessária ao seu pleno funcionamento, sem qualquer custo adicional para a CONTRATANTE.
- 7.9.14. Deverão ser fornecidas, no mínimo, 500 (quinhentas) licenças para verificação de postura de dispositivos diversos conectados simultaneamente à rede Wi-Fi, sem limitação por tipo de equipamento ou fabricante.
- 7.9.15. As licenças da solução do NAC deverão ser dinâmicas, não sendo vinculadas a usuários ou dispositivos fixos (*endpoints*), mas sim operando em regime de *pool*, de forma que licenças não utilizadas retornem ao conjunto disponível para reutilização.
- 7.9.16. A autenticação de usuários visitantes por meio do portal Gov.BR e login social com integração com Google e Facebook e outros, não deverá computar as licenças de verificação de postura.
- 7.9.17. As funcionalidades descritas, sejam elas integrais ou parciais, poderão ser implementadas por qualquer componente da solução (*Access Points*, controladora, solução de gerenciamento, monitoramento ou controle de acesso) ou pela combinação entre eles, desde que atendam aos requisitos especificados nesta contratação.

7.10. REQUISITOS DE ARQUITETURA TECNOLÓGICA (IN 94/2022 SGD/ME - Art. 16, inciso II, alínea a)

7.10.1. TERMOS E DEFINIÇÕES

- 7.10.1.1. **Wi-Fi** (Wireless Fidelity): Tecnologia de comunicação sem fio baseada no padrão IEEE 802.11, que permite que dispositivos se conectem a uma rede local (LAN) utilizando ondas de rádio, sem a necessidade de cabos.
- 7.10.1.2. **SSID** (Service Set Identifier): Nome da rede Wi-Fi que a identifica de forma única em um ambiente. Os dispositivos utilizam o SSID para localizar e se conectar à rede.
- 7.10.1.3. **WPA** (Wi-Fi Protected Access): Protocolo de segurança para redes Wi-Fi.
- **WPA**: Primeira versão, com melhorias em relação ao WEP.
 - **WPA2**: Mais segura, baseada em AES (Advanced Encryption Standard).
 - **WPA3**: É o padrão mais recente de segurança para redes Wi-Fi, ele oferece proteção mais forte contra ataques, autenticação mais robusta e criptografia mais avançada para usuários e dispositivos
- 7.10.1.4. **WEP** (Wired Equivalent Privacy): Protocolo de segurança obsoleto, com diversas vulnerabilidades, substituído por WPA e WPA2.
- 7.10.1.5. **Virtual Machine** (VM): Instância virtualizada de um computador, executada por meio de software, permitindo a operação de múltiplos sistemas em um único hardware físico.
- 7.10.1.6. **Hypervisor**: Software que permite a criação e gerenciamento de máquinas virtuais, agregando e alocando recursos físicos como CPU, memória e armazenamento entre VMs.
- 7.10.1.7. **Appliance**: Equipamento com hardware e software dedicados a uma função específica, como controladora de rede, firewall, entre outros.
- 7.10.1.8. **Access Point** (Ponto de Acesso): Dispositivo que estende a conectividade de uma rede cabeada, criando uma rede Wi-Fi e permitindo a conexão de dispositivos sem fio.
- 7.10.1.9. **Mesh Network**: Arquitetura em que múltiplos Access Points trabalham juntos, repassando sinal entre si para ampliar a cobertura e estabilidade da rede.
- 7.10.1.10. **Hotspot**: Ponto de acesso Wi-Fi, normalmente instalado em locais públicos, oferecendo acesso à internet.
- 7.10.1.11. **Captive Portal**: Página de autenticação exibida ao usuário ao conectar-se à rede, comum em redes públicas e corporativas.
- 7.10.1.12. **NAC** (Network Access Control): Sistema de controle de acesso. Conjunto de tecnologias e políticas que controlam o acesso de usuários e dispositivos à rede, baseando-se em autenticação e verificação de conformidade.
- 7.10.1.13. **SSID Oculto**: SSID configurado para não ser divulgado publicamente. Requer conhecimento prévio do nome da rede para conexão.
- 7.10.1.14. **QoS** (Quality of Service): Técnica que prioriza certos tipos de tráfego de rede (voz, vídeo, etc.) para garantir

qualidade e desempenho.

7.10.1.15. **MIMO** (Multiple Input, Multiple Output): Tecnologia que permite múltiplos fluxos simultâneos de dados, usando múltiplas antenas, aumentando desempenho e confiabilidade.

7.10.1.16. **Beamforming**: Técnica que concentra o sinal Wi-Fi na direção dos dispositivos conectados, aumentando o alcance e a qualidade da conexão.

7.10.1.17. **Roaming**: Capacidade de um dispositivo se manter conectado à rede Wi-Fi ao transitar entre diferentes *Access Points* da mesma rede, sem perda de conexão.

7.10.1.18. **Canal** (Channel): Faixa de frequência utilizada pela rede Wi-Fi para transmissão de dados. A escolha adequada evita interferências.

7.10.1.19. **Frequências 2.4GHz e 5GHz:**

- 2.4 GHz: Maior alcance, mais suscetível à interferência.
- 5 GHz: Mais canais, menos interferência, menor alcance.
- 6 GHz: Maior densidade

7.10.1.20. **Wi-Fi 6** (802.11ax): Sexta geração de Wi-Fi que conta com maior desempenho, eficiência e capacidade, ideal para ambientes com muitos dispositivos conectados.

7.10.1.21. **Throughput**: Quantidade de dados transmitida por unidade de tempo, expressa em Mbps ou Gbps.

7.10.1.22. **Latência**: Tempo necessário para que um pacote de dados percorra de um ponto a outro na rede, medido em milissegundos (ms). Baixa latência é desejável.

7.10.1.23. **Interferência**: Obstáculo à transmissão de sinal causado por dispositivos operando na mesma frequência ou por barreiras físicas.

7.10.1.24. **HotSwap**: Capacidade de substituir componentes de hardware sem desligar o sistema.

7.10.1.25. **Injetor PoE** (Power over Ethernet): Tecnologia que transmite dados e energia elétrica através de um único cabo de rede, simplificando a instalação de APs e outros dispositivos.

7.10.1.26. **End-of-Life** (EoL): Data após a qual o fabricante encerra a produção e distribuição do produto.

7.10.1.27. **End-of-Sale** (EoS): Data a partir da qual o produto não é mais comercializado, embora suporte ainda possa ser mantido por um período.

7.10.1.28. **End-of-Support-Life** (EoSL): Data em que o fabricante encerra suporte técnico e atualizações para o produto.

7.10.1.29. **RADIUS** (Remote Authentication Dial-In User Service): Protocolo utilizado para autenticação, autorização e contabilização (AAA) de usuários em redes Wi-Fi corporativas, frequentemente integrado ao NAC.

7.10.2. REQUISITOS DE INFRAESTRUTURA TECNOLÓGICA

7.10.2.1. A solução de rede Wi-Fi e o sistema de controle de acesso poderá ser entregue na forma de equipamento físico (*appliance*) ou como aplicação virtual (*virtual machine*), para instalação *on-premises* no Datacenter do HUB-UnB, respeitando os seguintes requisitos conforme o modelo adotado:

a) No caso de equipamento físico (*appliance*):

- Deverá ser instalada no datacenter do HUB-UnB, devidamente montada em rack padrão de 19" (dezenove polegadas), acompanhada dos acessórios necessários para a fixação.
- Deverá operar com alimentação elétrica em tensão entre 100 a 240 VAC, 50/60Hz, com suporte a recursos de redundância e alta disponibilidade, incluindo redundância de fonte de alimentação.
- Deverá suportar operação em temperatura ambiente de 10°C a 40°C.
- Deverá possuir, no mínimo, 2 (duas) portas de *uplink* com conector SFP+, compatíveis com *transceivers* 10GBASE-SR. Os *transceivers* e cabos ópticos necessários, devem ser fornecidos pela CONTRATADA.
- Deverá possuir LEDs indicadores para status do equipamento e das interfaces Ethernet.
- Deverá permitir armazenamento da configuração em memória não volátil, garantindo a retomada da operação com a mesma configuração após falhas de energia.
- Deverá implementar os padrões abertos de gerenciamento SNMPv2c e SNMPv3, com suporte à MIB II (RFC 1213), geração de traps e MIB privativa com documentação completa.
- Deverá permitir a coleta via SNMP de informações sobre configuração, desempenho, utilização de CPU e memória, e status das interfaces.
- Os equipamentos deverão ser específicos e compatíveis com a solução rede Wi-Fi ofertada, sendo do mesmo fabricante ou oficialmente homologados por este.
- Não será necessário o fornecimento do rack de 19" para instalação da solução.

b) No caso de aplicação virtual (*virtual machine*):

- Deverá ser compatível, no mínimo, com os *hypervisors* XCP-ng 8.2 ou Microsoft Hyper-V.
- Deverá permitir instalação em ambiente Windows Server 2019 ou superior, disponibilizado pelo HUB-UnB, ou em Linux Debian 12 ou superior.
- Deverão ser fornecidas aplicações do mesmo fabricante da Solução rede Wi-Fi ou comprovadamente compatíveis com a solução.
- Não serão aceitas controladoras baseadas exclusivamente em nuvem (*cloud*) externa.

7.10.3. REQUISITOS DA CONTROLADORA WI-FI

7.10.3.1. Deverá operar em modo de alta disponibilidade com redundância. Em caso de falha de uma das controladoras ou de sua comunicação, os *Access Points* deverão ser realocados automaticamente a outra controladora, garantindo a persistência de sessão e a continuidade do acesso para usuários já conectados, sem intervenção manual e de forma transparente. A comutação entre controladoras deverá ser inferior a 2 segundos.

7.10.3.2. Deverá possuir integração com o *Microsoft Active Directory* para autenticação de usuários na solução de gerência de modo a permitir níveis de acesso administrativo para apenas leitura, leitura/escrita, criação de contas de usuários do tipo visitante (*guest*), entre outros.

7.10.3.3. Deverá permitir o direcionamento do tráfego de saída de usuários visitantes (*guests*) para uma rede isolada do tráfego da rede corporativa por meio de VLAN específica.

7.10.3.4. As funções de gerenciamento deverão ser acessíveis através de servidores ou estações de trabalho com sistemas operacionais Microsoft Windows Server 2019 e superiores ou Microsoft Windows 11 e superiores.

7.10.3.5. Deverá gerar e permitir visualizar registros de eventos relacionados à solução de rede Wi-Fi e que os eventos gerados possam ser encaminhados para servidor externo via protocolo *syslog*, indicando pelo menos a severidade, IP do equipamento, mensagem, data e horário do evento.

7.10.3.6. Deverá fornecer ambiente de visualização de dados coletados com estatísticas de performance de todos os elementos pertencentes à solução, incluindo o monitoramento do desempenho da rede Wi-Fi, consolidando informações de níveis de ruído, relação sinal-ruído, utilização de canais, número de cliente conectados, interferência e potência de sinal de *Access Point*.

7.10.3.7. Deverá permitir a visualização de informações de clientes conectados à rede sem fio, tais como: endereço IP, endereço MAC, nome do usuário, caso estejam logados via 802.1x, SSID, ponto de acesso.

7.10.3.8. Deverá permitir realizar as configurações e o gerenciamento completo centralizado dos parâmetros da rede Wi-Fi, políticas de segurança, QoS e gerenciamento de rádio frequência, onde os *Access Points* fazem parte de um cluster com informações centralizadas e controle da rede Wi-Fi;

7.10.3.9. A solução de controle e gerência da rede Wi-Fi deve ser do mesmo fabricante dos *Access Points*, para garantir a interoperabilidade entre os recursos;

7.10.3.10. Deverá permitir realizar o *upgrade* remoto de firmwares dos *Access Points*;

7.10.3.11. Deverá empregar criptografia de dados no canal de comunicação com os *Access Points* Wi-Fi;

7.10.3.12. Deverá implementar a comunicação de dados por meio do modo "*local switching*".

7.10.3.13. No modo "*local switching*" não é necessário que todo o tráfego seja direcionado a controladora antes de ser encaminhado ao restante da rede, sendo possível a comunicação local entre os usuários e os recursos (impressoras, servidores) de rede sem o controle prévio da controladora.

7.10.3.14. Deverá permitir a realização de backups das configurações da controladora.

7.10.3.15. Deverá permitir integração com os servidores de autenticação do HUB-UnB (*Microsoft Active Directory* e LDAP) para autenticação dos usuários internos;

7.10.3.16. Deverá permitir roaming transparente, sem troca de endereçamento para o cliente móvel, pelo menos em *Layer 2*.

7.10.3.17. Deverá suportar, no mínimo, 500 (quinhentos) *Access Points* simultâneos, com objetivo de suportar expansões futuras.

7.10.3.18. Deverá implementar, no mínimo, 32 (trinta e dois) SSID, permitindo configurações distintas de autenticação, QoS, criptografia, SSID e VLAN para cada domínio. Deve ser possível especificar em quais *Access Points* ou Grupos de *Access Points* serão aplicados.

7.10.3.19. Deverá possuir capacidade de centralização, manutenção, gerência e distribuição das configurações da solução de rede Wi-Fi, inclusive das configurações e atualizações dos *Access Points*.

7.10.3.20. Deverá realizar a gerência das configurações de segurança da rede sem fio e parâmetros de rádio frequência (RF).

7.10.3.21. Deverá permitir que os SSIDs operem em comutação de tráfego local.

7.10.3.22. Deverá permitir a utilização de *captive portal* externo a controladora.

7.10.3.23. Deverá permitir, a criação de SSID para visitantes, que terão seu acesso controlado através de criação de usuário e senha cadastrados internamente, sendo que este deverá possuir tempo predeterminado de acesso à rede Wi-Fi.

7.10.3.24. Deverá permitir que, após o processo de autenticação de usuários visitantes, os mesmos sejam redirecionados para uma página de navegação específica.

7.10.3.25. Deverá proporcionar AAA (*Authentication, Authorization, and Accounting*) em servidor RADIUS.

7.10.3.26. Deverá implementar protocolo de autenticação para acesso administrativo ao equipamento tanto localmente, (*Local Authentication Database*), quanto por autenticação externa (RADIUS).

7.10.3.27. Deverá permitir a configuração e operação de no mínimo dois servidores RADIUS para fornecer redundância na autenticação.

7.10.3.28. Deverá permitir que na ocorrência de falha na comunicação com o servidor RADIUS principal, o sistema deverá buscar um servidor RADIUS secundário.

7.10.3.29. Deverá permitir a seleção/uso de servidor RADIUS com atributos *radius standard*.

7.10.3.30. Deverá permitir a configuração de servidor diferente para autorização e *accounting*.

7.10.3.31. Deverá atender a conformidade com a RFC 3576/5176 (*Change of Authorization*).

7.10.3.32. Deverá permitir a programação e a ativação ou desativação de SSID baseado em dia/hora, permitindo ao administrador do sistema, habilitar ou não um determinado SSID somente em hora/dia determinados.

7.10.3.33. Deverá possuir ferramentas de *debug* e *log* de eventos para depuração e gerenciamento em primeiro nível (*ping, trace e logs*).

7.10.3.34. Deverá possibilitar cópia (*backup*) da configuração, bem como a funcionalidade *restore* da configuração através de browser padrão (*HTTPS*).

7.10.3.35. Deverá permitir a captura dos pacotes transmitidos na rede sem fio atuando como um wireless *sniffer* para fins de *debug*. Os pacotes capturados poderão ser armazenados no ponto de acesso ou exportados diretamente para softwares de terceiros que suporte arquivos com padrão pcap ou cap.

7.10.3.36. Deverá implementar os protocolos NTP para atualização de horário.

7.10.3.37. Toda comunicação entre a controladora wireless e o ponto de acesso deve ser criptografado.

7.10.3.38. Deverá suportar a configuração de no mínimo 4.000 (quatro mil) VLANs ativas.

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

7.10.3.40. Deverá implementar, pelo menos, os seguintes padrões de segurança *wireless*:

- Wi-Fi *Protected Access* (WPA) com algoritmo de criptografia TKIP (*Temporal Key Integrity Protocol*);
- Wi-Fi *Protected Access 2* (WPA2) - Enterprise com os seguintes algoritmos: AES mínimo de 128bits (WPA2-AES);

7.10.3.41. Deve implementar os seguintes mecanismos de autenticação:

- Personal (PSK - Pre-Shared Key)
- Enterprise (IEEE 802.1x/EAP)

7.10.3.42. Deverá implementar o protocolo IEEE 802.1x com associação dinâmica de usuário a VLAN com base nos parâmetros da etapa de autenticação fornecidos por servidor RADIUS, com pelo menos os seguintes métodos EAP:

- EAP - Flexible Authentication via Secure Tunneling (EAP-FAST) ou EAP - Tunneled Transport Layer Security (EAP- TTLS);
- PEAP - Microsoft Challenge Authentication Protocol Version 2 (PEAP- MSCHAPv2);
- EAP-Transport Layer Security (EAP-TLS), suportando terminação do túnel EAP.

7.10.3.43. Deverá possuir a funcionalidade capaz de fazer a admissão de novos usuários de acordo com sua capacidade de operação para permitir a maior dispersão de usuários e melhoria nas condições de RF e performance nas faixas de frequência de 2.4GHz e 5GHz, ou seja, a controladora deve escolher sem intervenção do usuário ou administrador, em qual frequência o usuário se conectará, de acordo com hardware disponível do usuário e condições de rede, independente do SSID que o usuário estará conectando-se.

7.10.3.44. Deverá implementar os seguintes controles/filtros:

- L3 - Baseado em endereço IP;
- L4 - Baseado em portas TCP/UDP;
- L7 - Baseado na Identificação de Aplicações.

7.10.3.45. Deverá permitir a autenticação para acesso dos usuários conectados nas redes WLAN (wireless LAN)

- MAC Address;
- Base interna do equipamento;
- Portal de autenticação;
- RADIUS;
- IEEE 802.1x;
- LDAP;
- *Microsoft Active Directory*.

- *MAC Address-Spoofing;*
- *Adhoc.*

7.10.3.48. Deverá permitir prevenção e contenção de *Access Points* intrusos não autorizados (*rogues*), de forma integrada e automática, classificando-os como conhecidos, maliciosos e ou não autorizados e não classificados.

7.10.3.50. Deverá ajustar automaticamente a potência dos *Access Points* para eliminar lacunas de cobertura e otimizar o desempenho de RF. Deve ser possível desabilitar o ajuste de potência e ajuste de canal automático;

7.10.3.52. Deverá implementar filtragem de pacotes (ACL - *Access Control List*) pelo menos para IPv4, incluindo endereço IP de origem e destino, portas TCP e UDP de origem e destino.

7.10.3.54. Deverá permitir a identificação de qual ponto de acesso o usuário está conectado.

7.10.3.56. Deverá implementar funcionalidades de wIDS com intuito de controlar e identificar tentativas de ataques a rede WLAN, implementando mecanismos contra-ataques tipo *Auth Flood*, *Deauth Flood*, *EAPOL Flood* e *Broadcast Deauth*;

7.10.3.58. Deverá possuir mecanismo de autenticação entre cliente móvel e ponto de acesso para evitar ataques de camada 2 com foco em pacotes de gerenciamento como *association* e *disassociation*.

7.10.3.60. Deverá ajustar automaticamente os canais de modo a otimizar a cobertura de rede e mudar as condições de RF baseado em performance.

7.10.3.61. Deverá detectar, classificar e mitigar, de forma automática, as interferências não Wi-Fi que impactem diretamente no funcionamento da rede.

7.10.3.62. Deverá possuir recursos para implementar balanceamento de carga de usuários, de modo automático através de múltiplos *Access Points* para otimizar a performance durante elevada utilização da rede.

- WMM (Wi-Fi Multimedia);
- U-APSD (*Unscheduled Automatic Power Save Delivery*).

7.10.3.64. Deverá possuir mecanismo automático de Qualidade de Serviço (*QoS*) para protocolos de voz, utilizando inspeção automática de pacotes, sem a necessidade de fazer a marcação prévia (*tagging*) de pacotes ou por prioridades baseado na porta TCP com protocolo SVP.

7.10.3.65. Deverá implementar QoS com a marcação de pacotes utilizando Diffserv e suporte a 802.1p para QoS de rede, para otimização de aplicações sensíveis, como por exemplo, VoIP, videoconferência dentre outros.

7.10.3.66. Deverá possibilitar roaming com integridade de sessão, dando suporte a aplicações em tempo real, tais como, VoIP, VoWLAN e videoconferência.

7.10.3.67. Deverá implementar *roaming* (deslocamento) baseado nos protocolos IEEE 802.11r, 802.11k e 802.11v.

7.10.3.68. Deverá permitir visibilidade e controle das aplicações, permitindo a priorização de aplicações críticas, redução na prioridade de aplicações menos críticas e o bloqueio de aplicações não permitidas já na camada de acesso.

7.10.3.69. Deverá implementar detecção de ataques de RF e prevenção de intrusão para ajudar o administrador a detectar rapidamente ataques de RF *Denial of Service (DoS)*.

7.10.3.70. Deverá ter a capacidade de identificação automática de novos *Access Points* inseridos na rede e realizar o comissionamento do equipamento remotamente.

7.10.3.71. Deverá permitir a atualização de *software* de cada *Access Point* de forma remota, individualizada ou em grupos de atualização.

7.10.3.72. As funcionalidades descritas, sejam elas integrais ou parciais, poderão ser implementadas por qualquer componente da solução (*Access Points*, controladora, solução de gerenciamento, monitoramento ou controle de acesso) ou pela combinação entre eles, desde que atendam aos requisitos especificados nesta contratação.

7.10.4. **REQUISITOS DA SOLUÇÃO DE GERÊNCIA, MONITORAMENTO E SISTEMA DE CONTROLE DE ACESSO À REDE - NAC**

GERÊNCIA E MONITORAMENTO

7.10.4.1. Deverá gerenciar todos os *Access Points* e a controladora, especificados nesta solução de rede Wi-Fi, sendo todos os itens envolvidos fornecidos pelo mesmo fabricante.

7.10.4.2. Deverá permitir acesso à interface gráfica através de navegador padrão por protocolo HTTPS, compatível com os principais *browsers* do mercado (Edge, Firefox e Chrome), garantido que o acesso aos recursos das controladoras e *Access Points* sejam feito por meio de conexão segura para controle de todas as funcionalidades dos equipamentos de forma unificada.

7.10.4.3. Deverá permitir o direcionamento de eventos e logs para um servidor de *syslog*, além de permitir a visualização dos eventos em própria ferramenta indicando pelo menos a severidade, IP do equipamento, mensagem, data e horário do evento.

7.10.4.4. Deverá permitir a criação e distribuição dos arquivos de configuração dos equipamentos gerenciados na solução de rede Wi-Fi.

7.10.4.5. Deverá possibilitar configuração de *templates* para replicação das configurações entre equipamentos.

7.10.4.6. Deverá realizar gerência das configurações, com armazenamento de versões e suporte a *rollback* das configurações.

7.10.4.7. Deverá ter a capacidade de configuração por interface gráfica completa dos recursos das controladoras e dos *Access Points*.

7.10.4.8. Deverá ser possível a verificação contínua de conformidade de configuração (*compliance check*) dos dispositivos de rede, permitindo garantir que todos os elementos da infraestrutura estejam alinhados às políticas operacionais, requisitos de segurança e padrões definidos pelo HUB-UnB.

7.10.4.9. Deverá oferecer suporte à delegação de papéis, permitindo que os administradores atribuam permissões específicas a usuários ou grupos com base tanto no papel funcional (ex: administrativo, assistencial, aluno, docente, etc.) quanto na localização física ou lógica da rede.

7.10.4.10. Deverá permitir a criação de grupos de equipamentos para realização de configurações específicas para cada grupo.

7.10.4.11. Deverá permitir a importação de plantas baixas nos seguintes formatos CAD (.dwg e .dxf) ou não-CAD (imagens em JPG, PNG ou arquivos em PDF).

7.10.4.12. Deverá implementar recursos de descoberta automática dos dispositivos individuais da infraestrutura de rede Wi-Fi, permitindo filtros de rede e sub-rede, endereço IP específico e intervalo de endereços IP, incluindo-os em uma lista de dispositivos descobertos.

7.10.4.13. Deverá monitorar o desempenho da rede Wi-Fi, consolidando informações de níveis de ruído, relação sinal-ruído, utilização de canais, número de cliente conectados, interferência e potência de sinal.

7.10.4.14. Deverá elaborar mapa da topologia da rede, automaticamente e baseado nas informações das regras definidas durante o processo de descoberta dos dispositivos ou através da atualização das informações dos dispositivos no inventário.

7.10.4.15. Deverá permitir a visualização detalhada das informações dos dispositivos apresentados nos mapas e da topologia selecionando por área, prédio ou andar.

7.10.4.16. Deverá representar o mapa lógico da rede sem fio, identificando e monitorando equipamentos, realizando o relacionamento dos eventos e estado operacional, com sinalização por cores.

- 7.10.4.17. Deverá permitir salvar as alterações efetuadas no layout para uma visão completa da topologia.
- 7.10.4.18. Deverá identificar eventos e alertas em tempo real, com indicação da severidade e separação por cores.
- 7.10.4.19. Deverá possibilitar a configuração de alertas, sendo possível designar que determinado evento seja de responsabilidade de um usuário ou área, determinado previamente.
- 7.10.4.20. Deverá permitir o monitoramento em tempo real de informações de disponibilidade, utilização de CPU, memória e estatísticas de rede e rádio.
- 7.10.4.21. Deverá fornecer relatórios gráficos contendo as informações dos subitens abaixo em tempo real ou demanda:
- Tipos de dispositivos;
 - Fabricante do dispositivo;
 - Sistema Operacional;
 - Endereço IP associado;
 - Informação detalhada dos usuários;
 - Políticas em uso;
 - Regras de Controle de Acesso.
- 7.10.4.22. Deverá implementar funcionalidades de Classificação Automática de Dispositivos (“*Device profiling*”), de forma a descobrir, classificar e agrupar os dispositivos conectados na rede, permitindo extrair informações de contexto que devem ser usadas na aplicação de políticas de acesso;
- 7.10.4.23. Deverá permitir a atualização das categorias de Classificação de Dispositivos, pelo fabricante;
- 7.10.4.24. Deverá permitir que o administrador cadastre manualmente um determinado dispositivo em uma categoria.
- 7.10.4.25. Deverá possuir base de regras e categorias de dispositivos pré-configurada;
- 7.10.4.26. Deverá suportar mecanismo de atualização das regras e categorias pré configuradas;
- 7.10.4.27. Deverá permitir a identificação de áreas sem cobertura de sinal (*coverage holes*) com capacidade para efetuar os devidos ajustes para a correção automática das áreas de sombras.
- 7.10.4.28. Deverá possibilitar a visualização de informações de clientes conectados à rede Wi-Fi, tais como: endereço IP, endereço MAC, nome do usuário, SSID, ponto de acesso, dados de associação e de autenticação 802.1x.
- 7.10.4.29. Deverá permitir a identificação de falhas no processo de autenticação/associação dos clientes na rede Wi-Fi, para possibilitar a identificação de forma ágil na autorização de acesso dos usuários/clientes.
- 7.10.4.30. Deverá armazenar informações históricas sobre autenticação de usuários da rede sem fio, tanto da rede corporativa (802.1x) como da rede visitante.
- 7.10.4.31. Deverá implementar solução para localização dos elementos irradiantes (*Access Points*) presentes na área de cobertura da rede Wi-Fi.
- 7.10.4.32. Deverá permitir a identificação e listagem dos rádios vizinhos e respectivos SSID/BSSID.
- 7.10.4.33. Deverá permitir a detecção e localização de equipamentos/SSID, bem como o bloqueio de *Access Points* não autorizados (*rogues*) e redes *ad-hoc*.
- 7.10.4.34. Deverá permitir a identificação e geração de alertas para eventos indicativos de ataques na rede sem fio.
- 7.10.4.35. Deverá permitir a visualização das seguintes informações:
- Listagem de clientes da rede Wi-Fi;
 - Listagem de *Access Points*;
 - Informações de configuração das controladoras Wi-Fi;
 - Utilização da rede;
 - Detalhes dos *Access Points* estranhos detectados (*rogue*).
- 7.10.4.36. Deverá permitir a visualização das informações de toda a rede, tais como, alertas gerais, interferências de RF e localização de *Access Points rogues*, devendo ser apresentadas em console único.
- 7.10.4.37. Deverá permitir, a partir da identificação das aplicações, definir ações para classes de tráfego específico, como realizar marcação de pacote com *tags* ou DSCP e alocação de banda.
- 7.10.4.38. Deverá fornecer modelos de relatórios para geração automática ou possibilidade de criação personalizada de relatórios e filtros.
- 7.10.4.39. Deverá fornecer maneiras para solução de problemas relacionados à rede, aos clientes e às aplicações, devendo possuir no mínimo as seguintes funcionalidades identificadas por cores representativas e diferenciadas da situação da rede, com no mínimo os seguintes status:
- Problemas Críticos;
 - Problemas que necessitam serem verificados;
 - Nenhum problema;

- Não existem informações coletadas;

7.10.4.40. Deverá apresentar o histórico dos principais problemas e eventos críticos ocorridos no período dos últimos 14 dias.

7.10.4.41. Deverá possuir base de conhecimento capaz de indicar ações para remediar problemas e detalhar qual o seu impacto no ambiente.

7.10.4.42. Deverá possibilitar que os dispositivos gerenciados enviem informações de telemetria diretamente à plataforma de gerência e monitoramento, sem a necessidade de coleta.

7.10.4.43. Deverá incluir mecanismos de análise, para identificar, correlacionar e prever problemas de conectividade e desempenho a partir da coleta de métricas como:

- Tempo de associação Wi-Fi;
- Falhas de DHCP e DNS;
- Retransmissões e perda de pacotes;
- Qualidade de aplicações prioritárias;

7.10.4.44. Deverá suportar Gerenciamento Dinâmico de Recursos de Rádio (*Dynamic Radio Resource Management - DRRM*) de forma autônoma, com base em dados coletados em tempo real do histórico do ambiente, oferecendo:

- Otimização contínua dos canais e potência de transmissão das redes Wi-Fi;
- Reação automática a interferências internas e externas;
- Detecção de áreas com cobertura deficiente ou excessiva;
- Equilíbrio de carga entre *Access Points* (*load balancing*);
- Redução interferência para melhorar a eficiência espectral.

7.10.4.45. Deverá oferecer mecanismos avançados de segurança para redes sem fio, com foco na prevenção de intrusões, detecção de ameaças e mitigação de dispositivos não autorizados.

7.10.4.46. Deverá possuir integração com o sistema de Controle de Acesso à Rede, para garantia que as políticas de segurança sejam aplicadas à infraestrutura Wi-Fi e assim efetuar todas as configurações que sejam necessárias para implementação das políticas para acesso dos clientes aos recursos da Rede (cabeadas ou sem fio).

7.10.4.47. Deverá suportar a análise contínua da latência e perda de pacotes, permitindo identificar se um problema está na rede interna ou externa.

7.10.4.48. Deverá implementar ferramentas de *troubleshooting* para análise de falhas nas conexões de clientes ou dispositivos com dificuldade de se conectarem à rede Wi-Fi.

7.10.4.49. Deverá possuir a capacidade de desativação e reativação de determinada rede sem fio.

7.10.4.50. Deverá permitir a configuração de administradores de recursos da rede Wi-Fi com diferentes visões administrativas.

7.10.4.51. Deverá realizar o monitoramento e o inventário dos dispositivos da rede Wi-Fi, com no mínimo as seguintes informações:

1. Nome do dispositivo;
2. Endereço IP;
3. Status do dispositivo;
4. Endereço MAC;
5. Versão de software;
6. Número de série;
7. Modelo do dispositivo (*Part-number*);
8. Tempo que o dispositivo está ativo e operacional;
9. Localização geográfica do dispositivo;

7.10.4.52. Deverá permitir que os *Access Points* sejam gerenciados pelo controlador Wi-Fi por meio de túnel seguro que ofereça controle total dos equipamentos.

7.10.4.53. Deverá permitir o ajuste dinâmico de nível de potência dos rádios de modo a otimizar o tamanho da célula de RF.

7.10.4.54. Deverá possuir a capacidade de selecionar faixas de frequências diferentes (2.4Ghz, 5Ghz) de acordo com as requisições dos clientes da rede Wi-Fi para que se associem ao ponto de acesso de forma eficiente.

7.10.4.55. As funcionalidades descritas, sejam elas integrais ou parciais, poderão ser implementadas por qualquer componente da solução (*Access Points*, controladora, solução de gerenciamento, monitoramento ou controle de acesso) ou pela combinação entre eles, desde que atendam aos requisitos especificados nesta contratação.

SISTEMA DE CONTROLE DE ACESSO À REDE (NAC)

7.10.4.56. Deverá implementar solução de controle de acesso de usuários para que haja perfeito funcionamento do processo de autenticação, autorização, manutenção dos registros e categorização dos usuários conforme especificações

definidas pela CONTRATANTE.

7.10.4.57. Deverá permitir a criação de páginas personalizadas para o *captive portal*, com a inclusão de imagens, instruções em texto e campos de texto que possam ser preenchidos pelos clientes.

7.10.4.58. Deverá implementar associação dinâmica de usuário à VLAN com base nos parâmetros da etapa de autenticação via IEEE 802.1x.

7.10.4.59. Deverá implementar protocolo de autenticação para controle do acesso de usuários da rede HU Brasil à solução utilizando servidor RADIUS.

7.10.4.60. Deverá detectar, em conjunto com a controladora Wi-Fi e com o *Access Point*, pelo menos, os seguintes ataques: *flood* de autenticação e *spoofed* MAC.

7.10.4.61. Deverá gerenciar, de forma centralizada, a autenticação de usuários e dispositivos, permitindo a autenticação pelo menos através dos seguintes métodos:

- a) Local por tipo de usuário;
- b) Local por tipo de dispositivo;
- c) RADIUS;
- d) LDAP;
- e) *Microsoft Active Directory*;

7.10.4.62. Deverá implementar autenticação de dispositivos e usuários utilizando o padrão IEEE 802.1x, suportando pelo menos os seguintes métodos EAP: EAP-TLS, PEAP ou superiores.

7.10.4.63. Deverá permitir a customização de atributos de autorização de acesso condicional com base nos seguintes fatores:

- a) Atributos LDAP do usuário autenticado;
- b) Grupo de *Active Directory* do usuário autenticado;
- d) Meios de acesso;
- e) Localização;
- f) Tipo de dispositivo (exemplo: iPad, iPhone, Android, Windows, Mac OS).

7.10.4.64. Deverá oferecer autenticação de usuários através de portal web seguro HTTPS com redirecionamento automático.

7.10.4.65. Deverá implementar autenticação específica para dispositivos baseado em endereço MAC.

7.10.4.66. Deverá ter uma base de dados interna para registrar dispositivos pelo endereço MAC. Deve ser permitindo que tal base seja pré-preenchida automaticamente por meio de um mecanismo automático de detecção de perfil do dispositivo.

7.10.4.67. Deverá implementar validação de certificados digitais atendendo as seguintes características:

- a) Suportar o cadastramento de pelo menos um CA (*Certificate Authority*) externo;
- b) Suportar consulta periódica da lista de revogados CRL (*Certificate Revocation List*) via HTTP;
- c) Suportar o protocolo OCSP para verificação do estado do certificado.

7.10.4.68. Deverá permitir a customização de usuários visitantes (*guests*), podendo atribuir privilégios de acesso distintos à rede Wi-Fi.

7.10.4.69. Deverá permitir, durante a criação da conta de usuário visitante, a definição da validade temporal da conta e níveis de acesso.

7.10.4.70. Deverá permitir a customização do formulário, de auto registro, com os campos e informações necessários para criação do acesso visitante (*guest*), tais como:

- Nome (obrigatório);
- Sobrenome (obrigatório);
- E-mail (obrigatório);
- Empresa (opcional);
- Telefone (obrigatório);
- CPF (obrigatório).

7.10.4.71. Deverá implementar a importação e exportação da relação de credenciais temporárias através de arquivos txt, csv ou xls.

7.10.4.72. Deverá implementar a funcionalidade de geração aleatória de lotes de credenciais temporárias.

7.10.4.73. Deverá permitir a customização do nível de segurança da senha temporária que será gerada ao visitante, especificando a quantidade mínima de caracteres, quantos caracteres especiais e quantos números serão utilizados para compor a senha temporária.

7.10.4.74. Deverá fornecer, no mínimo, os seguintes modelos de criação de usuários visitantes (*guest*):

- a) Permitir que grupos de usuários corporativos autorizados possam criar contas de usuários

visitantes com os seguintes requisitos:

- Criar conta individual;
- Enviar senha via e-mail;
- Definir a senha do visitante;
- Ver, editar ou suspender contas criadas pelo próprio autorizador, pelo mesmo grupo autorizador e por outros grupos autorizadores;
- Estabelecer duração máxima da conta visitante;
- Especificar o perfil de acesso à rede que será atribuído a conta visitante;

b) Deverá permitir o auto-cadastramento ou “*self-registration*”, direcionando o visitante para página web integrada com o GOV.BR onde o próprio usuário cria seu acesso de visitante na rede Wi-Fi, sem necessidade de autorizador. Para atendimento deste item, poderá ser utilizada solução open source ou solução proprietárias que ofereçam a mesma integração de forma a atender o requisito.

c) Deverá permitir o auto-cadastramento ou “*self-registration*” por meio de integração com logins sociais do Google e Facebook (Meta) e outros.

d) Deverá implementar um portal web seguro SSL a ser apresentado automaticamente aos usuários temporários (visitantes) durante a sua conexão com a rede (*hotspot*);

e) Deverá implementar pelo menos as seguintes funções no Portal Web (*hotspot*):

- Exigir a cada login na rede o aceite do “termo de uso aceitável de rede”; ou
- Exigir somente no primeiro login o aceite do “termo de uso aceitável de rede”; ou
- Customização da página de “termo de uso aceitável de rede”;

7.10.4.75. Deverá implementar um mecanismo flexível de regras que permita selecionar o banco de dados onde um usuário e/ou dispositivo serão autenticados com base em atributos RADIUS existentes na solicitação enviada pelo equipamento de rede e tipo de protocolo, permitindo pelo menos a seguinte combinações de regras:

- Com fio 802.1x
- Wireless 802.1x
- Autenticação sem 802.1x

7.10.4.76. Deverá ser possível obter informações de outros sistemas para realizar a identificação passiva de usuários, através de protocolos / especificações, como *syslog* e API REST.

7.10.4.77. Deverá ser possível fornecer informações para a identificação passiva de usuários em outros sistemas através de uma API.

7.10.4.78. Deverá permitir a criação e aplicação de políticas de controle de acesso à rede baseada em IP ou em grupos de usuários;

7.10.4.79. Deverá ser capaz de traduzir as políticas em configurações necessárias e aplicá-las automaticamente em diferentes tipos de equipamentos;

7.10.4.80. Deverá permitir criar através de uma interface gráfica políticas de micro segmentação dentro das redes virtuais;

7.10.4.81. Deverá permitir a criação e aplicação de políticas de aplicações, configurando QoS na rede;

7.10.4.82. Deverá permitir que a autenticação dos dispositivos móveis seja efetuada por software de controle de acesso.

7.10.4.83. Deverá implementar as seguintes funcionalidades:

- AAA: 802.1x, designação de VLAN por DACL, *Downloadable-ACL* ou *Dynamic ACL*.
- Implementar RADIUS CoA (*Change of Authorization*) - RFC 5176.
- Suportar BYOD: RADIUS CoA, Redirecionamento de URL.

7.10.4.84. Deverá implementar mecanismo de descobrimento automático e transparente de dispositivos que se conectam a rede Wi-Fi e cabeada classificando-os nas seguintes categorias:

- Tablet e/ou *Smart Device*;
- Impressora;
- Telefone IP;
- *Workstation*;
- Dispositivo IoT

7.10.4.85. Deverá implementar os seguintes mecanismos para coleta de informações do dispositivo a ser utilizada na construção das regras de classificação.

- Coleta do tráfego DHCP e HTTP enviado pelo dispositivo;
- Coleta de tráfego *NetFlow* ou *sFlow*;
- Coleta dos atributos RADIUS referente a sessão 802.1X do dispositivo;
- Consulta SNMP ao switch de acesso ou controlador wireless;
- Consulta DNS ou coleta do tráfego para identificação do nome do dispositivo;

- Coleta de informações do dispositivo no *Active Directory*.

7.10.4.86. Deverá possuir interface para construção de regras customizadas de classificação de dispositivo com suporte a operadores lógicos;

7.10.4.87. Deverá Possuir uma base de regras e categorias pré-configuradas;

7.10.4.88. Deverá suportar mecanismo de atualização das regras e categorias pré-configuradas;

7.10.4.89. Deverá permitir que a classificação do dispositivo descoberto seja utilizada como parâmetro de autorização nas regras de admissão de dispositivos;

7.10.4.90. Deverá permitir que o administrador cadastre manualmente um determinado dispositivo numa categoria;

7.10.4.91. Deverá suportar a criação de regras para diferenciação de dispositivos corporativos e pessoais, possibilitando a adoção de políticas de “BYOD (*Bring Your Own Device*)”;

7.10.4.92. Deverá fornecer um portal para os usuários registrarem e gerenciarem seus próprios dispositivos para uso na rede. O auto-registro de dispositivos dos usuários deverá suportar o provisionamento de um certificado digital ou agente que identifique o dispositivo BYOD e sirva como um método de autenticação para a rede com fio e sem fio.

7.10.4.93. Deverá possuir uma Autoridade Certificadora interna para o provisionamento e gerenciamento de certificados digitais para dispositivos BYOD.

7.10.4.94. Deverá ser possível suspender/reactivar dispositivos e revogar certificados a partir da interface de gerência da solução.

7.10.4.95. Deverá permitir a configuração de políticas distintas para usuários “on-line” (quando o usuário está dentro e/ou comunicando-se remotamente com a rede corporativa) e “offline” (quando o usuário está fora e/ou desconectado da rede corporativa) e permitir herança de políticas por grupos.

7.10.4.96. Deverá permitir o controle do acesso de usuários que se conectem na rede corporativa interna via LAN, WLAN e VPN;

7.10.4.97. Deverá implementar autenticação via portal web para os usuários da rede wireless que não puderem se autenticar via 802.1X;

7.10.4.98. Deverá implementar controle de acesso administrativo a dispositivos de rede com, no mínimo, os seguintes requisitos:

- Registrar para fins de auditoria, todas as tentativas de acesso administrativos efetuadas. Devem ser registradas, no mínimo, as seguintes informações: usuário autenticado e grupo a que pertence, IP a partir do qual se solicitou o acesso, dispositivo em que solicitou acesso administrativo (incluindo endereço IP), horário de início e término da conexão, comandos de configuração executados.
- Registrar todas as falhas de autenticação (nas tentativas de acesso administrativo), assim como as falhas de autorização (tentativas de execução de comandos não permitidos para um dado usuário).

7.10.4.99. As funcionalidades descritas, sejam elas integrais ou parciais, poderão ser implementadas por qualquer componente da solução (*Access Points*, controladora, solução de gerenciamento, monitoramento ou controle de acesso) ou pela combinação entre eles, desde que atendam aos requisitos especificados nesta contratação.

7.10.5. REQUISITOS GERAIS DOS ACCESS POINTS TIPO 1 E TIPO 2

7.10.5.1. Deverá ser do tipo *thin Access Point*, ou seja, ponto de acesso (*Access Point*) que permita acesso à rede *ethernet* via rede Wi-Fi e que possua todas as suas configurações centralizadas nas controladoras wireless.

7.10.5.2. Deverão ser compatíveis com, no mínimo, o padrão Wi-Fi 6 (IEEE 802.11ax) ou superior.

7.10.5.3. Deverão ser compatíveis e totalmente gerenciáveis pela solução de controle, gerenciamento e monitoramento, obrigatoriamente do mesmo fabricante dos *Access Points*.

7.10.5.4. Deverão suportar os seguintes padrões IEEE:

- 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ax, com configuração via software.

7.10.5.5. Deverão operar simultaneamente nas bandas 2.4GHz, 5GHz, com rádios independentes.

7.10.5.6. Deverão se associar automaticamente à controladora Wi-Fi.

7.10.5.7. Deverão conectar-se à controladora WLAN através de protocolo de túnel seguro.

7.10.5.8. Deverão suportar:

- VLANs (IEEE 802.1q);
- Autenticação via *MAC Address*, *Captive Portal*, 802.1x (base local, RADIUS ou LDAP);
- Integração com RADIUS Server.

7.10.5.9. Deverão implementar os seguintes padrões de segurança:

- WPA2 (AES 128 bits);
- WPA3 Enterprise, WPA3 Enterprise 192, WPA3 Enhanced Open (OWE);
- IEEE 802.1x com suporte a EAP-FAST/TLS/TTLS/GTC/MSCHAPv2;
- IEEE 802.11i.

7.10.5.10. Deverão suportar mecanismos de roaming seguro e otimizado:

- IEEE 802.11r, 802.11k, 802.11v;
- Fast Secure Roaming com 802.1x;

7.10.5.11. Deverá implementar o protocolo de controle CAPWAP ou equivalente.

7.10.5.12. Deverão permitir alimentação por PoE nos padrões IEEE 802.3at (PoE+) ou 802.3bt, com todas as funcionalidades especificadas ativas mesmo sob PoE.

7.10.5.13. Deverão possuir interface de gerenciamento via CLI, com RJ-45 ou USB (A, B, C – em suas variantes). Cabos proprietários serão aceitos, desde que uma das pontas utilize padrões citados.

7.10.5.14. Deverão possuir pelo menos 1 porta LED indicadora de status operacional.

7.10.5.15. Deverão possuir todos os acessórios originais necessários para instalação em teto ou parede.

7.10.5.16. Deverão permitir ajuste dinâmico de potência e canal, otimizando a célula de cobertura conforme ambiente.

7.10.5.17. Deverão permitir seleção automática de canal, com capacidade de resposta a interferência.

7.10.5.18. Deverão possuir suporte a:

- *Beamforming*;
- *Band Steering* (preferência por bandas 5GHz);
- DFS (*Dynamic Frequency Selection*);
- Uplink / Downlink OFDMA (*Orthogonal Frequency Division Multiplexing*);
- Uplink / Downlink MU-MIMO;
- BSS coloring;
- TWT (*Target Wake Time*);
- IEEE 802.11h e 802.11e (WMM para QoS de voz e vídeo em tempo real);
- Limitação de banda por SSID ou grupo de usuários.

7.10.5.19. Deverão suportar à análise de espectro em 2.4GHz e 5GHz, com acesso remoto à análise e captura de espectro.

7.10.5.20. Deverão possuir capacidade de operar como sensor de RF (modo monitor), isoladamente ou em conjunto com o modo cliente, para:

- Otimização de RF;
- Detecção de interferências 802.11 e não Wi-Fi;
- Identificação e contenção de dispositivos intrusos (*rogue APs*);
- Mitigação de interferência e alteração automática de canais.

7.10.5.21. Deverão implementar tecnologia de *Maximum Ratio Combining* (MRC) ou equivalente.

7.10.5.22. Deverão implementar técnica *Cyclic Shift Diversity* (CSD) para melhorar desempenho das múltiplas antenas.

7.10.5.23. Deverão permitir integração e gerenciamento centralizado de dispositivos BLE (*Bluetooth Low Energy*) através da mesma plataforma de gerência da rede Wi-Fi.

7.10.5.24. Deverão suportar comunicação BLE em conformidade com os padrões **Bluetooth 5.0 ou superior**, garantindo alcance, eficiência energética e taxa de transmissão adequados para ambientes corporativos.

7.10.5.25. Deverão implementar medidas de segurança para comunicação BLE, incluindo autenticação, criptografia e prevenção contra-ataques de *spoofing* ou rastreamento não autorizado.

7.10.5.26. Deverão fornecer APIs ou integração para aplicações de localização *indoor*, autenticação de proximidade e análise de dados de dispositivos BLE.

7.10.5.27. Deverão permitir que os *Access Points* que suportam BLE funcionem simultaneamente como "pontos de acesso" Wi-Fi e sensores BLE, sem perda de desempenho em nenhuma das funções ou degradação de performance.

7.10.5.28. Deverão possibilitar bloqueio de tráfego lateral entre dispositivos no mesmo SSID.

7.10.5.29. Deverão permitir desativar a divulgação de SSID e criar célula para visitantes (*Guest SSID*).

7.10.5.30. Deverão possuir Firmware homologado pelo fabricante, com suporte a atualizações remotas.

7.10.5.31. Deverão suportar o protocolo SNMPv2c com MIBs para integração com soluções de monitoramento.

7.10.5.32. Em caso de falha de comunicação com a controladora, o *Access Point* deverá manter conectividade funcional

com usuários autenticados, incluindo funções como roteamento, QoS e autenticação local.

7.10.5.33. A comprovação dos requisitos poderá ser realizada por meio de documentação técnica do fabricante, *datasheets*, manuais ou certificados oficiais, inclusive se as funcionalidades estiverem na controladora ou gerenciador central, desde que acessíveis pelo *Access Point*.

7.10.5.34. As funcionalidades descritas, sejam elas integrais ou parciais, poderão ser implementadas por qualquer componente da solução (*Access Points*, controladora, solução de gerenciamento, monitoramento ou controle de acesso) ou pela combinação entre eles, desde que atendam aos requisitos especificados nesta contratação.

7.10.6. REQUISITOS ESPECÍFICOS DOS ACCESS POINTS TIPO 1 (Moderado – Áreas Comuns)

7.10.6.1. Deverão possuir antenas internas omnidirecionais compatíveis com as frequências 2.4GHz, 5GHz, conforme o padrão IEEE 802.11ax, com potência mínima de transmissão de 23 dBm nas frequências acima, com *beamforming* e ajuste automático de potência.

7.10.6.2. No caso de falhas de comunicação entre o ponto de acesso e a controladora Wi-Fi, o ponto de acesso, em conjunto com os demais componentes do sistema, deverá manter todos os usuários e/ou equipamentos, previamente autenticados, com conectividades a rede sem fio, mantendo todas as funcionalidades;

7.10.6.3. Deverão ser compatíveis com o padrão IEEE 802.11ax e canais com largura de 20, 40, 80, 160 MHz (HE 20/40/80/160 ou HE 20/40/80/80+80).

7.10.6.4. Deverão suportar no mínimo: 1000 VLANs (IEEE 802.1q) e 15 SSIDs ou mais.

7.10.6.5. Deverão suportar no mínimo 100 dispositivos conectados, simultâneos por *Access Point*, sem degradação da qualidade.

7.10.6.6. Deverão possuir suporte a tecnologia MU-MIMO 4x4:4 (quatro transmissores, quatro receptores e quatro fluxos espaciais) no rádio de 5 GHz, conforme padrão IEEE 802.11ac Wave 2 ou superior.

7.10.6.7. Deverão possuir suporte a tecnologia MU-MIMO 2x2:2 (dois transmissores, dois receptores e dois fluxos espaciais) no rádio de 2,4 GHz, conforme padrão IEEE 802.11n ou superior.

7.10.6.8. Deverão oferecer taxa de transferência agregada mínima de 1 Gbps, considerando a soma das capacidades máximas teóricas nas bandas de 2,4 GHz e 5 GHz.

7.10.6.9. Deverão possuir pelo menos 1 (uma) interface de rede 1000BASE-T Gigabit Ethernet, compatível com IEEE 802.3af/at PoE, com detecção automática de velocidade (*auto-sensing*), detecção automática de polaridade (auto MDI/MDX) e conector RJ-45, para conexão à rede local.

7.10.6.10. Deverão suportar operação simultânea de 2,4 GHz e 5 GHz (*dual concurrent*).

7.10.6.11. Deverão implementar WPA2 Enterprise, garantindo a segurança dos usuários e dispositivos conectados.

7.10.6.12. Deverão possuir balanceamento automático de carga por SSID, *band steering*, controle automático de potência e seleção automática de canal, para otimização do desempenho em ambientes de alta densidade de usuários.

7.10.6.13. Deverão permitir VLAN *tagging* e configuração de QoS, para priorização de tráfego sensível, como voz e vídeo.

7.10.6.14. Deverão possuir Gerenciamento Dinâmico de Recursos de Rádio (*Dynamic Radio Resource Management – RRM*), incluindo ajuste automático de potência de transmissão, seleção de canal, largura de canal, balanceamento de carga, *band steering* e mitigação de interferências, garantindo otimização contínua da cobertura, capacidade e desempenho da rede Wi-Fi sem necessidade de intervenção manual.

7.10.6.15. Deverão suportar a gerência centralizada, atualização de firmware remota, monitoramento de desempenho e integração com controladoras e soluções de gerenciamento do mesmo fabricante da solução de rede Wi-Fi, garantindo interoperabilidade total.

7.10.7. REQUISITOS ESPECÍFICOS DOS ACCESS POINTS TIPO 2 (Robusto – Auditórios ou Alta Densidade)

7.10.7.1. Deverão possuir antenas internas omnidirecionais compatíveis com as frequências 2.4GHz e 5GHz, conforme o padrão IEEE 802.11ax, com potência mínima de transmissão de 23 dBm nas frequências acima, com *beamforming* e ajuste automático de potência.

7.10.7.2. No caso de falhas de comunicação entre o ponto de acesso e a controladora Wi-Fi, o ponto de acesso, em conjunto com os demais componentes do sistema, deverá manter todos os usuários e/ou equipamentos, previamente autenticados, com conectividades a rede sem fio, mantendo todas as funcionalidades;

7.10.7.3. Deverão ser compatíveis com os padrões IEEE 802.11ac Wave 2 e IEEE 802.11ax, suportando canais com largura de 20, 40, 80 e 160 MHz, incluindo HE 20/40/80/160 ou HE 20/40/80/80+80, para operação em bandas de alta eficiência.

- 7.10.7.4. Deverão suportar no mínimo 4000 VLANs (IEEE 802.1q) e 15 SSIDs ou mais.
- 7.10.7.5. Deverão suportar no mínimo 150 dispositivos simultâneos por *Access Point*, sem degradação da qualidade.
- 7.10.7.6. Deverão possuir suporte a MU-MIMO 4x4:4 no rádio de 5 GHz, com quatro fluxos espaciais, e MU-MIMO 2x2:2 no rádio de 2,4 GHz, com dois fluxos espaciais.
- 7.10.7.7. Deverão oferecer taxa de transferência agregada mínima de 2,5 Gbps nas bandas de 2,4 GHz e 5 GHz.
- 7.10.7.8. Deverão possuir pelo menos 1 (uma) interface 2.5GBASE-T *Multigigabit Ethernet, auto-sensing*, auto MDI/MDX, com conector RJ-45, compatível com PoE+ (IEEE 802.3at) ou superior, para conexão à rede local.
- 7.10.7.9. Deverão suportar operação simultânea de 2,4 GHz e 5 GHz (*dual concurrent*).
- 7.10.7.10. Deverão implementar WPA2 Enterprise, garantindo a segurança dos usuários e dispositivos conectados.
- 7.10.7.11. Deverão possuir balanceamento automático de carga por SSID, *band steering*, controle automático de potência e seleção automática de canal, para otimização do desempenho em ambientes de alta densidade de usuários.
- 7.10.7.12. Deverão permitir VLAN *tagging* e configuração de QoS, para priorização de tráfego sensível, como voz e vídeo.
- 7.10.7.13. Deverão possuir Gerenciamento Dinâmico de Recursos de Rádio (*Dynamic Radio Resource Management - RRM*), incluindo ajuste automático de potência de transmissão, seleção de canal, largura de canal, balanceamento de carga entre *Access Points*, *band steering* e mitigação de interferências, garantindo otimização contínua da cobertura, capacidade e desempenho da rede Wi-Fi sem necessidade de intervenção manual.
- 7.10.7.14. Deverão suportar a gerência centralizada, atualização de firmware remota, monitoramento de desempenho e integração com controladoras e soluções de gerenciamento do mesmo fabricante da solução de rede Wi-Fi, garantindo interoperabilidade total.

7.10.8. **REQUISITOS DOS INJETORES DE POTÊNCIA (POWER INJECTOR)**

- 7.10.8.1. Deverá ser da mesma marca da solução de rede Wi-Fi ou ser comprovadamente homologado pelo fabricante e ainda atender todas as especificações de garantias e demais exigências da solução de rede Wi-Fi.
- 7.10.8.2. Deverá permitir, pelo menos, o fornecimento de energia conforme o padrão IEEE 802.3at ou superior, provendo a potência necessária para que o *Access Point* possa ser alimentado sem perder nenhuma funcionalidade.
- 7.10.8.3. Deverá fornecer alimentação eficiente para cabos CAT 6 com pelo menos 100m;
- 7.10.8.4. Deverá possuir 2 (duas) interfaces de dados compatíveis com IEEE 802.3bz 100/1000/2500 Multigigabit Ethernet, com conectores RJ-45 fêmea, sendo uma interface de entrada para conexão com switch não PoE e uma interface de saída para fornecimento simultâneo de dados e energia ao *Access Point*. A interface de saída deverá ser compatível com o padrão IEEE 802.3bt.
- 7.10.8.5. Deverá acompanhar cabos e acessórios para o seu perfeito funcionamento, incluído cabo para conexão à rede elétrica no padrão brasileiro (NBR-14136);
- 7.10.8.6. Deverá operar em tensões nominais entre 110V e 220V, com comutação automática e frequência de 60Hz e proteção contra picos de energia.
- 7.10.8.7. Deverá ser compatível com os *Access Points* TIPO 1 e TIPO 2 ou qualquer outro modelo fornecido durante o período de garantia.

7.10.9. **REQUISITOS DE LEVANTAMENTO DE CAMPO (SITE SURVEY)**

- 7.10.9.1. A área interna total estimada das edificações de HUB-UnB, as quais serão objeto da contratação é de 50.000 m2, conforme Anexo I - Mapa preditivo Wi-Fi - HUB-UnB (55421234).
- 7.10.9.2. Após a Ordem de serviço de implantação a CONTRATADA, vencedora do item avulso (item 8) deverá elaborar um levantamento de campo prático (*site survey* prático) para definir os locais onde os *Access Points* serão de fato instalados.
- 7.10.9.3. Os locais e as quantidades indicadas deverão ser validadas pela equipe técnica da CONTRATANTE.
- 7.10.9.4. A execução do serviço de site survey prático deverá utilizar, obrigatoriamente, equipamento especializado em análise de espectro, específico para esta finalidade e comprovadamente calibrado, a fim de garantir a precisão das medições, a confiabilidade dos dados coletados e a correta identificação de interferências no ambiente.
- 7.10.9.5. O levantamento deverá ser executado de segunda a sexta-feira, das 08h00 às 18h00.
- 7.10.9.6. A CONTRATADA deverá atender, no mínimo, aos requisitos abaixo para a execução do site survey que subsidiará a instalação dos pontos de acesso (*Access Points*) da solução de rede Wi-Fi do HUB-UnB:

I - Considerar a cobertura total de todas as áreas internas das edificações do HUB-UnB, definidas pela CONTRATANTE, observando sempre a densidade de usuários por ponto de acesso, a existência de possíveis interferências eletromagnéticas e obstáculos físicos (paredes e metais), a fim de garantir cobertura contínua e desempenho adequado da rede sem degradação de sinal.

II - O site survey deverá contemplar a avaliação das frequências de 2.4GHz, 5GHz e 6GHz, afim de garantir a adequação aos itens a serem adquiridos no grupo 1.

III - Elaborar estudo de cobertura e capacidade, utilizando ferramentas e metodologias reconhecidas no mercado, com o bjetivo de definir os locais ideais de instalação dos *Access Points* e para assegurar dimensionamento preciso dos *Access Points* e evitar sub ou superdimensionamento da rede.

IV - Considerar cenários de alta densidade de usuários, requisitos de segurança e melhores práticas de redes Wi-Fi corporativas, com o objetivo de manter estabilidade, desempenho e conformidade com padrões atuais de segurança.

V - Apresentar relatório técnico completo com mapas de calor, recomendações de posicionamento dos *Access Points*, identificação de pontos críticos e infraestrutura necessária, para permitir validação técnica e correta execução da implantação.

VI - Utilizar software e equipamentos profissionais para medições de espectro, RSSI e interferências, garantindo precisão nas análises e confiabilidade dos dados coletados.

VII - Adotar metodologias compatíveis com padrões reconhecidos internacionalmente (ex.: IEEE, Wi-Fi Alliance), para assegurar padronização, interoperabilidade e qualidade técnica do levantamento.

VIII - Comprovar que os profissionais possuem certificação CWNA (CWNP) ou equivalente, a fim de garantir qualificação técnica adequada para execução do site survey.

IX - Entregar relatório técnico final, contendo:

- a) Mapa de calor com os dados e parâmetros de qualidade de sinal e a distribuição recomendada dos *Access Points*, para evidenciar a cobertura proposta;
- b) Tabelas informando quantidades de equipamentos por edificação, para subsidiar o dimensionamento e aquisição;
- c) Justificativa técnica para cada posicionamento, para demonstrar critérios objetivos de instalação;
- d) Recomendações de infraestrutura (energia, rede, suportes), para viabilizar a implantação física adequada;
- e) Outras informações consideradas úteis, para complementar a análise técnica.

X - Participar de, pelo menos, uma reunião técnica com a equipe do HUB-UnB, para apresentação, validação e alinhamento final das soluções propostas

7.10.9.7. Os serviços prestados deverão estar em conformidade com as políticas de segurança da informação vigentes no HUB-UnB, através da Política de Segurança da Informação (PSI) - Versão 2.0.

7.10.9.8. O serviço de site survey será contratado em item separado e fica vedada a adjudicação simultânea ao mesmo fornecedor da solução de rede Wi-Fi, como medida necessária e proporcional para mitigar potenciais conflitos de interesse, assegurando a independência técnica do levantamento e a fidedignidade dos resultados.

7.10.9.9. A vedação de adjudicação simultânea ao mesmo fornecedor da solução de rede Wi-Fi não restringe a competição, pois permite a participação de empresas especializadas nesse tipo de serviço, conforme evidenciado por pesquisa de mercado que demonstra a existência de prestadores independentes, bem como a vantajosidade do parcelamento da contratação.

7.10.10. REQUISITOS DE PROJETO E DE IMPLEMENTAÇÃO DA SOLUÇÃO (IN 94/2022 SGD/ME - Art. 16, inciso II, alínea b)

7.10.10.1. Deverá ser elaborado um plano de projeto detalhando as ações necessárias, os responsáveis envolvidos, o cronograma, o plano de implantação e a análise do risco associado às atividades de fornecimento, implantação da solução, observando as boas práticas de mercado.

7.10.10.2. O plano de projeto deverá ser elaborado pela CONTRATADA em até 20 (vinte) dias úteis após a abertura da Ordem de Serviço e validado e aprovado pela equipe de fiscalização do contrato. São atividades que serão executadas:

- a) Abertura do projeto: realização de reunião inicial (*kick-off*) com os responsáveis da CONTRATADA e da CONTRATANTE que atuarão diretamente na gestão do Projeto.
- b) Na reunião a CONTRATADA deverá apresentar sua equipe de trabalho, bem com o Gerente de Projetos que será o ponto focal para tratativa de assuntos relativos à execução dos serviços, sendo este o responsável por coordenar e orientar todos os técnicos para execução dos serviços, de forma que os prazos e qualidade estabelecidos sejam respeitados. Caberá ainda ao Gerente de Projetos apresentar na reunião uma lista de contatos de comunicação para esclarecimento de dúvidas ou apoio de itens

relacionados ao projeto.

- c) Apresentação do escopo do serviço: consiste na elaboração e apresentação do Escopo do Projeto.
- d) Definição do Cronograma do Projeto: consiste na etapa em que a CONTRATADA deverá apresentar o Cronograma de Execução Detalhado, que conste atividades, subatividades e marcos, em cada uma das fases, contemplando ainda todas as ações previstas para o fornecimento da solução, datas de entrega da documentação, datas das reuniões de ponto de controle, dentre qualquer outro evento que se julgar relevante e necessário.
- e) Apresentação dos participantes do projeto: etapa que ocorrerá em até 7 (Sete) dias consecutivos após emissão da ordem de serviço, onde a CONTRATADA deverá agendar reunião (*kick-off*) junto aos responsáveis técnicos da CONTRATANTE, objetivando dar início ao acompanhamento da execução do Contrato.

7.10.11. As reuniões de controle do projeto deverão ser documentadas e a seu fim registradas em ata com assinatura dos presentes ou gravadas quando *on-line*. A data e periodicidade de sua realização será definida em comum acordo entre as partes envolvidas no contrato.

7.10.12. Caberá ao Gerente de Projetos a responsabilidade por elaborar e entregar a CONTRATADA os relatórios de progresso, bem como apresentar todas as situações pertinentes à situação do projeto (Relatório de Acompanhamento), constando neste a relação de atividades executadas período, pendências e solicitações de mudança no cronograma do projeto, dentre outros assuntos relativos e pertinentes.

7.10.13. Os relatórios de progresso e relatórios de acompanhamento deverão ser disponibilizados à CONTRATANTE em data e periodicidade a ser definida em comum acordo entre as partes. A CONTRATADA deverá realizar reuniões de planejamento e consultoria com a CONTRATANTE a fim de se definir os detalhes técnicos requeridos para as configurações e realização da implantação e operação da solução contratada.

7.10.14. O Plano de Implantação deverá conter detalhes das atividades de instalação, dos impactos previstos, dos testes necessários, das estratégias de continuidade e as informações de configuração e parametrização da solução.

7.10.15. Os requisitos técnicos devem ser coletados através de informações do ambiente computacional do CONTRATANTE, através de reuniões e verificação de informações *in-loco*, com o objetivo de documentar e analisar as informações quanto aos componentes de infraestrutura, bem como estabelecer os parâmetros necessários à configuração e integração dos produtos.

7.10.16. Deverá conter no Plano de Implantação a identificação dos ativos da solução, detalhando e posicionando todos os ativos que serão utilizados na implementação, bem como as interações com os demais ativos do ambiente computacional do CONTRATANTE.

7.10.17. Deverá conter no Plano de Implantação o desenho da arquitetura lógica da solução, com identificação dos principais recursos e serviços para o ambiente computacional do CONTRATANTE, visão geral da arquitetura da rede, seus componentes e ativos em fornecimento.

7.10.18. Deverá conter no Plano de Implantação o desenho da arquitetura física da solução, com detalhes de todas as conexões físicas e interligações entre os ativos da solução e o ambiente computacional da CONTRATANTE, com destaques para informações de portas, interconexões e endereços de configuração.

7.10.19. Deverá conter no Plano de Implantação o detalhamento das especificações necessárias para a implementação dos serviços - instalação, configuração e integração de todos os produtos da solução.

7.10.20. Deverá conter no Plano de Implantação todo o processo de homologação dos produtos e detalhamento dos testes que serão executados para validar a solução implementada.

7.10.21. Deverá conter no Plano de Implantação o planejamento das estratégias de continuidade para os serviços providos pela solução, sendo previsto a elaboração de documentos com detalhes do contingenciamento dos serviços e descrevendo os procedimentos necessários para restabelecimento do ambiente à normalização, em caso de falha ou indisponibilidade que acarretem interrupção no uso dos serviços em produção.

7.10.22. A CONTRATADA deverá preencher os documentos de requisição de mudança (RDM), sempre que a atividade impactar o ambiente de produção.

7.10.23. Ao término do Projeto de Implantação o Gerente de Projetos deverá consolidar toda documentação gerada e entregá-la em meio eletrônico à CONTRATANTE. A referida documentação estará sujeita à revisão e aprovação pelos membros técnicos da equipe de fiscalização designados pela CONTRATANTE.

7.11. REQUISITOS DE IMPLANTAÇÃO DA SOLUÇÃO (IN 94/2022 SGD/ME - Art. 16, inciso II, alínea c)

7.11.1. A implantação será iniciada após a aprovação do Plano de Implantação pela CONTRATANTE.

7.11.2. A implementação deverá ser gerenciada de tal forma que incidentes de indisponibilidade ou interrupção dos serviços presentes no ambiente de produção sejam mínimos e gerenciados, com as devidas tratativas para restabelecimento em caso de falha, bem como documentado e aprovado pela CONTRATANTE. É de responsabilidade da CONTRATADA, com supervisão de membro designado pela CONTRATANTE, a instalação e configuração de todos os produtos adquiridos no contrato, sejam estes *hardwares* (exceto *Access Points*), *softwares* ou que tenham

relacionamento com o licenciamento da solução.

7.11.3. A CONTRATANTE será responsável pela instalação física dos Access Points nos locais indicados pelo *Site Survey*. No entanto, a CONTRATADA, por sua vez, deverá entregar a solução totalmente configurada garantindo a adoção automatizada dos Access Points após a sua conexão à rede.

7.11.4. A CONTRATADA deverá prover equipe adequadamente capacitada para a implantação das soluções adquiridas.

7.11.5. A CONTRATADA deverá credenciar junto a CONTRATANTE, os profissionais que terão acesso às instalações do HUB-UnB para prestação de serviços.

7.11.6. Todos os requisitos técnicos devem ser cumpridos prontamente pela CONTRATADA para implantação da solução, tais como:

7.11.7. Avaliação, levantamento, interligação da rede elétrica para alimentação dos equipamentos, se necessário, não é necessário entregar *Power Distribution Unit* (PDU) para ligação da solução de rede Wi-Fi, em caso de equipamentos físicos.

7.11.8. Realizar a avaliação, levantamento, integração e adequação das condições de rede de dados física e lógica para interconexão dos equipamentos da solução Wi-Fi ao ambiente existente na CONTRATANTE.

7.11.9. Realizar atualização de firmware, configuração de rede, configuração de monitoramento e sincronização de horário, configuração de autenticação integrada com *Active Directory*, criação de SSID, configurações de funcionalidades dos dados de ambiente de virtualização, quando for o caso, dentre outras ações que visem adequar o funcionamento inicial dos equipamentos ao ambiente da CONTRATANTE;

7.11.10. Todo o trabalho referente ao cabeamento deverá ser realizado atendendo às normas técnicas aplicáveis, incluindo a adequada organização e identificação de cabos, segundo padrão de qualidade já existente;

7.11.11. Todos os aspectos relacionados à adequação das condições elétricas e de rede de dados necessários à instalação dos equipamentos deverão ser levantados durante a vistoria facultativa na fase licitatória ou vistoria obrigatória, após a assinatura do contrato. Durante esta etapa, as Licitantes deverão avaliar os detalhes técnicos necessários ao cumprimento de suas obrigações;

7.11.12. A adequação deverá englobar o fornecimento de todos os cabos, conectores, guias, leitos aramados, abraçadeiras, velcros e demais componentes necessários à interligação de todos os produtos de hardware ofertados, em caso de equipamentos físico (*appliance*);

7.11.13. Todos os cabos e conectores fornecidos deverão ser certificados por órgãos competentes e deverão possuir o comprimento adequado para interligar todos os equipamentos fornecidos;

7.11.14. O fornecimento de toda e qualquer ferramenta, instrumento, material e equipamento de proteção, bem como materiais complementares necessários à instalação são de inteira responsabilidade da CONTRATADA e não deverá gerar ônus à CONTRATANTE;

7.11.15. A falta de peças ou equipamentos não será considerada como alegação de motivo de força maior e não eximirá a CONTRATADA das penalidades a que estará sujeita pelo não cumprimento dos prazos estabelecidos;

7.11.16. A CONTRATADA deverá atuar em qualquer movimentação de ativos dentro do datacenter – entre espaços e racks, dentro do ambiente da CONTRATANTE, e de fora deste, que se fizer necessário.

7.11.17. Na instalação dos produtos, a CONTRATADA deverá fornecer um Relatório de Instalação, com no mínimo:

- a) relação dos pré-requisitos do ambiente operacional para a instalação dos produtos;
- b) confirmação de todos os pré-requisitos do ambiente operacional necessários ao perfeito funcionamento de cada produto, nos locais onde deverá estar instalado;
- c) confirmação da presença e funcionamento adequado de cada um dos produtos;
- d) a identificação de cada produto (marca, modelo, versão, número de licença e outras informações pertinentes);
- e) informações de contato dos técnicos da CONTRATADA que instalaram os produtos;

7.11.18. A CONTRATADA deverá realizar em conjunto com a CONTRATANTE os testes necessários para validação do perfeito funcionamento da solução;

7.11.19. O ambiente composto pela interconexão dos novos equipamentos aos existentes, será testado e validado pela CONTRATADA em conjunto com o HUB-UnB;

7.11.20. A CONTRATADA deverá manter o local de execução dos serviços em perfeitas condições de limpeza e uso;

7.11.21. A empresa CONTRATADA ao final do processo de instalação, deverá fornecer documentação em meio eletrônico, contendo descritivo atualizados (*as-built*) e completo do processo de instalação da solução, e ainda os detalhes sobre a comunicação dos equipamentos, onde deverá ser demonstrada as velocidades e qualidade da transmissão de dados, conforme plano de testes, para fins de comprovação da conclusão da implantação.

7.11.22. Após a conclusão da implantação da solução (entrega, instalação e configuração), a CONTRATADA disponibilizará ao HUB-UnB a documentação final do projeto, completa e atualizada (*as-built*), de modo a sinalizar a conclusão da etapa de implantação e solicitará a validação para fins de recebimento definitivo.

7.11.23. O HUB-UnB avaliará todos os aspectos relacionados ao fornecimento e implantação da solução e, caso todos os requisitos tenham sido atendidos, emitirá o Termo de Recebimento Definitivo (**MODELO DO TERMO DE RECEBIMENTO DEFINITIVO - ENCARTE VI**).

7.12. REQUISITOS DE GARANTIA (IN 94/2022 SGD/ME - Art. 16, inciso II, alínea d)

7.12.1. A CONTRATADA deverá fornecer garantia de 60 meses, a contar da data de assinatura do Termo de Recebimento Definitivo, para TODOS os itens (*hardware, software, acessórios* etc.) que compõem a solução de rede Wi-Fi ofertada.

7.12.2. A exigência de garantia mínima de 60 (sessenta) meses fundamenta-se no princípio da economicidade e no dever de planejamento da contratação, conforme reiterado entendimento do Tribunal de Contas da União (TCU), que orienta a Administração a considerar o custo total de propriedade (TCO) e o ciclo de vida das soluções de TIC.

7.12.3. Considerando que a vida útil estimada da solução é de, no mínimo, 60 meses, a exigência de garantia integral durante esse período visa assegurar a continuidade operacional, mitigar riscos de indisponibilidade e evitar custos adicionais com contratações futuras de suporte e manutenção.

7.12.4. Ademais, a medida não configura restrição indevida à competitividade, uma vez que se trata de prática disponível no mercado para soluções equivalentes, sendo tecnicamente justificada pela criticidade da solução e pela necessidade de previsibilidade orçamentária.

7.12.5. A CONTRATADA deverá descrever, em sua proposta, os termos da garantia técnica oferecida pelo fabricante da solução, incluindo o *Part Number* ou equivalente da garantia ofertada.

7.12.6. A CONTRATANTE deverá ter acesso direto ao centro de assistência técnica do fabricante para abertura de chamados, bem como para acompanhar e gerenciar os casos quando necessário. Esse acesso deverá ser provido 8 (oito) horas por dia, 5 (cinco) dias por semana, em horário comercial.

7.12.7. A garantia deverá cobrir, sem ônus adicionais, substituição de peças defeituosas, correções e novas versões disponíveis para todos os *softwares, firmwares*, atualizações de *bug*, patches de segurança e afins dos componentes das soluções.

7.12.8. A aquisição e a instalação dos *Access Points* poderá ser gradativa de acordo com a necessidade da CONTRATANTE. No entanto, a garantia dos equipamentos deverá obedecer às mesmas condições estabelecidas para a solução de rede Wi-Fi, sendo de 60 (sessenta) meses a contar da data do recebimento definitivo de cada lote de *Access Points*.

7.12.9. A CONTRATANTE deverá ter acesso direto à base de dados de conhecimento do fabricante que contenham especificações técnicas, informações, assistência e orientação para instalação, desinstalação, configuração e atualização de *firmware* e *software*, aplicação de correções (*patches*), diagnósticos, avaliações e resolução de problemas e demais atividades relacionadas à correta operação e funcionamento dos equipamentos.

7.12.10. Em caso de substituição de equipamentos ou componentes, estes passarão à propriedade da CONTRATANTE, devendo o mesmo ser incluído no contrato de garantia vigente em substituição ao equipamento danificado.

7.12.11. Os reparos físicos decorrentes do exercício da garantia devem ser executados onde se encontram os equipamentos (modalidade *on-site*).

7.12.12. Deverá ser assegurado que a substituição de equipamento, peça ou componente defeituoso, em qualquer caso, seja feita por item equivalente, ou que possua características iguais ou superiores a estas, desde que homologadas pelo fabricante como parte compatível da solução de rede Wi-Fi.

7.12.13. A substituição de componentes será considerada consumada, para todos os efeitos, após aceitação formal pela CONTRATANTE.

7.12.14. A CONTRATADA ficará responsável pelo devido recolhimento no momento da substituição, bem como dos resíduos dos processos de manutenção e limpeza dos equipamentos, que deverão ser tratados de forma ambientalmente adequada, respeitando a legislação ambiental vigente.

7.12.15. O HUB-UnB reserva-se ao direito de conectar equipamentos de outros fabricantes aos equipamentos fornecidos, sem que isso implique na perda da garantia do fabricante. Desde que tal fato não implique danos materiais aos equipamentos, isso não deve constituir motivo para a CONTRATADA se desobrigar dos serviços de suporte técnico em garantia.

7.12.16. Durante o período da garantia, a CONTRATADA deverá prestar os serviços de SUPORTE TÉCNICO em garantia, sem custo adicional.

7.12.17. O suporte técnico em garantia deverá ser prestado sem prejuízo de qualquer política de garantia adicional oferecida pelo fabricante.

- 7.12.18. O suporte técnico em garantia deverá ser prestado de forma remota ou presencial, na modalidade *on-site*, nas dependências da CONTRATANTE, na modalidade 8/5, a partir da comunicação do problema, via serviço gratuito telefônico ou sistema web indicado pela CONTRATADA ou via notificação automática emitida pela solução. Na indisponibilidade do canal de atendimento estabelecido, o HUB-UnB encaminhará e-mail à CONTRATADA solicitando a abertura do chamado, de forma que a contagem de prazo de atendimento se iniciará a partir da data de encaminhamento do e-mail.
- 7.12.19. Caberá à CONTRATADA a responsabilidade pelo deslocamento, alimentação e estadia do seu técnico ao/no local da instalação do equipamento, bem como pela retirada e entrega de peças de reposição e demais componentes necessários, com todas as despesas de transporte, frete e seguro correspondentes.
- 7.12.20. A CONTRATADA deverá disponibilizar meios para que a equipe técnica do HUB-UnB possa acompanhar os atendimentos do suporte técnico em garantia, *on-line*, em portal web com acesso controlado por senha.
- 7.12.21. Os chamados de suporte técnico em garantia junto à CONTRATADA deverão ser atendidos por profissionais da CONTRATADA, em português e serão usados para solicitações de informações, reportar incidentes ou esclarecer dúvidas quanto à utilização da solução ofertada.
- 7.12.22. Se necessário, a CONTRATADA deverá assistir remotamente na instalação e uso dos *softwares* ofertados, fornecendo orientações para diagnóstico de problemas e ajuda na interpretação de *logs e debugs*, assim como apoiar no envio de informações relevantes ao fabricante para tratativas de eventuais problemas.
- 7.12.23. Em caso de indisponibilidade total da solução de rede Wi-Fi, a CONTRATADA deverá disponibilizar solução de contorno, em caráter temporário, fornecendo componente/equipamento equivalente para substituição do item danificado, estando a CONTRATADA responsável por toda logística, instalação e configuração dos equipamentos, assim como pela retirada dos antigos, sem qualquer ônus adicional ao HUB-UnB.
- 7.12.24. A CONTRATADA deverá garantir que os serviços objeto do Termo de Referência atenderão ao padrão de qualidade implementados no mercado e de critérios da CONTRATANTE.
- 7.12.25. A realização de mudanças no ambiente de operação deverá cumprir requisitos estabelecidos no processo de gerenciamento de mudanças da CONTRATANTE.
- 7.12.26. A CONTRATANTE poderá solicitar à CONTRATADA, a cada 6 (seis) meses uma visita técnica para realização de manutenção preventiva, destinada a reduzir a probabilidade de falha ou a degradação do funcionamento da solução.
- 7.12.27. Um chamado técnico somente poderá ser fechado após o aceite da CONTRATANTE e o término de atendimento se dará com a disponibilidade do recurso para uso em perfeitas condições de funcionamento.
- 7.12.28. Ao final do atendimento, o técnico da CONTRATADA deverá elaborar um relatório de ocorrência onde conste o problema causador do chamado, a solução encontrada, as pendências, a data e hora do chamado, do início e do fim do atendimento. Esse relatório deve ter a concordância e assinatura de um técnico da CONTRATANTE.
- 7.12.29. Deverá ser observado os **NÍVEIS MÍNIMOS DE SERVIÇO**, conforme a tabela 4:

Severidade	Descrição	Tipo de Atendimento	Tempo de início de Atendimento	Tempo de Solução ou Contorno	Observação
1 - Alta	Chamados associados a situações de alto impacto, incluindo os casos de indisponibilidade da solução de Wi-Fi ou degradação severa de desempenho	On-site ou Remoto	No máximo 12 (doze) horas corrida após a abertura do chamado	No máximo 24 (vinte e quatro) horas corridas após o início do atendimento	Caso o problema não possa ser resolvido remotamente dentro do prazo estabelecido, a CONTRATADA deverá colocar à disposição e às suas expensas, um especialista devidamente habilitado e credenciado que trabalhará o tempo que for necessário para a solução do problema.
2 - Média	Chamados referentes a situações de baixo impacto ou para aqueles problemas que se apresentem de forma intermitente, incluindo os casos em que haja a necessidade de substituição de componente(s) que possua(m) redundância	On-site ou Remoto	No máximo 24 (vinte e quatro) horas úteis após a abertura do chamado	No máximo 5 (cinco) dias corridos após o início do atendimento	Caso o problema não possa ser resolvido remotamente dentro do prazo estabelecido, a CONTRATADA deverá colocar à disposição e às suas expensas, um especialista devidamente habilitado e credenciado que trabalhará o tempo que for necessário para a solução do problema.
					Caso a dúvida não

3 - Baixa	Chamados de suporte técnico em garantia	On-site ou Remoto	No máximo 24 (vinte e quatro) horas úteis após a abertura do chamado	No máximo 72 (setenta e duas) horas corridas após o início do atendimento	possa ser respondida pela CONTRATADA ou dependa do Fornecedor ou de um terceiro para composição da resposta, deve ser informado ao requisitante dentro do prazo estabelecido para atendimento do chamado.
-----------	---	-------------------	--	---	---

Tabela 4 - Níveis de Serviço

7.12.30. Caso seja necessário, a CONTRATADA poderá aplicar solução de Contorno, providenciando em caráter temporário componente/equipamento equivalente para substituição do item danificado, estando a CONTRATADA responsável por toda logística, instalação e configuração dos equipamentos, assim como pela retirada dos antigos, sem qualquer ônus adicional ao HUB-UnB.

7.12.31. O fechamento do chamado poderá se dar, quer pela aplicação de correção ao produto ou pela aplicação de solução de contorno que possibilite a operação do sistema.

7.12.32. A disponibilização de medida corretiva definitiva poderá, a critério da CONTRATADA, vir a ser incorporada em futuras versões do software.

7.12.33. A CONTRATADA manterá cadastro das pessoas indicadas pelo HUB-UnB, as quais poderão efetuar abertura e autorizar fechamento de chamados.

7.12.34. DA RETIRADA DOS EQUIPAMENTOS EM CASO DE ACIONAMENTO DE GARANTIA OU TROCA DE PEÇAS:

7.12.35. A retirada de equipamentos pela CONTRATADA deverá ocorrer em até 5 dias úteis a contar da solicitação, devendo o ato da retirada ser previamente comunicado ao HUB-UnB, com no mínimo 2 (dois) dias úteis de antecedência à retirada.

7.12.36. A responsabilidade do serviço de remoção, logística e embalagem dos equipamentos para transporte é da CONTRATADA.

7.13. **REQUISITOS DE CAPACITAÇÃO (IN 94/2024 SGD/ME - Art. 16, inciso II, alínea e)**

7.13.1. Deverá ser realizado de forma presencial ou remota, onde a CONTRATADA arcará com todas as despesas relativas e necessárias, caso seja presencial.

7.13.2. Deverá contemplar todos os aspectos essenciais de funcionamento e operação, devendo conter a instalação, configuração, gerenciamento, melhores práticas e resolução de problemas de todos os componentes ofertados, incluindo hardware e software.

7.13.3. Deverá contemplar toda parte de acionamento de suporte técnico e garantia.

7.13.4. Deverá ser apresentada e disponibilizada toda documentação e orientações para estabelecer procedimentos de aplicação de pacotes de correção, migração de versões e demais pacotes disponibilizados pelo fabricante.

7.13.5. A capacitação deverá ser gravada pela CONTRATADA e disponibilizada para a CONTRATANTE, com o devido consentimento dos envolvidos. O HUB-UnB poderá utilizar o material, sempre que necessário, para capacitação interna dos colaboradores.

7.13.6. O instrutor da capacitação deve ser profissional certificado pelo fabricante da solução e com experiência comprovada na solução ofertada, de modo a assegurar a correta transferência de conhecimento, a aderência às melhores práticas oficiais do fabricante e a correta alicação das funcionalidades e configurações específicas da tecnologia implementada.

7.13.7. O conteúdo da capacitação deverá abranger, no mínimo, os seguintes tópicos:

- Instalação e configuração dos equipamentos, via sistema de gerenciamento;
- Acompanhamento de índices de qualidade e estatísticas de uso;
- Diagnóstico de falhas e procedimentos de resolução por meio da gerência;
- Alterações de configurações e sua aplicação aos dispositivos;
- Parâmetros principais da controladora;
- Aplicação de políticas da controladora a equipamentos em locais remotos;
- Atualização e sincronização de políticas entre os dispositivos;
- Identificação de indicadores de desempenho;
- Execução de backup de configurações e logs para repositório externo;
- Restauração de configurações a partir dos backups;

- Monitoramento de tráfego entre controladora e *Access Points*, bem como o status e informações básicas dos dispositivos da rede;
- Gerenciamento da solução de controle de acesso (NAC);
- Gerenciamento de políticas de acesso;
- Gerenciamento de usuários administrativos e de visitantes;
- Configuração de acesso e permissões ao equipamento incluindo autenticação por RADIUS e *Microsoft Active Directory* utilizado pelo HUB-UnB.
- Integração com fontes externas de autenticação como Gov.BR, Google, Facebook (Meta) e outros;
- Emissão de relatórios de acesso;
- Demais tópicos relevantes da solução identificados pela CONTRATADA que sejam pertinentes à operação da solução Wi-Fi.

7.14. REQUISITOS DE EXPERIÊNCIA PROFISSIONAL (IN 94/2022 SGD/ME - Art. 16, inciso II, alínea f)

7.14.1. A CONTRATADA vencedora do Grupo 1 deverá comprovar ser representante oficial da solução ofertada, por meio de documento emitido pelo fabricante, de modo a assegurar a procedência dos equipamentos, o acesso a suporte técnico oficial, atualizações e garantia.

7.14.2. A CONTRATADA vencedora do item 8 (Item avulso) deverá apresentar a comprovação de que os profissionais responsáveis pela execução do site survey possuem, no mínimo, a certificação CWNA (Certified Wireless Network Administrator) ou superior, da Certified Wireless Network Professionals (CWNP) ou equivalente de modo a assegurar a qualificação técnica necessária para a adequada execução do levantamento.

7.15. REQUISITOS DE FORMAÇÃO DA EQUIPE DE PROJETO E IMPLANTAÇÃO (IN 94/2022 SGD/ME - Art. 16, inciso II, alínea g)

7.15.1. Deverá ser apresentado um Preposto, nos termos do Art. 208, do Regulamento de Compras e Contratos da HU Brasil, aceito pela Administração, para representar a CONTRATADA ao longo da execução contrato.

7.15.2. Deverá ser apresentado um Gerente de Projetos, que será o ponto focal para tratativas de assuntos relativos à execução dos serviços, sendo este o responsável por coordenar e orientar todos os técnicos para execução dos serviços, de forma que os prazos e qualidade estabelecidos sejam respeitados.

7.15.3. Caberá ainda ao Gerente de Projetos apresentar na reunião uma lista de contatos de comunicação para esclarecimento de dúvidas ou apoio de itens relacionados ao projeto.

7.15.4. A instalação e configuração devem ser realizadas por técnicos certificados, com capacidade técnica comprovada para a execução do serviço, mediante apresentação de certificação emitida pelo fabricante do equipamento ou por empresa de treinamento por ele reconhecida, de modo a assegurar a correta implementação da solução, a aderência às melhores práticas e a preservação das condições de garantia e suporte do fabricante. Tal exigência se mostra necessária e proporcional para mitigar riscos de falhas de implantação e retrabalho.

7.15.5. O suporte técnico em garantia deve ser realizado por profissionais devidamente habilitados, treinados e qualificados na solução ofertada.

7.16. REQUISITOS DE METODOLOGIA DE TRABALHO (IN 94/2022 SGD/ME - Art. 16, inciso II, alínea h)

7.16.1. Deverão ser adotadas as boas práticas e técnicas de gerenciamento de projeto.

7.16.2. Os serviços de suporte técnico em garantia deverão seguir as melhores práticas preconizadas pelo ITIL.

7.17. REQUISITOS DE SEGURANÇA E PRIVACIDADE DE TECNOLOGIA (IN 94/2022 SGD/ME - Art. 16, inciso II, alínea i)

7.17.1. A solução de rede Wi-Fi a ser adquirida pelo Hospital Universitário de Brasília (HUB-UnB) deve atender aos requisitos de segurança da informação estabelecidos na Política de Segurança da Informação da Rede HU Brasil, que visa assegurar a confidencialidade, integridade e disponibilidade dos dados institucionais e de seus usuários. É fundamental que a rede Wi-Fi seja projetada e configurada para mitigar riscos e ameaças cibernéticas, protegendo informações sensíveis e garantindo um ambiente seguro para a execução das atividades assistenciais, administrativas, de ensino e pesquisa.

7.17.2. A solução de rede Wi-Fi deve contemplar mecanismos robustos de autenticação e controle de acesso, criptografia de dados e monitoramento contínuo, em alinhamento com as diretrizes da HU Brasil para a proteção do patrimônio informacional e a conformidade com as legislações aplicáveis.

7.17.3. Deverá possuir mecanismos de segurança que garantam a disponibilidade, integridade, confidencialidade e autenticidade dos dados.

7.17.4. Deverá possuir solução de gerência que permita gerenciar diferentes perfis de acesso, com autenticação por

usuário e senha.

7.17.5. Deverá gerar registros de logs das ações de administração e eventos relevantes da solução de rede Wi-Fi.

7.17.6. Deverá possuir recursos que permitam o monitoramento automático de eventos relevantes da solução de gerenciamento e dos *Access Points*.

7.17.7. Deverá ainda prevê os recursos apresentados abaixo:

- **Autenticação Segura:** A rede Wi-Fi deve utilizar mecanismos de autenticação robustos, integrando-se com o *Active Directory* para autenticação de usuários.
- **Controle de Acesso Granular:** Deve ser possível configurar políticas de acesso segmentadas, garantindo que cada perfil de usuário (administrativo, assistencial, docente, discente, visitantes, etc.) tenha acesso apenas aos recursos necessários para suas atividades. Implementar segmentação de rede (VLANs) para isolar tráfegos de diferentes áreas e dispositivos.
- **Criptografia de Dados:** Todo o tráfego da rede Wi-Fi deve ser criptografado usando padrões de segurança fortes (AES-256) para proteger a integridade e confidencialidade das informações transmitidas, incluindo comunicações de dados sensíveis, como prontuários eletrônicos e informações administrativas.
- **Gerenciamento e Monitoramento Contínuo:** A solução deve incluir funcionalidades de gerenciamento centralizado para monitoramento em tempo real do uso da rede, comportamento anômalo e possíveis tentativas de acesso não autorizado. Implementar alertas automáticos para detecção e resposta a incidentes de segurança.
- **Segurança em Redes de Visitantes:** As redes destinadas a visitantes e dispositivos não gerenciados devem ser separadas da rede corporativa e assistencial, com políticas de acesso restritivas que limitem a conectividade a serviços públicos, como internet, sem acesso aos sistemas internos do HUB-UnB.
- **Atualizações e Patches de Segurança:** Todos os equipamentos da rede Wi-Fi devem ser mantidos com firmware e patches de segurança atualizados, conforme as recomendações do fabricante, para evitar vulnerabilidades conhecidas.
- **Registros de Atividade (Logs):** A solução deve registrar logs detalhados de acesso, atividade e tentativas de violação, permitindo auditorias regulares e investigação em caso de incidentes de segurança. Os registros devem ser armazenados de forma segura e com retenção adequada para conformidade com normas e políticas internas.
- **Segmentação e Isolamento de Dispositivos IoT:** Dispositivos IoT conectados à rede Wi-Fi devem ser isolados em segmentos de rede dedicados, com políticas de segurança específicas para limitar seu acesso e minimizar o impacto em caso de comprometimento.
- **Conformidade com Normas e Regulamentos:** A solução deve estar em conformidade com as normas e regulamentos de segurança da informação aplicáveis, incluindo a LGPD (Lei Geral de Proteção de Dados), e as diretrizes de segurança da HU Brasil, garantindo a proteção dos dados pessoais e sensíveis dos usuários do HUB-UnB.

8. DA SUBCONTRATAÇÃO

8.1. Não será admitida a subcontratação integral do objeto contratual. A subcontratação parcial poderá ser autorizada, em caráter excepcional, desde que haja justificativa técnica que demonstre a inviabilidade técnico-econômica da execução integral pela CONTRATADA, mediante autorização formal e expressa da CONTRATANTE, sem que a atuação da CONTRATADA se limite à mera intermediação ou administração do contrato.

8.2. É vedada a subcontratação de atividades que envolvam tratamento de dados pessoais sem prévia autorização formal e por escrito da CONTRATANTE. Na hipótese de autorização de subcontratação parcial, a CONTRATADA permanecerá integralmente responsável perante a CONTRATANTE pelo cumprimento de todas as obrigações contratuais e legais aplicáveis, inclusive aquelas relacionadas à proteção de dados pessoais, respondendo solidariamente pelos atos praticados pela subcontratada.

9. APLICABILIDADE DA LEI COMPLEMENTAR 123/2006

9.1. Não foi fixada cotas reservadas para ME/EPP, considerando que para o atendimento do objeto deste processo licitatório não foi identificado o mínimo de 3 (três) fornecedores competitivos enquadrados como microempresas ou empresas de pequeno porte sediadas local ou regionalmente e capazes de cumprir as exigências estabelecidas no instrumento convocatório, em respeito ao disposto no art. 49, inciso II, da Lei Complementar nº 123 de 2006, sendo necessário que se abra para ampla concorrência para que seja alcançado maior número de participantes.

10. OBRIGAÇÕES DA CONTRATANTE (IN 94/2022 SGD/ME - ART. 17, INCISO I)

10.1. Os critérios referentes ao modelo de gestão do contrato estão definidos no instrumento contratual.

11. OBRIGAÇÕES DA CONTRATADA (IN 94/2022 SGD/ME - ART. 17, INCISO II)

11.1. Os critérios referentes ao modelo de gestão do contrato estão definidos no instrumento contratual.

12. DO MODELO DE EXECUÇÃO (IN 94/2022 SGD/ME - ART. 18)

12.1. DOS PRAZOS, HORÁRIOS DE FORNECIMENTO DE BENS, PRESTAÇÃO DOS SERVIÇOS E LOCAIS DE ENTREGA (IN 94/2022 SGD/ME - Art. 18, inciso I, alínea a)

12.1.1. Após a abertura da Ordem de Serviço, os bens que compõem a solução devem ser entregues em até 60 (sessenta) dias corridos.

12.1.2. Os equipamentos deverão ser entregues nas dependências do HUB-UnB, no horário compreendido entre 08h e 12h e entre 14h e 18h (horário de Brasília), de segunda a sexta-feira (dias úteis), no endereço:

HUB-UnB - Hospital Universitário de Brasília
Endereço: Setor de Grandes Áreas Norte, nº 605
Asa Norte, Brasília - Distrito Federal
CEP: 70840-901
Telefone: (61) 2028-5346

12.1.3. De comum acordo, poderão ser combinados diferente horários e local de entrega.

12.1.4. A entrega dos equipamentos pela transportadora deverá ser previamente comunicada ao HUB-UnB com no mínimo 2 (dois) dias úteis de antecedência.

12.1.5. Os horários de execução dos serviços de instalação e configuração, deverão ser previstos no Plano de Projeto.

12.1.6. Após a entrega de todos os itens que compõem a solução de rede Wi-Fi, será emitido em até 5 dias úteis o Termo de Recebimento Provisório (MODELO DO TERMO DE RECEBIMENTO PROVISÓRIO - ENCARTE V).

12.2. DA DOCUMENTAÇÃO MÍNIMA EXIGIDA (IN 94/2022 SGD/ME - Art. 18, inciso I, alínea b)

12.2.1. Deverá a CONTRATADA apresentar os relatórios de execução de serviço.

12.2.2. Deverá a CONTRATADA apresentar toda documentação referente ao fornecimento dos bens que compõem a solução.

12.3. DOS PAPÉIS E RESPONSABILIDADES (IN 94/2022 SGD/ME - Art. 18, inciso I, alínea c)

12.3.1. Os critérios referentes ao modelo de gestão do contrato estão definidos no instrumento contratual.

12.4. DA QUANTIFICAÇÃO OU ESTIMATIVA PRÉVIA DO VOLUME DE SERVIÇOS DEMANDADOS, QUANTIDADE DE BENS A SEREM FORNECIDOS (IN 94/2022 SGD/ME - Art. 18, inciso II)

12.4.1. Deverão ser fornecidos os bens definidos neste termo de referência, conforme quantidades estabelecidas.

12.5. DA DEFINIÇÃO DE MECANISMOS FORMAIS DE COMUNICAÇÃO A SEREM UTILIZADOS PARA TROCA DE INFORMAÇÕES ENTRE A CONTRATADA E O HUB-UNB (IN 94/2022 SGD/ME - Art. 18, inciso III)

12.5.1. A solicitação de bens e serviços será por meio de emissão de Ordem de Serviço e Fornecedor de Bens (MODELO DA ORDEM DE SERVIÇO - ENCARTE II) .

12.5.2. Documentos formais deverão ser assinados, preferencialmente, pelo sistema SEI da HU Brasil.

12.5.3. Deverão ser utilizados e-mails corporativos para envio de mensagens e documentos digitais.

12.5.4. Videoconferências, serão realizadas através de ferramenta institucional do HUB-UnB, preferencialmente o Microsoft Teams.

12.5.5. Os mecanismos de comunicação para fins de acionamento de garantia e suporte técnico deverão seguir as definições estabelecidas neste Termo de Referência.

12.6. DA FORMA DE PAGAMENTO (IN 94/2022 SGD/ME - Art. 18, inciso IV)

12.6.1. Os pagamentos serão realizados, por meio de Ordem Bancária, de acordo com cada item, observando as seguintes condições:

- a) Para os itens 1, 2, 6, 7 (Grupo 1) e 8 (avulso), cujo fornecimento se caracterize como entrega única e integral, o pagamento será realizado após o recebimento definitivo do objeto, atestado pela CONTRATANTE;
- b) Para os itens 3, 4 e 5 (Grupo 1), cujo fornecimento e quantidades estão sujeitos às necessidades do HUB-UnB, o pagamento será realizado de forma parcelada, em conformidade com as quantidades efetivamente entregues e recebidas definitivamente, mediante atesto pela CONTRATANTE;

GRUPO	ITEM	DESCRIÇÃO	FORMA DE PAGAMENTO
-------	------	-----------	--------------------

1	1	Solução de Controladora WI-FI	Parcela única após o Termo de Recebimento Definitivo do item
	2	Solução de Gerência, Monitoramento e Controle de Acesso (NAC)	Parcela única após o Termo de Recebimento Definitivo do item
	3	Ponto de Acesso (Access Point) indoor 802.11ax - TIPO 1	Conforme as quantidades solicitadas pela CONTRATANTE, por meio da Ordem de Serviço
	4	Ponto de Acesso (Access Point) indoor 802.11ax - TIPO 2	Conforme as quantidades solicitadas pela CONTRATANTE, por meio da Ordem de Serviço
	5	Injetor de Potência (<i>Power Injector</i>)	Conforme as quantidades solicitadas pela CONTRATANTE, por meio da Ordem de Serviço
	6	Instalação e configuração da solução	Parcela única após o Termo de Recebimento Definitivo do item
	7	Treinamento e capacitação da solução	Parcela única após o Termo de Recebimento Definitivo do item
Item Avulso	8	Site Survey	Parcela única após o Termo de Recebimento Definitivo do item

Tabela 5 - Formas de Pagamento

12.7. DOS TERMOS DE COMPROMISSO E MANUTENÇÃO DO SIGILO

12.7.1. Deverá ser consentido e assinado pelo representante da CONTRATADA, o Termo de Compromisso e Confidencialidade (**MODELO DO TERMO DE COMPROMISSO - ENCARTE III**) emitido pela CONTRATANTE.

12.7.2. Deverá ser consentido e assinado por todos os colaboradores da CONTRATADA envolvidos no projeto, no suporte e manutenção, o Termo de Ciência (**MODELO DO TERMO DE CIÊNCIA - ENCARTE IV**) emitido pela CONTRATANTE.

12.8. DAS ETAPAS PREVISTAS

12.8.1. Após a nomeação da equipe de Gestão/Fiscalização do contrato, a equipe do HUB-UnB deverá proceder-se com as atividades de início do contrato:

I - Elaboração do Plano de Inserção da CONTRATADA, pelo Gestor do Contrato e pelos Fiscais Técnico, Administrativo e Requisitante do Contrato, contemplando, no mínimo:

- o repasse à CONTRATADA de conhecimentos necessários à execução dos serviços ou ao fornecimento de bens;
- a disponibilização de infraestrutura à CONTRATADA, quando couber.

II - Elaboração do Plano de Fiscalização da CONTRATADA, pelo Gestor do Contrato e pelos Fiscais Técnico, Administrativo e Requisitante do Contrato, contemplando, no mínimo:

- o refinamento dos procedimentos de teste e inspeção detalhados no Modelo de Gestão do contrato, para fins de elaboração dos Termos de Recebimento Provisório e Definitivo;
- configuração e/ou criação de ferramentas, computacionais ou não, para implantação e acompanhamento dos indicadores; e
- refinamento ou elaboração de Listas de Verificação e de roteiros de testes com base nos recursos disponíveis para aplicá-los.

III - Criação de processo administrativo específico, pela equipe de Gestão/Fiscalização do contrato, para registro histórico do contrato.

12.8.2. Após a assinatura do contrato, deverão ser observadas as etapas abaixo:

#	ETAPA	RESPONSÁVEL	PRAZO	ATIVIDADES
1 - REUNIÃO INICIAL				
				1. Realização de reunião inicial convocada pelo Gestor do Contrato para o repasse à

1.1	Reunião Inicial	Gestor do Contrato Fiscal Técnico Fiscal Requisitante Fiscal Administrativo CONTRATADA	Após a assinatura do contrato.	CONTRATADA de conhecimentos necessários à execução dos serviços ou ao fornecimento de bens, cuja pauta observará, pelo menos: a) presença do representante legal da CONTRATADA, que apresentará o preposto da mesma; b) entrega, por parte da CONTRATADA, do Termo de Compromisso e do Termo de Ciência; e c) esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato.
-----	-----------------	--	--------------------------------	--

2 - PROJETO, IMPLANTAÇÃO E TREINAMENTO

2.1	Emitir a Ordem de Serviço	Gestor Contrato	Após a reunião inicial.	1. Emitir a Ordem de Serviço - OS.
2.2	Apresentar o Plano de Projeto	CONTRATADA	Até 20 (vinte) dias úteis, após a emissão da Ordem de Serviço	- CONTRATADA deverá realizar visita(s) técnica(s) para averiguar condições de instalação para os equipamentos em cada local onde estes serão instalados, devendo: - verificar a infraestrutura física e lógica das dependências do HUB-UnB e demais pré-requisitos necessários à instalação dos equipamentos; - alinhar as condições de entrega e armazenamento dos equipamentos na unidade; - definir a estratégia de instalações dos equipamentos. - Emitir o Plano de Projeto para validação do HUB-UnB.
2.3	Validar o Plano de Projeto	Gestor Contrato Fiscal Técnico Fiscal Requisitante	Até 5 (cinco) dias úteis após a emissão do Plano de Projeto	1. Validação do Plano de Projeto.
2.4	Realizar a entrega dos equipamentos	CONTRATADA	Em até 60 (sessenta) dias corridos a partir da abertura da Ordem de Serviço.	1. Entregar os equipamentos no local e prazo definido.
2.5	Sinalização de recebimento dos equipamentos	Fiscal Técnico	Até 5 (cinco) dias úteis após o recebimento da Entrega.	- Validar os quantitativos de equipamentos entregues, conforme proposta e Nota Fiscal; - Emitir o Termo de Recebimento Provisório - TRP.
2.6	Realizar a instalação e configuração dos equipamentos	CONTRATADA	Até 30 (trinta) dias corridos após a emissão do TRP	- Realizar os serviços de instalação, configuração e testes dos equipamentos. - Emitir a documentação final e completa do projeto

2.7	Realizar o repasse de conhecimento da Solução	CONTRATADA	Iniciado em até 5 (cinco) dias úteis após conclusão da implantação. Essa etapa pode ser remarcada a critério do HUB-UnB, sem prejuízo às demais etapas.	1. Realizar o repasse de conhecimento sobre toda solução implantada. 2. Emitir certificado de participação.
2.8	Sinalização de conclusão da implantação da solução	CONTRATADA	Até 5 (cinco) dias úteis após conclusão da implantação plena da solução.	1. Emitir e disponibilizar a documentação final do projeto, completa e atualizada, de modo a sinalizar a conclusão da etapa de implantação 2. Solicitar a validação para fins de recebimento definitivo.
2.9	Emissão do Termo de Recebimento Definitivo	Fiscal Técnico Fiscal Requisitante Gestor do Contrato	Em até 10 (dez) dias úteis após o recebimento relatório de final do projeto.	1. Emitir o Termo de Recebimento Definitivo. 2. Emite autorização para Faturamento.
3 - DO FATURAMENTO				
3.1	Emissão das Notas Fiscais para Faturamento	CONTRATADA	Após a autorização de Faturamento.	1. Emissão da Nota Fiscal de faturamento contendo o detalhamento dos serviços executados, número de série dos equipamentos, quantidades e valores unitários e os materiais e serviços empregados, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pela CONTRATADA.
3.2	Realizar Pagamento	Fiscal Técnico Fiscal Administrativo Gestor do Contrato	Até 30 (trinta) dias úteis após o recebimento da Nota Fiscal de Faturamento.	1. Elabora despacho de pagamento para o Fiscal Administrativo; 2. Realiza a análise de certidões e conformidades, elabora despacho para Área Financeira; 3. Realiza o Pagamento. - o No caso do atraso de pagamento por conta da administração, sugere-se em caso de cobrança das multas e juros previstas em lei por este atraso, que esta se dê por meio de cobrança separada do faturamento ordinário.

Tabela 6 - Principais etapas da execução contratual.

12.9. DOS CRITÉRIOS DE ACEITAÇÃO DOS SERVIÇOS E BENS FORNECIDOS (IN 94/2022 SGD/ME - Art. 19, inciso I)

12.9.1. APÓS A IMPLANTAÇÃO DA SOLUÇÃO:

I - Será realizada a aferição da capacidade e cobertura, utilizando a informação obtida pelo sistema de gerenciamento e monitoramento da solução Wi-Fi, devendo ficar evidenciado a cobertura da rede Wi-Fi nas áreas implantadas e as funcionalidades de controle de acesso estão de acordo com as especificações deste Termo de Referência.

12.9.2. APÓS A REALIZAÇÃO DO TREINAMENTO:

I - O HUB-UnB poderá acompanhar e avaliar a capacitação, com pesquisa de satisfação e, caso a mesma não atinja pontuação superior a 80% (oitenta por cento), esta deverá ser reestruturada e aplicada novamente, sem nenhum custo adicional para o HUB-UnB.

12.10. DOS PROCEDIMENTOS DE TESTE E INSPEÇÃO (IN 94/2022 SGD/ME - Art. 19, inciso II)

12.10.1. O procedimento de comprovação do atendimento aos requisitos técnicos da solução de rede Wi-Fi, será realizado através da análise de documentos comprobatórios (*datasheets e ou* manuais), emitidos pelo fabricante do equipamento, disponibilizado pela proponente.

12.11. DA FIXAÇÃO DOS VALORES E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO (IN 94/2022 SGD/ME - Art. 19, inciso III)

12.11.1. Caso a CONTRATADA não atinja os valores mínimos aceitáveis fixados neste Termo de Referência, não venha a produzir os resultados esperados, deixe de executar as atividades contratadas, deixe de utilizar os materiais e recursos humanos exigidos para fornecimento da solução, ou utilize-os com qualidade ou quantidade inferior à demandada, estará sujeita a aplicação de glosas nos valores estabelecidos para multas e/ou penalidades ou retenção do pagamento até que as pendências sejam sanadas.

13. DA GESTÃO E FISCALIZAÇÃO CONTRATUAL (IN 94/2022 SGD/ME - ART. 19)

13.1. Os critérios referentes ao modelo de gestão do contrato estão definidos no instrumento contratual.

14. DAS SANÇÕES ADMINISTRATIVAS APLICÁVEIS (IN 94/2022 SGD/ME - ART. 19, INCISO IV)

14.1. Os critérios referentes a sanções administrativas estão definidos no instrumento contratual.

15. DOS PROCEDIMENTOS PARA O PAGAMENTO (IN 94/2022 SGD/ME - ART. 19, INCISO V)

15.1. O pagamento deverá ser precedido da conclusão dos serviços e entrega completa dos bens que compõem a solução.

15.2. O pagamento será efetuado até o 30º (trigésimo) dia útil, a contar da emissão da nota fiscal de faturamento, após o ateste da conclusão da entrega da solução e os serviços relacionados.

15.3. A CONTRATADA somente poderá emitir a nota fiscal de faturamento após autorização do Fiscal Técnico com a emissão do Termo de Recebimento Definitivo.

15.4. O valor faturado deverá ter descontado os valores oriundos da aplicação de eventuais glosas ou sanções, caso existam.

15.5. Constatando alguma incorreção nas notas fiscais que desaconselhe o seu pagamento, o prazo será contado a partir da respectiva regularização. O uso da carta de correção será admitido nos casos previstos pelas legislações tributárias.

15.6. A nota fiscal deverá ser emitida em favor do HUB-UnB, conforme endereço e CNPJ constante no Contrato.

15.7. Deverá ser indicado na nota fiscal o número deste contrato, o mês de referência, a quantidade consumida de cada item da solução, a descrição do item, o número de série do bem quando couber, o valor unitário, o valor total, a referência à(s) Ordem de Serviço(s), o nome do banco, a agência e número da conta corrente onde será efetuado o pagamento.

15.8. Os valores dos tributos incidentes sobre os serviços ora contratados deverão ser destacados na respectiva nota fiscal, sempre que a legislação tributária permitir, sendo certo que, no preço ajustado, já estarão inclusos os valores dos referidos tributos.

15.9. O atraso nos pagamentos devidos, motivados por descumprimento de obrigações da CONTRATADA, decorrentes de decisões relativas a multas ou outras sanções e seus recursos, não gera direito a reajustamento, correção ou quaisquer ônus adicionais para o HUB-UnB.

15.10. Os pagamentos efetuados à CONTRATADA não a isentarão de suas obrigações e responsabilidades vinculadas ao fornecimento, especialmente aquelas relacionadas com a qualidade do serviço.

15.11. Os custos de eventuais erros de recolhimentos de impostos sob a responsabilidade do HUB-UnB, em decorrência de informações incorretas por parte da CONTRATADA, serão cobrados desta, observando os princípios de direito ao contraditório, ampla defesa e a compatibilidade com a legislação tributária, a ressarcir a CONTRATANTE, sujeita às penalidades previstas no contrato.

15.12. A documentação de cobrança não aceita pelo HUB-UnB será devolvida à CONTRATADA para a devida correção, com as informações que motivaram sua rejeição pela fiscalização.

15.13. A devolução da documentação de cobrança, não aprovada pelo HUB-UnB, não servirá de motivo para que a CONTRATADA suspenda a execução dos serviços.

15.14. O valor referente à multa será descontado de qualquer fatura ou crédito existente no HUB-UnB em favor da CONTRATADA. Caso esse valor seja superior ao crédito eventualmente existente, a diferença será cobrada em fatura posterior ou administrativamente ou judicialmente, se necessário.

15.15. No caso de atraso pela Contratante, os valores devidos à contratada 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.

16. DO ENCERRAMENTO CONTRATUAL (IN 94/2022 SGD/ME - ART. 35)

16.1. A CONTRATADA deverá garantir que a solução continue operacional, com todas as funcionalidades descritas neste Termo de Referência, habilitadas, mesmo após o encerramento da garantia. Sem obrigação de disponibilizar novas atualizações por parte do fabricante;

16.2. A CONTRATADA deverá entregar as versões finais dos produtos e da documentação;

16.3. O HUB-UnB deverá cancelar todos os perfis de acesso da CONTRATADA em seu ambiente computacional, providos durante a execução do contrato;

16.4. O HUB-UnB deverá inativar as caixas postais da CONTRATADA, se aplicável;

16.5. O HUB-UnB deverá realizar o encerramento administrativo do contrato, com a devida baixa de pendências de pagamentos e demais pendências em aberto;

16.6. O HUB-UnB deverá emitir o Termo de Encerramento Contratual (**MODELO DO TERMO DE ENCERRAMENTO DO CONTRATO - ENCARTE VII**), que deverá ser assinado pelo representante legal da CONTRATADA.

17. ESTIMATIVA DE PREÇOS DA CONTRATAÇÃO (IN 94/2022 SGD/ME - ART. 20)

17.1. Em atenção ao Art. 30 do Regulamento de Compras e Contratos da HU Brasil (Art. 34, *caput*, da Lei 13.303, de 2016), a **estimativa de preços da contratação** será **sigilosa**.

17.2. O detalhamento da pesquisa de preços encontra-se no processo SEI nº 23522.021199/2025-82, o qual será anexado ao presente processo após a fase externa da licitação.

17.3. O prazo de vigência da ata de registro de preços será de 12 meses, contado do primeiro dia útil subsequente à data de divulgação no PNCP, e poderá ser prorrogado por igual período, desde que comprovado que o preço é vantajoso (Art.99, *caput*, do RCC 3.0).

18. DA ADEQUAÇÃO ORÇAMENTÁRIA E O CRONOGRAMA FÍSICO-FINANCEIRO (IN 94/2022 SGD/ME - ART. 21)

18.1. A contratação prevista neste Termo de Referência será processada pelo Sistema de Registro de Preços - SRP, portanto, a indicação da dotação orçamentária ocorrerá somente no momento da formalização do contrato, nos termos do art. 17 do Decreto nº. 11.462/2023.

18.2. Quanto ao cronograma físico-financeiro dos itens do Grupo 1:

#	EVENTO	PRAZO	PERCENTUAL PAGO
1	Emitir a Ordem de Serviço	Dia D após a assinatura do contrato	0% (zero)
2	Elaborar o plano de projeto	Até 30 (trinta) dias corridos após o evento #1	0% (zero)
3	Realizar a entrega dos equipamentos	Até 60 (sessenta) dias corridos após o evento #1	0% (zero)
4	Emissão do Termo de Recebimento Provisório (TRP)	Até 7 (sete) dias corridos, após a conclusão do evento #3	0% (zero)
5	Realizar a implantação da solução	Até 30 (trinta) dias corridos, após a conclusão dos eventos #2 e #3.	0% (zero)
6	Realizar treinamento para repasse de conhecimento	Iniciado em até 7 (sete) dias corridos, após a conclusão do evento #5	0% (zero)
7	Emissão do Termo de Recebimento Definitivo (TRD)	Até 14 (quatorze) dias corridos, após a conclusão do evento #5 e #6.	0% (zero)
8	Emissão do Faturamento	Após o evento #7.	0% (zero)
9	Ateste e Realização do Pagamento	Até 30 (trinta) dias corridos, após o evento #8.	100% (cem por cento)

Tabela 9 - etapas do cronograma físico-financeiro do Grupo 1.

18.3. Quanto ao cronograma físico-financeiro dos itens do item 8 (Item avulso):

		PERCENTUAL
Termo de Referência - TI - SEI 58654735		SEI 23522.034786/2025-31 / pg. 38

#	EVENTO	PRAZO	PAGO
1	Emitir a Ordem de Serviço	Dia D após a assinatura do contrato	0% (zero)
2	Elaborar o site survey	Até 30 (trinta) dias corridos após o evento #1	0% (zero)
3	Realizar a entrega dos relatórios do site survey	Até 14 (quatorze) dias corridos após o evento #1	0% (zero)
4	Emissão do Termo de Recebimento Provisório (TRP)	Até 7 (sete) dias corridos, após a conclusão do evento #3	0% (zero)
5	Emissão do Termo de Recebimento Definitivo (TRD)	Até 14 (quatorze) dias corridos, após a conclusão do evento #4.	0% (zero)
6	Emissão do Faturamento	Após o evento #5.	0% (zero)
7	Ateste e Realização do Pagamento	Até 30 (trinta) dias corridos, após o evento #6.	100% (cem por cento)

Tabela 10 – etapas do cronograma físico-financeiro do item 8.

19. DO REGIME DE EXECUÇÃO (IN 94/2022 SGD/ME - ART. 22)

19.1. O Objeto deste contrato será executado sob o regime de contratação por empreitada integral, em conformidade com o Inciso III, Art. 22, IN 94/2022 SGD/ME;

"contratação de empreendimento em sua integralidade, compreendida a totalidade das etapas de serviços e instalações necessárias, sob inteira responsabilidade do contratado até sua entrega ao contratante em condições de entrada em operação, com características adequadas às finalidades para as quais foi contratado e atendidos os requisitos técnicos e legais para sua utilização com segurança estrutural e operacional"

19.2. E conforme o disposto no inciso IV, art. 9º, do Regulamento de Compras e Contratos da HU Brasil;

20. DOS CRITÉRIOS TÉCNICOS PARA SELEÇÃO DO FORNECEDOR (IN 94/2022 SGD/ME - ART. 23)

20.1. As empresas, deverão comprovar, ainda, a qualificação técnica, por meio da comprovação de aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis com o objeto desta licitação ou com o grupo pertinente, mediante a apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado.

20.2. A licitante vencedora do Grupo 1 deverá apresentar, juntamente com a proposta, atestado de capacidade técnica, emitido por pessoa jurídica de direito público ou privado, comprovando o fornecimento de uma solução semelhante, com no mínimo **100 (cem) Access Points**, o que representa 20% (vinte por cento) da capacidade total da solução de rede Wi-Fi pretendida. Para comprovação deste requisito, serão aceitos atestados combinados.

20.3. A licitante vencedora do item 8 (item avulso) deverá apresentar comprovação de experiência técnica por meio de atestado(s) de capacidade técnica, fornecido(s) por pessoa(s) jurídica(s) de direito público ou privado, que comprovem a execução anterior de site survey para redes sem fio corporativas de médio ou grande porte com, no mínimo, 100 (cem) pontos de acesso, a fim de assegurar que a empresa possui experiência comprovada em projetos de complexidade e escala compatíveis com o objeto da contratação.

20.3.1. Para fins de comprovação deste requisito, serão aceitos atestados combinados, de modo a permitir a soma de experiências similares e ampliar a competitividade, mantendo a exigência de qualificação técnica compatível com o porte do projeto.

20.4. Os atestados devem conter nome (razão social), CNPJ e endereço completo do órgão emitente do atestado e licitante vencedora, características dos serviços realizados, data de emissão, nome, cargo, telefone e assinatura do responsável pela emissão do atestado, em papel timbrado;

20.5. Os atestados solicitados visam garantir que as licitantes tenham condições de cumprir as obrigações objeto do contrato licitado, observando-se a comprovação da aptidão para o desempenho de atividade similar e compatível com o negócio praticado pela licitante vencedora.

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

20.7. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação de diferentes atestados.

20.8. No caso de atestados emitidos por empresa da iniciativa privada, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa proponente. Serão considerados como pertencentes ao mesmo grupo empresarial da empresa proponente, empresas controladas ou controladoras da empresa proponente, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da empresa proponente.

20.9. A licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, podendo ser exigida, nos casos de dúvida justificada por parte do agente de licitação, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços."

20.10. A licitante deverá indicar, claramente, quais itens do atestado apresentado, correspondem aos exigidos

neste certame para habilitação técnica. Tal indicação pode ser realizada por relatório adicional que correlacione o atestado com os itens do Termo de Referência ou Contrato que originou o atestado de capacidade técnica apresentado.

20.11. O HUB-UnB poderá realizar diligências para averiguação da autenticidade dos atestados.

20.12. O critério de julgamento adotado será o de menor preço GLOBAL. Modo de disputa aberto, intervalo mínimo entre lances 0,75%.

20.12.1. Será considerado vencedor o licitante que ofertar a proposta classificada em 1ª lugar, com o menor preço global e que atenda a todas as especificações e exigências estabelecidas neste Termo de Referência e seus anexos.

20.12.2. Serão consideradas inexecutáveis as propostas cujos preços unitários ou globais se revelem insuficientes para a execução do objeto, observados os parâmetros do art. 59 da Lei 14.133/2021.

20.12.3. Ainda que a licitação seja do tipo menor preço global, os preços unitários deverão guardar coerência com os valores de mercado constantes da planilha estimativa.

20.13. As exigências de habilitação jurídica, regularidade fiscal, seguridade social e trabalhista e capacidade econômico-financeira estão previstas no Edital.

20.14. NA FASE DE HABILITAÇÃO:

I - A licitante deverá anexar à Proposta de Preços (**MODELO DA PROPOSTA DE PREÇOS - ENCARTE I**) a correlação entre os requisitos técnicos deste Termo de Referência e seus anexos, com os equipamentos e sistemas ofertados que compõem a solução de rede Wi-Fi, indicando a referência de cada item da especificação. **A licitante que não apresentar a devida correlação terá sua proposta desclassificada.**

II - A licitante deverá anexar à proposta de preço as informações técnicas do próprio fabricante ou por ele atestadas, conforme parâmetros estabelecidos neste Termo de Referência, a fim de possibilitar a verificação objetiva da compatibilidade e aderência dos equipamentos ofertados às especificações técnicas exigidas

21. DO REAJUSTE DE PREÇOS (IN 94/2022 SGD/ME - ART. 24)

21.1. O reajuste de preços esta definido no instrumento contratual.

22. DA NECESSIDADE DE REALIZAÇÃO DE PROVA DE CONCEITO (IN 94/2022 SGD/ME - ART. 12, § 1º)

22.1. Não será realizada prova de conceito.

23. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO (IN 94/2022 SGD/ME - ART. 12, § 2º, INCISO I)

23.1. A Súmula nº 247/TCU dispõe que é obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala.

23.2. A solução de rede Wi-Fi necessária é composta por um conjunto de componentes que se inter-relacionam para produzir os resultados esperados para a contratação. A separação total destes componentes compromete o conjunto da solução, **logo optou-se pelo não parcelamento da composição do objeto do Grupo 1.**

23.3. Em atenção aos Acórdãos 2.977/2012-TCU-Plenário, 2.695/2013-TCU-Plenário, 343/2014-TCU-Plenário, 4.205/2014-TCU-1ª Câmara, 757/2015-TCU-Plenário, 588/2016-TCU-Plenário, 2.901/2016-TCU-Plenário e 3.081/2016-TCU-Plenário, a licitação será realizada em dois grupos, subdivido em itens, de modo a ampliar a concorrência, sem deixar de observar a interoperabilidade dos equipamentos e funcionalidades desejadas.

23.4. O Grupo 1 será adjudicado a um **único fornecedor**, uma vez que se refere a uma solução única e integrada de tecnologia da informação, composta por diversos itens que, por sua natureza, operam de forma interdependente. Os benefícios esperados somente serão plenamente alcançados mediante a aquisição e implantação da solução completa e coesa.

23.5. O item 8, referente ao serviço de *site survey*, que será contratado separadamente, **não deverá ser adjudicado ao mesmo fornecedor do Grupo 1.**

23.5.1. Com a vedação, fica estabelecida, de forma objetiva, a regra de que licitantes poderão disputar ambos os itens, sendo, contudo, vedada a acumulação na adjudicação, de modo a preservar os princípios da competitividade, economicidade, proporcionalidade e motivação.

24. DA PARTICIPAÇÃO DE CONSÓRCIO E DA SUBCONTRATAÇÃO (IN 94/2022 SGD/ME - ART. 12, § 2º, INCISO II)

24.1. Face ao objeto de contratação, que prevê a *"aquisição de Solução de Rede sem fio WLAN - Wi-Fi, com fornecimento de equipamentos, sistema de gerenciamento integrado, sistema de controle de acesso - NAC, serviço de instalação, configuração e treinamento, garantia e suporte técnico on-site por 60 meses para atender o HUB-UnB e serviço de site survey"*, a figura do consórcio não se justifica, dado que não há demanda que necessite de forças de trabalho diferentes ou dispersas para atendimento do objeto.

24.2. Os potenciais fornecedores dos componentes previstos no objeto da contratação, tem plena condição de ofertar todos os itens previstos em cada grupo sem a necessidade de estabelecimento de Consórcio entre empresas. Durante o estudo foram consultados diversos certames da mesma natureza e notou-se como padrão a vedação da participação de consórcios o que demonstra ser prática de mercado.

24.3. Assim, o presente Termo de Referência não prevê as condições de participação de empresas reunidas em consórcio, vez que a experiência prática demonstra que as licitações que permitem essa participação são aquelas que envolvem serviços de grande vulto e/ou de alta complexidade técnica. Como o presente Termo foi elaborado com foco em práticas usuais e de amplo domínio do mercado fornecedor, consignou-se a vedação acima.

24.4. Destarte, caso fosse permitida a formação de consórcio, ao contrário do esperado, poderia ocorrer restrição à competição, caso dois ou mais fornecedores em potencial, viessem a formar consórcio para a participação no certame.

24.5. Não será permitida subcontratação total do objeto, a transferência ou a cessão das obrigações contratuais a terceiros.

25. ENQUADRAMENTO DO OBJETO COMO BENS E SERVIÇOS COMUNS (IN 94/2022 SGD/ME - ART. 25, PARÁGRAFO ÚNICO)

25.1. A presente contratação se enquadra no rol de bens e serviços comuns de TIC, por possuir padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, conforme previsto no Regulamento de Compras e Contratos e nos termos do Art. 2º, Inciso XXXII da IN 94 de 2022, devendo ser contratada por intermédio da modalidade Pregão:

"XXXII - bens e serviços comuns: aqueles cujos padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado;"

25.2. A prestação dos serviços relacionados às soluções não gera vínculo empregatício entre os empregados da CONTRATADA e o HUB-UnB, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta, assim não há o que se pensar em dedicação de mão de obra exclusiva.

25.3. Neste sentido, deve-se registrar que os requisitos de qualificação técnica e desempenho necessários para a prestação do serviço explicitado no Termo de Referência, foram objetivamente definidos por meio de especificações usuais praticadas no mercado e representa a real demanda o HUB-UnB, razão pela qual será adotado o critério de **MENOR PREÇO POR GRUPO** para o julgamento objetivo das propostas.

26. DA ALTERAÇÃO SUBJETIVA

26.1. É admissível a fusão, cisão ou incorporação da CONTRATADA com/em outra pessoa jurídica, desde que:

I - Sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original;

II - Sejam mantidas as demais cláusulas e condições do contrato;

III - Não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da administração quanto a continuidade do contrato.

27. DA VIGÊNCIA CONTRATUAL

27.1. O prazo de vigência do contrato para os itens do grupo 1 será de 8 (oito) meses, com início na data da última assinatura pelas partes, prorrogável na forma do art. 188 do RCC 3.0.

27.2. O prazo de vigência do contrato para o item 8 (item avulso) será de 5 (cinco) meses, com início na data da última assinatura pelas partes, prorrogável na forma do art. 188 do RCC 3.0.

27.3. O cronograma de execução está definido no Item 18 deste Termo de Referência.

28. DA GARANTIA CONTRATUAL

28.1. Será exigida a garantia da contratação de que trata o art. 185 do RCC 3.0, com validade durante a execução do contrato e 90 (noventa) dias após término da vigência contratual, podendo a CONTRATADA optar pela caução em dinheiro, seguro-garantia, fiança bancária ou título de capitalização, em valor correspondente a 0,5% (meio por cento) do valor total da contratação.

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

assinatura do contrato.

28.2.1. A apólice de seguro-garantia permanecerá em vigor mesmo que a CONTRATADA não pague o prêmio nas datas convencionadas.

28.2.2. Caso a adjudicatária não apresente a apólice de seguro de garantia antes da assinatura do contrato, ocorrerá a preclusão do direito de escolha dessa modalidade de garantia.

28.2.3. A apólice de seguro-garantia deverá acompanhar as modificações referentes à vigência do contrato principal mediante a emissão do respectivo endosso pela seguradora.

28.2.4. Será permitida a substituição da apólice de seguro-garantia na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto, ressalvados os períodos de suspensão contratual.

28.2.5. Caso a adjudicatária não opte pelo seguro-garantia ou não apresente a apólice de seguro de garantia antes da assinatura do contrato, deverá apresentar, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério da CONTRATANTE, contado da assinatura do contrato, comprovante de prestação de garantia nas modalidades de caução em dinheiro, fiança bancária ou títulos de capitalização.

28.3. Caso seja a garantia em dinheiro a modalidade de garantia escolhida pela CONTRATADA, deverá ser efetuada em favor da CONTRATANTE, em conta específica na Caixa Econômica Federal, com correção monetária.

28.4. No caso de garantia na modalidade de fiança bancária, deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

28.5. Na hipótese de opção pelo título de capitalização, a garantia deverá ser custeada por pagamento único, com resgate pelo valor total, sob a modalidade de instrumento de garantia, emitido por sociedades de capitalização regulamente constituídas e autorizadas pelo Governo Federal.

28.5.1. O título de capitalização deverá ser apresentado à CONTRATANTE juntamente com as condições gerais e o número do processo administrativo sob o qual o plano de capitalização foi aprovado pela Susep (art. 8º, III, da Circular SUSEP nº 656/2022).

28.6. A garantia assegurará, qualquer que seja a modalidade escolhida, sob pena de não aceitação, o pagamento de:

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

28.6.2. multas moratórias e punitivas aplicadas pela HU Brasil à CONTRATADA; e

28.6.3. obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pela CONTRATADA.

28.7. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada ou renovada, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, contado da data de assinatura do termo aditivo ou da emissão do apostilamento, seguindo os mesmos parâmetros utilizados quando da contratação.

28.8. Na hipótese de suspensão do contrato por ordem ou inadimplemento da HU Brasil, a CONTRATADA ficará desobrigada de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela HU Brasil.

28.9. Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a CONTRATADA obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério da CONTRATANTE, contados da data em que for notificada.

28.10. A CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.

28.10.1. O emitente da garantia ofertada pela CONTRATADA deverá ser notificado pela CONTRATANTE quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

28.10.2. Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep nº 662/2022.

28.11. Extinguir-se-á a garantia com a restituição da carta fiança, autorização para a liberação de importâncias depositadas em dinheiro a título de garantia ou anuência ao resgate do título de capitalização, acompanhada de declaração da CONTRATANTE, mediante termo circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do contrato.

28.11.1. A extinção da garantia na modalidade seguro-garantia observará a regulamentação da Susep.

28.11.2. A HU Brasil deverá apurar se há alguma pendência contratual antes do término da vigência da apólice.

28.12. A garantia somente será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por

culpa exclusiva da HU Brasil e, quando em dinheiro, será atualizada monetariamente.

28.13. A CONTRATADA autoriza a CONTRATANTE a reter, a qualquer tempo, a garantia, na forma prevista neste Termo de Referência.

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

28.15. A garantia de execução é independente de eventual garantia do produto ou serviço prevista neste Termo de Referência.”

29. DA GARANTIA E ASSISTÊNCIA TÉCNICA

29.1. Será exigida a prestação de garantia do produto/serviço na presente contratação, conforme regras constantes no item 7.12 deste Termo de Referência.

30. LISTA DE ANEXOS

30.1. São partes integrantes deste Termo de Referência os respectivos anexos:

- I - Modelo da Proposta de Preços (55417783);
- II - Modelo da Ordem de Serviço (55418156);
- III - Modelo do Termo de Compromisso (55420528);
- IV - Modelo do Termo de Ciência (55420674);
- V - Modelo do Termo de Recebimento Provisório (61900800);
- VI - Modelo do Termo de Recebimento Definitivo (55420949);
- VII - Modelo do Termo de Encerramento do Contrato (55421090);
- VIII - Mapa preditivo Wi-Fi - HUB-UnB (55421234);
- IX - Modelo de Declaração de Vistoria (61900678);
- X - Modelo de Declaração de dispensa de vistoria (61900717).

31. DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO

31.1. A Equipe de Planejamento da Contratação, foi instituída pela Portaria - SEI 731 (55351081) e publicada no Boletim de Serviço Nº 760, de 17 de novembro de 2025 (55400632).

31.2. Conforme o §6º do Art. 12 da IN SGD/ME nº 94, de 2022, O Termo de Referência será assinado pela Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC e aprovado pela autoridade competente.

Integrante Requisitante	Integrante Técnico	Integrante Administrativo
(assinado eletronicamente) HUGGO LOPES LIRA FERREIRA	(assinado eletronicamente) PAULO ALEXANDRE AGUEDA GOBBATO	(assinado eletronicamente) JAQUELINE JUSTINO DE OLIVEIRA

Ciente e de acordo,

(assinado eletronicamente)
FABIANO FRANCISCO NOETZOLD SALDANHA
Gestor de Tecnologia da Informação e Saúde Digital

 Documento assinado eletronicamente por **Paulo Alexandre Agueda Gobbato, Analista de Tecnologia da Informação**, em 22/06/2026, às 15:32, conforme horário oficial de Brasília, com fundamento no art. 6º, caput, do [Decreto nº 8.539, de 8 de outubro de 2015](#).

 Documento assinado eletronicamente por **Jaqueline Justino de Oliveira, Analista Administrativo**, em 22/06/2026, às 15:33, conforme horário oficial de Brasília, com fundamento no art. 6º, caput, do [Decreto nº 8.539, de 8 de outubro de 2015](#).

 Documento assinado eletronicamente por **Huggo Lopes Lira Ferreira, Analista de Tecnologia da Informação**, em 22/06/2026, às 15:33, conforme horário oficial de Brasília, com fundamento no art. 6º, caput, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Fabiano Francisco Noetzold Saldanha, Chefe de Setor**, em 24/06/2026, às 17:57, conforme horário oficial de Brasília, com fundamento no art. 6º, caput, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Wallace Enrico Boaventura Gonçalves dos Santos, Superintendente**, em 26/06/2026, às 12:03, conforme horário oficial de Brasília, com fundamento no art. 6º, caput, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site https://sei.ebserh.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **58654735** e o código CRC **9EDBA61E**.

Referência: Processo nº 23522.034786/2025-31 SEI nº 58654735