TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS
Av. André Araújo, S/N - Bairro Aleixo - CEP 69060-000 - Manaus - AM - www.tjam.jus.br

TERMO DE REFERÊNCIA

1. OBJETO DA CONTRATAÇÃO

1.1. Definição do Objeto: Aquisição de equipamentos, licenciamento, gerenciamento, serviços de instalação e configuração com banco de horas, conforme condições e exigências estabelecidas neste instrumento.

1.2. Justificativa para a aquisição/contratação:

1.2.1. IA modernização da infraestrutura de rede LAN do Tribunal de Justiça do Estado do Amazonas (TJAM) é fundamental para atender às demandas crescentes por conectividade, eficiência operacional e segurança da informação, alinhadas ao contexto de transformação digital em que a instituição está inserida.

1.2.2. A justificativa para a contratação encontra-se pormenorizada em tópico específico do Estudo Técnico Preliminar, anexo deste Termo de Referência.

1.3. Especificação técnica do Objeto e Quantitativo:

Item	Descrição	Quantidade
1	SWITCH GERENCIADO DE DISTRIBUIÇÃO (PARA UNIDADES COM ALTO TRÁFEGO DE DADOS)	2
2	SWITCH GERENCIADO DE ACESSO 48 PORTAS (PARA UNIDADES COM ALTO TRÁFEGO DE DADOS)	50
3	SWITCH GERENCIADO DE ACESSO BÁSICO 24 PORTAS COM POE (PARA UNIDADES COM BAIXO TRÁFEGO DE DADOS)	15
4	SWITCH GERENCIADO DE ACESSO BÁSICO 48 PORTAS COM POE (PARA UNIDADES COM BAIXO TRÁFEGO DE DADOS)	50
5	INTERFACE 10G ETHERNET PARA CURTA DISTÂNCIA	48
6	INTERFACE 10G ETHERNET PARA LONGA DISTÂNCIA	5
7	INTERFACE 40G ETHERNET	2
8	INTERFACE 100G ETHERNET - 100m	2
9	SOLUÇÃO DE CONTROLE DE ACESSO PARA 4500 USUÁRIOS OU DISPOSITIVOS	1
10	INSTALAÇÃO DE SWITCH GERENCIADO	117
11	IMPLEMENTAÇÃO DA SOLUÇÃO PARA CONTROLE DE ACESSO	1
12	BANCO DE HORAS PARA SERVIÇOS AVANÇADOS	142
13	TREINAMENTO OFICIAL DO FABRICANTE	1

14	SOLUÇÃO DE CONTROLE DE ACESSO PARA 1000 USUÁRIOS OU DISPOSITIVOS	1
15	SOLUÇÃO DE CONTROLE DE ACESSO PARA 2500 USUÁRIOS OU DISPOSITIVOS	1

1.3.1. A solução deverá permitir o gerenciamento centralizado dos switches através de um único sistema ou console.

1.3.1.1. Caberá à CONTRATADA implantar um sistema de gerenciamento unificado que permita a administração centralizada de todos os componentes da rede.

1.3.2. A solução abrange a aquisição, instalação, configuração e manutenção de equipamentos de rede, além de treinamento técnico e suporte especializado.

1.3.3. As especificações técnicas que detalham os bens e serviços objeto desta contratação estão descritos no Anexo I deste Termo de Referência.

1.4. Caracterização do Objeto:

1.4.1. O objeto do presente Termo de Referência se enquadra na definição de bens e serviços comuns, nos termos do inciso XIII, Art. 6º da Lei nº 14.133/2021.

1.4.3. A aquisição do material decorrente do Registro de Preços será realizada de acordo com a necessidade e conveniência do Tribunal de Justiça do Amazonas, mediante a emissão de requisição de fornecimento e da Nota de Empenho.

1.5. Fundamentação Legal:

1.5.1. A contratação/aquisição para a execução do objeto deverá obedecer, no que couber, ao disposto na legislação a seguir:

a) Lei nº 14.133, de 1º de abril de 2021;

b) Resolução n.º 64/2023, de 5 de dezembro de 2023;

c) Resolução CNJ nº. 468, de 15 de julho de 2022.

1.6. Indicação de necessidade de apresentação de amostras, catálogos, manuais, folders ou prospectos:

1.6.1. Apresentar catálogo ou prospecto, ou documento equivalente, em português ou inglês, com especificações técnicas da marca e modelo cotado, para verificação da compatibilidade com as especificações solicitadas.

1.7. Valor estimado da contratação:

1.7.1. A estimativa de valor da contratação será discriminada no Mapa de Preços a ser elaborado pela Divisão de Compras e Operações.

1.7.2. Tabela exemplificativa de cotação:

Item	Descrição	Quantidade	Valor Unitário	Valor Total
1	SWITCH GERENCIADO DE DISTRIBUIÇÃO (PARA UNIDADES COM ALTO TRÁFEGO DE DADOS)	2		
2	SWITCH GERENCIADO DE ACESSO 48 PORTAS (PARA UNIDADES COM ALTO TRÁFEGO DE DADOS)	50		
3	SWITCH GERENCIADO DE ACESSO BÁSICO 24 PORTAS COM POE (PARA	15		

	UNIDADES COM BAIXO TRÁFEGO DE DADOS)			
4	SWITCH GERENCIADO DE ACESSO BÁSICO 48 PORTAS COM POE (PARA UNIDADES COM BAIXO TRÁFEGO DE DADOS)	50		
5	INTERFACE 10G ETHERNET PARA CURTA DISTÂNCIA	48		
6	INTERFACE 10G ETHERNET PARA LONGA DISTÂNCIA	5		
7	INTERFACE 40G ETHERNET	2		
8	INTERFACE 100G ETHERNET - 100m	2		
9	SOLUÇÃO DE CONTROLE DE ACESSO PARA 4500 USUÁRIOS OU DISPOSITIVOS	1		
10	INSTALAÇÃO DE SWITCH GERENCIADO	117		
11	IMPLEMENTAÇÃO DA SOLUÇÃO PARA CONTROLE DE ACESSO	1		
12	BANCO DE HORAS PARA SERVIÇOS AVANÇADOS	142		
13	TREINAMENTO OFICIAL DO FABRICANTE	1		
14	SOLUÇÃO DE CONTROLE DE ACESSO PARA 1000 USUÁRIOS OU DISPOSITIVOS	1		
15	SOLUÇÃO DE CONTROLE DE ACESSO PARA 2500 USUÁRIOS OU DISPOSITIVOS	1		

1.8. <u>Adequação orçamentária:</u>

1.8.1. A aquisição pretendida está prevista no Plano de Contratação Anual 2024, sob os Códigos **SETIC-2024-20, SETIC-2024-21, SETIC-2024-22, SETIC-2024-23 e SETIC-2024-24.**

2. CONDIÇÕES GERAIS DA CONTRATAÇÃO

2.1. O objeto deste Termo de Referência caracteriza-se como situação prevista na modalidade Pregão, sob a forma Eletrônica, nos termos do artigo 28, inciso I da, Lei nº 14.133/2021.

2.2. A presente contratação adotará como regime de execução a Empreitada por Preço unitário.

2.3. O procedimento para a contratação pretendida neste instrumento será regido pelo Sistema de Registro de Preços.

2.4. O critério de julgamento será o de **MENOR PREÇO GLOBAL.**

2.5. O critério de adjudicação da contratação será GLOBAL, levando em consideração o prejuízo de ordem técnica que poderia ocorrer caso os serviços fossem prestados por diferentes empresas, uma vez que os serviços a serem contratados guardam estreita relação entre si e dependem de forte integração para que sejam efetivos e alcancem os resultados pretendidos.

2.6. Não será permitida a subcontratação do objeto deste Termo de Referência.

3. REQUISITOS DO FORNECEDOR

3.1. Vistoria:

3.1.1. Para a execução do objeto, a vistoria é facultativa. Caso o licitante tenha interesse em realizar vistoria para levantamento de necessidades específicas nos locais de instalação informados no Anexo II deste Termo de Referência, deverá entrar em contato através do e-mail setic@tjam.jus.br

3.1.2. A não realização de vistoria não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da execução do objeto, devendo o interessado assumir o ônus dos serviços decorrentes.

3.1.3. A vistoria poderá ser substituída, quando for o caso, por declaração formal assinada pelo responsável técnico do licitante acerca do conhecimento pleno das condições e peculiaridades da contratação.

3.2. Capacidade Técnica:

3.2.1. As licitantes deverão encaminhar a seguinte documentação complementar para verificação da sua Qualificação Técnica:

a) Apresentação da proposta contendo a descrição detalhada do objeto ofertado juntamente com os documentos exigidos no item 1.6.1 deste Termo de Referência;

b) Apresentação de documento declarando ter capacidade técnica para atender a todos os requisitos especificados no Termo de Referência;

c) Comprovação de aptidão para o fornecimento de serviços similares, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado. São considerados serviços similares: fornecimento de switches e acessórios, incluindo os serviços de instalação, configuração e manutenção de equipamentos de rede, além de treinamento técnico e suporte especializado, com características semelhantes e compatíveis com as descritas neste Termo de Referência.

4. MODELO DE GESTÃO

4.1. A fiscalização do objeto será realizada pela Secretaria de Tecnologia da Informação.

4.1.1. A execução do objeto deverá ser acompanhada e fiscalizada por servidor designado como responsável ou por seu substituto.

4.1.2. A Secretaria de Tecnologia da Informação será responsável pela avaliação da conformidade dos materiais/equipamentos, e anotará em registro próprio todas as ocorrências relacionadas à falhas ou problemas observados, determinando o que for necessário à regularização das mesmas.

4.1.3. A existência da fiscalização de nenhum modo diminui ou altera a responsabilidade do fornecedor na total execução do objeto.

4.1.4. Deverá ser mantido preposto, aceito pela CONTRATANTE, durante o período de execução do objeto, para representá-lo sempre que for necessário.

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

4.3. Indicação de instrumento para efetivar a contratação:

4.3.1 Será necessária a formalização de contrato para a execução do serviço objeto desse termo.

4.3.2. Após a assinatura do contrato, o órgão poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano

complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

4.4. Vigência contratual:

4.4.1 A vigência do contrato a ser firmado será de 12 (doze) meses, podendo ser prorrogado nos termos dos arts. 105 e seguintes da Lei n.° 14.133/21.

4.5. Índice de reajuste:

4.5.1. Os preços contratados poderão ser reajustados, após solicitação da CONTRATADA, observado o interregno mínimo de 12 (doze) meses, tendo como limite máximo a variação do Índice de Custos de Tecnologia da Informação - ICTI, ocorrida nos últimos 12 (doze) meses.

4.6. Será necessária a formalização de Ata de Registro de Preços.

4.6.1. O prazo de vigência da ata de registro de preços será de 1 (um) ano e poderá ser prorrogado, por igual período, desde que comprovado o preço vantajoso.

4.6.2. Os órgãos e entidades poderão aderir à ata de registro de preços na condição de não participantes, observados os seguintes requisitos:

I - apresentação de justificativa da vantagem da adesão, inclusive em situações de provável desabastecimento ou descontinuidade de serviço público;

II - demonstração de que os valores registrados estão compatíveis com os valores praticados pelo mercado;

III - prévias consulta e aceitação do órgão ou entidade gerenciadora e do fornecedor.

4.6.3. A faculdade de aderir à ata de registro de preços na condição de não participante poderá ser exercida:

I - por órgãos e entidades da Administração Pública federal, estadual, distrital e municipal, relativamente a ata de registro de preços de órgão ou entidade gerenciadora federal, estadual ou distrital; ou

4.6.4. As aquisições ou as contratações não poderão exceder, por órgão ou entidade, a 50% (cinquenta por cento) dos quantitativos dos itens do instrumento convocatório registrados na ata de registro de preços para o órgão gerenciador e para os órgãos participantes.

4.6.5. O quantitativo decorrente das adesões à ata de registro de preços não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o órgão gerenciador e órgãos participantes, independentemente do número de órgãos não participantes que aderirem.

5. OBRIGAÇÕES DA CONTRATADA E DO CONTRATANTE.

5.1. São obrigações e responsabilidades do CONTRATANTE:

5.1.1. Efetuar os pagamentos nas condições e preços pactuados.

5.1.2. Promover o acompanhamento e a fiscalização da execução do objeto, sob os aspectos quantitativos e qualitativos, anotando em registro próprio as faltas detectadas e comunicando à empresa as ocorrências de qualquer fato que, a seu critério, exija medidas por parte daquela.

5.1.3. Rejeitar, no todo ou em parte, os materiais entregues em desacordo com as exigências deste Termo.

5.1.4. Notificar por escrito a ocorrência de eventuais imperfeições na execução do objeto, fixando prazo para a sua correção.

5.1.5. Proporcionar todas as facilidades para que ocorra a correta execução do objeto.

5.1.6. Comunicar qualquer irregularidade ou ilegalidade encontrada no fornecimento do objeto.

5.1.7. Prestar as informações e os esclarecimentos atinentes à execução do objeto que venham a ser solicitados.

5.1.8. Solicitar o fornecimento do objeto deste Termo de Referência.

5.1.9. Fiscalizar e acompanhar a execução da Ata de Registro de Preços.

5.1.10. Manter sigilo e confidencialidade de todas as informações repassados em decorrência da execução contratual, em consonância com o disposto na Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

5.2. São obrigações e responsabilidades da CONTRATADA:

5.2.1. Executar o objeto desta contratação, atendendo às especificações estabelecidas neste Termo de Referência e as quantidades indicadas no instrumento contratual.

5.2.2. Manter todas as condições de habilitação e qualificação exigidas na licitação em compatibilidade com as obrigações assumidas.

5.2.3. Responsabilizar-se única e exclusivamente pelo pagamento de todos os encargos e demais despesas, diretas ou indiretas, decorrentes da execução do objeto do presente Termo de Referência, tais como impostos, taxas, contribuições fiscais, previdenciárias, trabalhistas, fundiárias; enfim, por todas as obrigações e responsabilidades, sem qualquer ônus adicional ao CONTRATANTE.

5.2.4. Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho quando, em caso de ocorrência, forem vítimas seus empregados no desempenho dos serviços ou em conexão com eles, ainda que ocorridos nas dependências do CONTRATANTE.

5.2.5. Cumprir os normativos e os procedimentos definidos pelo CONTRATANTE.

5.2.6. Primar pelo bom planejamento das atividades, utilizar as boas práticas e técnicas de governança, avaliar previamente a viabilidade técnica, os riscos e os impactos de suas ações.

5.2.7. Realizar a entrega do objeto em conformidade com os horários e períodos determinados pelo CONTRATANTE.

5.2.8. Submeter seus profissionais aos regulamentos de segurança e disciplina instituídos pelo CONTRATANTE, durante o tempo de permanência nas suas dependências.

5.2.9. Comunicar às unidades do CONTRATANTE responsáveis pela fiscalização do objeto, por escrito, qualquer anormalidade, bem como atender prontamente o que lhe for solicitado e exigido.

5.2.10. Responder por todas as despesas decorrentes do fornecimento.

5.2.11. Refazer todos os serviços que, a juízo do representante do CONTRATANTE, não forem considerados satisfatórios, sem que caiba qualquer acréscimo no custo contratado.

5.2.12. Não realizar, promover e incentivar a divulgação de qualquer dado ou informação do ambiente do CONTRATANTE.

5.2.13. Obedecer às normas internas do CONTRATANTE, relativas à segurança, à identificação, ao trânsito e à permanência de pessoas em suas dependências.

5.2.14. Manter sigilo e ciência das normas de segurança e privacidade vigentes no órgão, se responsabilizando por todos os seus empregados diretamente envolvidos na contratação.

5.2.15. Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto deste contrato, devendo orientar seus profissionais nesse sentido.

5.2.16. Tratar todas as informações a que tenha acesso, em caráter de estrita confidencialidade, não podendo, sob qualquer pretexto, divulgar, revelar, reproduzir, ou delas dar conhecimento a terceiros estranhos a esta contratação, bem como utilizá-las para fins diferentes dos previstos na presente contratação.

5.2.17. Acatar as determinações feitas pela fiscalização do CONTRATANTE no que tange ao cumprimento do objeto.

5.2.18. Prestar, de imediato, todos os esclarecimentos solicitados pela fiscalização do CONTRATANTE no que diz respeito a execução do objeto.

5.2.19. Fornecer os materiais, observadas rigorosamente as especificações constantes no Termo de Referência.

5.2.20. Observar conduta adequada na utilização dos materiais, equipamentos, ferramentas e utensílios.

5.2.21. Responder pelos vícios e defeitos dos materiais e serviços e assumir os gastos e as despesas que se fizerem necessários para adimplemento das obrigações decorrentes da execução do objeto.

5.2.22. Responsabilizar-se por danos causados ao patrimônio do CONTRATANTE, ou de terceiros, ocasionados por seus profissionais, em virtude de dolo ou culpa, durante a execução do objeto.

5.2.23. Notificar, formal e tempestivamente, a CONTRANTE sobre quaisquer irregularidades e inconformidades observadas durante a execução do objeto, bem como qualquer ocorrência relativa ao comportamento de seus empregados, quando em atendimento, que venha a ser considerada prejudicial ou inconveniente para a CONTRATADA.

5.2.24. Prestar as informações e os esclarecimentos que venham a ser solicitados pelo CONTRATANTE necessários à perfeita execução do objeto.

5.2.25. Manter sigilo e confidencialidade de todas as informações repassados em decorrência da execução contratual, em consonância com o disposto na Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

6. REGIME DE EXECUÇÃO

6.1. A execução do objeto deste Termo de Referência será por demanda.

6.2. A solicitação para início da execução dos serviços será com o acionamento de ARP e assinatura do contrato, etc. A comunicação será realizada por e-mail.

6.2.1. Os locais de execução dos serviços constam no Anexo II deste Termo de Referência.

6.3. As quantidades e o prazo de entrega do objeto que vier a ser adquirido será definido na respectiva Ordem de Fornecimento emitida pelo CONTRATANTE, sendo o prazo máximo de entrega de 90 (noventa) dias consecutivos a partir da emissão da Ordem de Fornecimento.
6.3.1. Excepcionalmente, o prazo de recebimento poderá ser prorrogado por até 30 (trinta) dias, desde que solicitado pelo fornecedor e com apresentação de justificativa, desde que em conformidade a Lei 14.133/2021 e legislação aplicável.

6.3.2. Toda prorrogação de prazo deverá ser justificada por escrito e previamente autorizada pela autoridade competente.

6.3.3. A contratada deverá transferir conhecimento técnico à equipe do TJAM, incluindo capacitação sobre a operação e manutenção dos equipamentos e sistemas adquiridos.

6.4. O objeto deste Termo de referência será recebido da seguinte forma:

6.4.1. **Provisoriamente**, no momento da entrega do objeto, pelo responsável por seu acompanhamento e fiscalização, mediante termo detalhado e assinado pelas partes, para efeito de verificação de conformidade com as especificações e exigências constantes neste Termo. Nesta etapa, o servidor ou a comissão designada procederá o recebimento do objeto limitando-se a verificar o discriminado na Nota Fiscal, e fazendo constar no canhoto e no verso da Nota Fiscal a data da entrega, e se for o caso, as irregularidades observadas.

6.4.2. **Definitivamente**, por servidor ou comissão designada pela autoridade competente, mediante termo detalhado e assinado pelas partes, no prazo de até 10 (dez) dias úteis, contados do recebimento provisório.

6.4.3. O objeto será recusado caso não atenda as especificações técnicas solicitadas no Termo de Referência, devendo a empresa providenciar os ajustes necessários para adequação, em um prazo de 10 (dez) dias contados a partir da comunicação, quando do não aceite.

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

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

6.8. Serviços de manutenção e assistência técnica:

6.8.1. Toda a solução deste Termo de Referência deverá considerar período de garantia por um prazo de pelo menos 36 (trinta e seis) meses para a solução como um todo (hardware e software), exceto para os switches, que deverão ter sua garantia do tipo *lifetime*, extensível pelo período mínimo de 05 anos após o *end of sales* do equipamento.

6.8.2. Conforme disposto na lei 14.133/2021, Art. 40, inciso V, alínea a) (V - atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho), todos os itens deverão ser do mesmo fabricante.

6.8.3. Os chamados serão abertos juntamente a autorizada oficial do fabricante no Brasil através de ligação telefônica gratuita (0800) no idioma português, website e e-mail durante a vigência da garantia. O suporte deverá ser na modalidade de 24x7 (24 horas por dia, 7 dias por semana) durante o prazo de garantia.

6.8.4. Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correção de bugs.

6.8.5. Em caso de defeitos de fabricação, a garantia deve incluir envio de peças ou equipamentos de reposição até o local onde o equipamento está instalado, obedecendo a modalidade NBD (*Next Business Day*);

7. PENALIDADES POR DESCUMPRIMENTO CONTRATUAL

7.1. Serão aplicadas as seguintes sanções no caso de descumprimento total ou parcial das regras estabelecidas no edital de licitação e no Contrato Administrativo e/ou Ata de Registro de Preços:

a) advertência;

b) multa;

c) impedimento de licitar e contratar;

d) declaração de inidoneidade para licitar ou contratar.

7.2. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas cumulativamente com a sanção de multa.

7.3. A sanção de impedimento de licitar e contratar com o ente federativo não poderá ser aplicada cumulativamente com a de declaração de inidoneidade.

7.4. A aplicação das sanções acima previstas não exclui a obrigação de reparação integral do dano causado à administração pública.

8. FORMA DE ACOMPANHAMENTO DO ATENDIMENTO AOS PRAZOS DE GARANTIA E NÍVEIS MÍNIMOS DE QUALIDADE ACEITÁVEL DE SERVIÇOS EXIGIDOS (NSE)

8.1. Os tempos de resposta e de solução para os chamados técnicos abertos serão contados a partir do registro dos mesmos através de contato telefônico ou por outro meio disponível.

8.2. Quanto aos níveis de SLA:

8.2.1. Ficam estabelecidos níveis mínimos de serviço a serem cumpridos pela CONTRATADA, com mensuração consolidada mensal e emissão de relatórios pelos fiscais do contrato para sua aferição.

8.2.2. O prazo de solução é o período compreendido entre a abertura do chamado pelo Tribunal e a solução efetiva do mesmo.

8.2.3. A Contratada deverá atender e solucionar todos os chamados, conforme os prazos estabelecidos.

8.2.4. Os prazos de atendimento definidos pelo Tribunal são os relacionados na tabela a seguir:

Falhas/Serviço	**Prazo de Solução**
Instabilidade do Sistema	6 Horas Úteis
Resolução de dúvidas de utilização	48 Horas

8.2.5. Na hipótese do descumprimento do nível de qualidade aceitável, o Tribunal poderá aplicar sanções administrativas, conforme tabela abaixo:

Serviço	Falhas	Grau da Infração	Tipo de Multa
Disponibilidade do Sistema	Atraso injustificado na instalação do sistema e habilitação dos usuários entre 6 a 12 horas consecutivas.	Descumprimento de obrigações contratuais, consideradas leves	1
	Atraso injustificado na instalação do sistema e habilitação dos usuários superior a 12 horas consecutivas.	Erros de execução do objeto	2
	Atraso injustificado na instalação do sistema superior a 12 horas consecutivas.	Execução imperfeita do objeto	3
Suporte Técnico	Chamados sem resposta entre 48 a 72 horas.	Descumprimento de obrigações contratuais, consideradas leves	1
	Chamados ao suporte em prazo superior a 72 horas.	Execução imperfeita do objeto	3

8.2.6. As penalidades a serem aplicadas pela Contratante estão discriminadas no Anexo III deste Termo de Referência.

9. FORMA DE PAGAMENTO

9.1. O pagamento será efetuado em até 30 (trinta) dias, mediante apresentação da Nota Fiscal/Fatura, após ser devidamente atestada a sua conformidade pelo Gestor designado para acompanhar e fiscalizar a execução.

9.2. Para fins de liquidação, o setor competente deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

a) o prazo de validade;

b) a data da emissão;

c) os dados do contrato e do órgão contratante;

d) o período respectivo de execução do contrato;

e) o valor a pagar; e

f) eventual destaque do valor de retenções tributárias cabíveis.

9.3. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus à contratante.

9.4. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta *on-line* ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais.

9.5. A Administração deverá realizar consulta ao SICAF para:

a) verificar a manutenção das condições de habilitação exigidas no edital;

b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

9.6. Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo

prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do contratante.

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

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

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

9.10. Considerando que a execução dos serviços será sob demanda, os pagamentos serão realizados para os itens efetivamente prestados, mediante apresentação da Nota Fiscal da empresa.

10. GARANTIA CONTRATUAL

10.1. Não será exigida garantia contratual para a execução do objeto deste Termo de Referência.

11. CRITÉRIOS E PRÁTICAS DE SUSTENTABILIDADE

11.1. A empresa contratada deverá contribuir para a promoção do desenvolvimento nacional sustentável no cumprimento de diretrizes e critérios de sustentabilidade ambiental, de acordo com o art. 225 da Constituição Federal de 1988, e em conformidade com o art. 5º da Lei nº 14.133/21.

11.2. Adicionalmente, a empresa contratada deverá, sempre que viável, observar as normas vigentes relacionadas à sustentabilidade ambiental e aderir às melhores práticas delineadas no Guia Prático de Critérios de Sustentabilidade para Compras no TJAM e Guia Nacional de Contratações Sustentáveis da AGU, durante a execução dos serviços.

11.3. Recomenda-se que a contratada deverá cumprir as cotas raciais, de gênero e de pessoas com deficiência.

11.4. Recomenda-se exigir da contratada um programa interno de treinamento visando a redução de consumo de energia elétrica, de consumo de água e redução de produção de resíduos sólidos.

11.5. Estabelecer a separação adequada e o descarte responsável de resíduos, incluindo a reciclagem de materiais quando aplicável.

11.6. Incentivar a redução de resíduos por meio de práticas de consumo consciente.

11.7. Fornecer aos empregados os equipamentos de segurança que se fizerem necessários para a execução de serviços e fiscalizar o uso.

11.8. Realizar a separação dos resíduos recicláveis descartados em função de seus serviços.

11.9. Respeitar as Normas Brasileiras – NBR publicadas pela Associação Brasileira de Normas Técnicas sobre resíduos sólidos.

11.10. No que diz respeito à gestão de resíduos, a contratada deve aderir às diretrizes estabelecidas na Lei nº 12.305/2010 - Política Nacional de Resíduos Sólidos, na Resolução nº 307/2002 do Conselho Nacional de Meio Ambiente (CONAMA), e na Instrução Normativa SLTI/MPOG n° 1/2010. A contratada assumirá como obrigações a aplicação de critérios e práticas sustentáveis, incorporando-as como especificações técnicas do objeto.

12. RESPONSÁVEIS PELO TERMO DE REFERÊNCIA

12.1. Subscrevem o Termo de Referência os servidores responsáveis por sua elaboração, nos moldes e parâmetros estabelecidos pelo Tribunal de Justiça do Estado do Amazonas. Além da exigência legal da aprovação da autoridade competente, o instrumento em tela carece da ratificação de que retrata o que fora ordenado aos responsáveis por sua elaboração.

13. DOS ANEXOS

13.1. São partes integrantes deste Termo de Referência os seguintes anexos:

a) Mapa de Gerenciamento de Riscos na Contratação;

b) Estudo Técnico Preliminar;

c) Mapa de Preços.

Manaus, *data do sistema*

Karla Rozeana Bau Zarth

Seção de Elaboração de Artefatos da Contratação

ANEXO I - ESPECIFICAÇÕES TÉCNICAS

1.ESPECIFICAÇÃO DOS BENS E SERVIÇOS QUE COMPÕE A INFRAESTRUTURA DA SOLUÇÃO DE LAN A SER ADQUIRIDA PELO TJAM

1.1.REQUISITOS GERAIS PARA PLATAFORMA DE GERENCIAMENTO DA SOLUÇÃO DE LAN

1.1.1.A solução deve ser ofertada com uma solução para gerenciamento unificada para os equipamentos de rede LAN no mínimo com as seguintes características, sem prejuízo das especificações previstas no item 14(solução para controle de acesso) deste mesmo documento.

1.1.1.1.As especificações a seguir visam apresentar os requisitos necessários e funcionalidades para a solução de gerenciamento unificada de rede LAN e demais funções necessárias para atendimento deste projeto.

1.1.1.2.Visando mitigar os esforços dispendidos no desenvolvimento de integrações, é preferível que as licitantes proponentes optem por fornecer uma solução única;

1.1.1.3.Como forma de garantir a concorrência sem prejuízo da eficiência técnica exigida, será admitido, em caráter excepcional, a junção de diversas soluções para integração(e não apenas compatibilidade) entre si, desde que garantidas as funcionalidades de uma solução unificada.

1.1.1.4.Caso a solução ofertada seja feita por integração com de produtos de diversos parceiros tecnológicos, a oferta deve estar homologada com os fabricantes e assim permitindo o pleno gerenciamento de rede pela ferramenta de modo a garantir total integração entre as soluções e fabricantes;

1.1.1.5.Para atendimento deste item, será exigido sendo que as informações de compatibilidade entre as soluções devem estar publicadas no site oficial de ambos os fabricantes ou em ultimo caso, a emissão de uma carta de compatibilidade a ser providenciada junto aos fabricantes selecionados pela licitante.

1.1.1.5.1.Ainda sobre a carta de compatibilidade tratada no item anterior, ela deverá ser emitida em nome da comissão de licitação do respectivo processo de contratação, citando o número do processo e data, devidamente assinada pelo responsável técnico em nível nacional, citando o nome da licitante proponente, descrevendo o nome do produto ofertado, e expressando quais ações de integração serão realizadas com outras soluções, assumindo assim o compromisso de compatibilidade, tudo visando o correto funcionamento e garantindo que a proponente de fato esteja apta para atender todos os requisitos de compatibilidade e integração entre todos os produtos.

1.1.1.5.2.Pela sua natureza técnica, a carta de compatibilidade entre soluções deverá ser analisada pela equipe de contratações, que poderá pedir diligências, esclarecimentos ou mesmo recusar tecnicamente o documento, garantido ao licitante a oportunidade de defesa técnica do teor do documento sob análise.

1.1.1.2.Deve ser acessada através de provedores de nuvem pública ou on-premise, de forma virtualizada, na infraestrutura existe do TJAM. Caso a solução necessite, de acordo com as boas práticas do fabricante, mais que uma máquina virtual essa infraestrutura deve ser fornecida pela CONTRATADA.

1.1.1.3.As funcionalidades descritas devem ser providas no modelo SaaS (Software as a Service), como

serviço, ou seja, todos os recursos de hardware, software, suporte, manutenção e segurança, para funcionamento da solução devem ser providos pelo fornecedor.

1.1.1.4.Deve ser acessível através de navegador WEB padrão, com criptografia de tráfego SSL v1.3.

1.1.1.5.Todo acesso deve ser controlado com autenticação de usuário em base própria e externa utilizando para isso Single-Sign-on através do protocolo SAML.

1.1.1.6.Os privilégios de acesso devem ser controlados através de RBAC (Role Base Access Control) permitindo derivar privilégios por usuário baseado em Roles para determinar quais níveis de acesso será permitido.

1.1.1.7.Deve prover tutoriais interativos como guia para acesso as facilidades básicas, incluindo no mínimo, criação de usuários e roles, configuração e gestão de redes, monitoramento de equipamentos e redes, diagnósticos e interface de usuário.

1.1.1.8.Deve permitir a gestão, monitoramento e ferramentas de diagnóstico para access points e switches através de um único painel.

1.1.1.9.Deve permitir a gestão, monitoramento e ferramentas de diagnóstico através de um único painel.

1.1.1.10.Toda a comunicação entre a solução de gerenciamento e os dispositivos gerenciados deve ser feita através de conexão segura SSL v1.3, utilizando porta TCP 443.

1.1.1.11Os certificados digitais utilizados para estabelecimento desta comunicação segura devem estar armazenados em hardware específicos (raiz de confiança de nível de hardware - Root of Trust ou através de um módulo de plataforma confiável integrado - Trusted Platform Module - TPM) nos dispositivos a serem gerenciados.

1.1.1.12.As URLs de destino necessárias para estabelecimento da comunicação com os dispositivos a serem gerenciados devem ser disponibilizadas.

1.1.1.13.Deve encaminhar por e-mail o convite para o usuário concluir seu cadastro, incluindo a definição de senha, para acesso a plataforma, assim que seu e-mail for incluído como novo usuário.

1.1.1.14.Deve ser ofertado licenciamento (subscrição) de dispositivos a serem gerenciados pelos períodos de 3 (três) anos e com garantia de renovação desta garantia por pelo menos mais 02(dois) anos após o término da garantia inicial.

1.1.1.15.Deve permitir que as licenças sejam migradas entre equipamentos da mesma família, para o caso de substituição de equipamentos com defeito ou outros, sem depender de abertura de chamado técnico para isso.

1.1.1.16.Deve contemplar todas as atualizações disponibilizadas de maneira automática durante o período de vigência das licenças, sem depender de intervenção manual do operador.

1.1.1.17.Deve disponibilizar aplicativo gratuito através das lojas oficiais (App Store e Google Play), específico para a implantação de uma nova localidade, permitindo a ativação de switches e access points.

1.1.1.18.A utilização do aplicativo para ativação deve ser controlada, permitindo definir, o usuário, localidade, data e hora em que poderá ser realizada.

1.1.1.19.O aplicativo para ativação deve permitir o envio de foto para comprovar o término da implantação pelo usuário, além de permitir o envio de instruções básicas para o instalador através do painel de acompanhamento e gestão da implantação.

1.1.1.20.Após marcada como concluída, ou finalizado o período para implantação, o usuário do aplicativo não terá mais acesso a referida rotina para implantação.

1.1.1.21.Toda a configuração, bem como a versão de software em que os equipamentos devem utilizar, devem ser automaticamente enviadas após a conclusão da implantação através do aplicativo.

1.1.1.22.Deve permitir o acesso a CLI dos Switches gerenciados através de console remota utilizando o protocolo SSH.

1.1.1.23.Deve estar disponível em português, permitindo alternar para o Inglês conforme desejado pelo operador.

1.1.1.24.A solução deve ter disponibilidade de no mínimo de 99,95% do tempo.

1.1.1.25.Deve permitir a configuração baseada em grupos, permitindo que em um mesmo grupo possam ser definidas graficamente as configurações para switches e access points.

1.1.1.26. As configurações do grupo ao qual o equipamento está associado devem ser substituídas pelas configurações associadas ao equipamento específico (interfaces, VLAN, endereçamento IP, gateway, hostname).

1.1.1.27.Os grupos devem permitir dois modos de configuração dos equipamentos, interface gráfica e através de templates em arquivos de linha de comando.

1.1.1.28.Os arquivos templates em linha de comando devem permitir a criação de variáveis e condicionantes para definição de parâmetros da configuração.

1.1.1.29.Deve permitir a visualização das diferenças de configuração entre o arquivo template e a

configuração vigente no equipamento.
1.1.1.30.Deve permitir que os equipamentos sejam movimentados entre grupos diferentes, assumindo sempre a configuração do grupo de destino.
1.1.1.31.Deve permitir que as configurações sejam salvas através da criação de backups de configuração dos equipamentos gerenciados, permitindo o restore das mesmas através da interface gráfica de gerenciamento.
1.1.1.32.Deve permitir a criação e armazenamento de ao menos 20 versões de configurações de backup, permitindo ao administrador identificar as versões que não poderão ser substituídas por versões mais atualizadas.
1.1.1.33.Deve promover o ZTP (Zero Touch Provisioning) das configurações de equipamentos (switches e access points) sem necessidade de acesso local.
1.1.1.34.Deve ser capaz de fazer o aprovisionamento de switches a partir da sua configuração de fábrica, sem a necessidade de configuração local.
1.1.1.35.Deve permitir a configuração de política de conformidade de versão de software dos equipamentos por grupo de configuração.
1.1.1.36.Deve executar a atualização de software automática quando o equipamento for associado ao grupo de destino, obedecendo a versão definida na política de conformidade.
1.1.1.37.Deve permitir programar a atualização de software por localidade, definindo a data e horário para execução.
1.1.1.38.Deve possuir API (Application Programming Interface) aberta que permita o acesso e integração a solução de gerenciamento, não só para monitoramento, mas também para configuração dos equipamentos e seus grupos.
1.1.1.39.Deve possuir Streaming API, que permita o envio de informações a partir da solução de gerenciamento sem depender de requisições externas, entre elas:
1.1.1.39.1.Auditoria (conexão, configuração e firmware de equipamentos).
1.1.1.39.2.Localização (coordenadas de localização de clientes WI-FI).
1.1.1.39.3.Fluxo de sessões (sessões WEB dos clientes conectados através do WI-FI).
1.1.1.39.4.Monitoramento (status e estatísticas) de clientes.
1.1.1.39.5.Presença (detalhes de clientes conectados e não conectados à rede WI-FI).
1.1.1.39.6.Segurança (reportar alertas de WIDS).
1.1.1.40.Deve permitir o encaminhamento de alertas utilizando e-mail e WEBHOOK, considerando, no mínimo, os seguintes escopos de alertas para encaminhamento:
1.1.1.40.1.Alertas de Usuários.
1.1.1.40.2.Alertas de Pontos de Acesso WI-FI.
1.1.1.40.3.Alertas de Switches.
1.1.1.40.4.Alertas de conectividade com a solução de gerência.
1.1.1.40.5.Alertas de auditoria.
1.1.1.40.6.Alertas de localidade.
1.1.1.41.Deve identificar o dispositivo conectado à rede através da rede WI-FI, expondo os seguintes parâmetros:
1.1.1.41.1.Categoria.
1.1.1.41.2.Família.
1.1.1.41.3.Sistema Operacional.
1.1.1.41.4.Atributos de fluxo de tráfego por dispositivo:
1.1.1.41.4.1.Destinos acessados e host de destino.
1.1.1.41.4.2.Aplicações e grupos de aplicações.
1.1.1.42.Deve permitir a integração, através de API, com solução que permita validar a experiência dos usuários no acesso aos recursos de rede e aplicações internas, externas (SaaS) e customizadas, permitindo visibilidade do status verificado nos últimos 5 minutos através do dashboard por localidades.
1.1.1.43.Deve possuir capacidade para realizar análise de presença (Presence Analytics) com no mínimo as seguintes funcionalidades:
1.1.1.43.1.Obtenção de informações em tempo real e baseado em dados históricos, de quantos clientes potenciais passaram pela área de cobertura, quantos entraram, quantos se conectaram e qual o tempo médio de permanência na área de cobertura.
1.1.1.43.2.Realizar comparações de métricas por múltiplas localidades.
1.1.1.43.3.Permitir a customização de níveis de potência de sinal (RSSI) e limiares de tempo para medir o tráfego e realizar as categorizações.
1.1.1.43.4.Caso seja utilizado soluções de terceiros para análise de presença (Presence Analytics), estas

devem ser homologadas pelo fornecedor dos equipamentos de rede.
1.1.1.1.Deve possuir capacidade para realizar relatórios com no mínimo as seguintes funcionalidades:
1.1.1.1.1.Capacidade de geração de relatório para armazenagem de informações.
1.1.1.1.2.Coleta de informações da rede por períodos pré-definidos.
1.1.1.1.3.Capacidade de geração e envio automático de relatórios por e-mail.
1.1.1.1.4.Caso seja utilizado soluções de terceiros para a geração de relatórios, estas devem ser homologadas pelo fornecedor dos equipamentos de rede.
1.1.1.1.Deve possuir capacidade para gerenciamento de convidados com no mínimo as seguintes funcionalidades:
1.1.1.1.1.Deve possuir recurso de gerenciamento de convidados permite que os usuários convidados se conectem à rede e, ao mesmo tempo, permite que o administrador controle o acesso dos usuários convidados à rede.
1.1.1.1.2.Os administradores podem criar um perfil de página inicial para seus usuários convidados.
1.1.1.1.3.Deve permitir a personalização do layout da página inicial (vertical ou horizontal) com base no tipo de dispositivo.
1.1.1.1.4.Deve permitir que os convidados acessem a Internet fornecendo as credenciais configuradas pelos operadores convidados ou suas respectivas credenciais de login na rede social.
1.1.1.1.5.Deve possuir capacidade de criar uma conta com permissão apenas de poder criar contas de usuários da rede Wi-Fi sem que tenha acesso as configurações dos elementos de rede ou outros serviços.
1.1.1.1.6.Deve permitir a criação de contas de usuários da rede Wi-Fi com prazos de tempo.
1.1.1.1.7.Deve permitir que os visitantes ou usuários convidados podem se registrar usando a página inicial ao tentar acessar a rede. A senha é entregue aos usuários por meio de impresso ou e-mail dependendo das opções selecionadas durante o cadastro.
1.1.1.1.8.Deve fornecer as credenciais de login por meio de impressão ou e-mail.
1.1.1.2.Deve possuir capacidade de projeto automatizado de redes sem fio nos padrões 802.11a, 802.11b e 802.11g, 802.11n, 802.11ac e 802.11ax, segundo a geografia dos prédios.
1.1.1.3.Deve considerar a área de cobertura e a banda por usuário desejada.
1.1.1.4.Deve permitir a visualização de alertas da rede em tempo real.
1.1.1.5.Deve permitir a visualização de eventuais áreas sem cobertura de RF (áreas de sombra).
1.1.1.6.Deve monitorar o desempenho da rede wireless, consolidando informações de rede tais como: níveis de ruído, relação sinal ruído, interferência, potência de sinal.
1.1.1.7.Deve possuir capacidade de listagem on-line da localização de usuário, endereço IP, endereço MAC, nível de potência de recepção e dados de associação e de autenticação 802.1x.
1.1.1.8.Deve possuir informação visual e gráfica, planta baixa dos andares, para:
1.1.1.8.1.Visualização dos access points instalados, com estado de funcionamento.
1.1.1.8.2.Visualização do mapa de calor de RF (Heatmap).
1.1.1.8.3.Localização de ativos conectados à rede (equipamentos 802.11).
1.1.1.8.4.Localização de rogue APs.
1.1.1.9.Deve possuir capacidade de identificação e listagem dos rádios vizinhos e respectivos SSID/BSSID que podem ser percebidos por cada AP;
1.1.1.10.Deve possibilitar a gerência e identificação individualizada de cada AP remoto.
1.1.1.11.Deve permitir a administração centralizada dos APs sem a necessidade de configurar os APs individualmente.
1.1.1.12.Deve possibilitar a identificação de paredes e divisórias com respectivos níveis de atenuação por tipo (alvenaria, vidro, drywall e divisória).
1.1.1.13.Deve disponibilizar em painel gráfico de controle informações referentes à:
1.1.1.13.1.Sistemas operacionais e tipos de dispositivos que estão se conectando à rede.
1.1.1.13.2.Informações sobre chamadas de voz, seus protocolos e qualidade das mesmas.
1.1.1.13.3.Informações sobre os tipos de aplicações mais utilizados.
1.1.1.13.4.Informações sobre usuários conectados.
1.1.1.14.Deve possuir informação sobre possíveis ameaças à rede detectadas pelos sistemas gerenciados.
1.1.1.15.Deve possibilitar criação de regras de detecção de ameaças e correlacionar todos os dispositivos gerenciados.
1.1.1.16.Deve prover funcionalidades de aprendizagem de máquina para utilizar qualquer informação, massa de dados ou funcionalidade disponível na plataforma para desenvolver a inteligência operacional.
1.1.1.17.Deve possuir recursos de inteligência artificial para identificação de causa raiz e resolução de problemas.
1.1.1.18.Deve possuir capacidade de analisar grande volume de dados para identificar e resolver incidentes

e realizar melhoria operacional.
1.1.1.19.Deve possuir capacidade de realizar filtragem dos eventos possibilitando análises mais limpas, ricas e focadas.
1.1.1.20.Deve realizar o agrupamento automático de alertas relacionados entre si facilitando o gerenciamento, a tomada de decisão e operação.
1.1.1.21.Deve possuir recursos de inteligência artificial para identificação de causa raiz e resolução de problemas.
1.1.1.22.Deve possuir recursos para analisar as razões dos problemas, descrições, impacto para os usuários e recomendações.
1.1.1.23.Deve possuir mecanismo de linguagem natural, onde o operador possa pesquisar guias de solução, usuários e localidades.
1.1.1.24.Deve possuir capacidades de aprendizado de máquina para identificar solicitações e perguntas ao suporte para treinar modelos e criar futuros insights de inteligência.
1.1.1.25.Deve ter capacidade de atualizar automaticamente as configurações de redes para eliminar eventuais impactos de tráfegos de clientes externos que estão degradando o desempenho do Wi-Fi.
1.1.1.26.Quando o assistente de inteligência artificial identificar um problema afetando a rede, deve mostrar quantos e quais switches e clientes foram afetados, sendo possível checar mais detalhes individualmente.
1.1.1.27.Deve criar baselines permitindo assim que seja possível comparar a rede com grupos de pares semelhantes.
1.1.1.28.Deve ser possível detectar e sugerir passos de resolução das seguintes falhas:
1.1.1.28.1.Os switches que possuem alta utilização de CPU e memória alta.
1.1.1.28.2.Os switches que possuem um número incomum de erros de porta.
1.1.1.28.3.Os switches que possuem um número alto com problemas de Power-over-Ethernet.
1.1.1.28.4.Os switches que possuem flaps de porta excessivos.
1.1.1.28.5.Os access points que possuem utilização de CPU e memória alta.
1.1.1.28.6.Os access points com número de mudanças de canais excessivas.
1.1.1.28.7.Os clientes com impacto na performance.
1.1.1.28.8.Problemas de DNS, DHCP e cobertura.
1.1.1.28.9.Os clientes que fizeram roaming excessivamente e com alta latência.
1.1.1.28.10.Os clientes com alto número de falhas de associação WIFI.
1.1.1.28.11.Os clientes com falhas de autenticação.

1.2.REQUISITOS TÉCNICOS PARA OS EQUIPAMENTOS / SERVIÇOS
1.2.1.ITEM 01: SWITCH GERENCIADO DE DISTRIBUIÇÃO (PARA UNIDADES COM ALTO TRÁFEGO DE DADOS) -
1.2.1.1.Deve possuir no mínimo as seguintes características Gerais:
1.2.1.1.1.Deve possuir no mínimo 24 portas SFP/SFP+.
1.2.1.1.2.Deve possuir no mínimo 4 portas 40/100G QSFP+/QSFP28 ou performance superior.
1.2.1.1.3.Deve possuir 1 interface RJ-45 ou USB-C ou serial para acesso console local.
1.2.1.1.4.Deve possuir uma interface de gerenciamento out-of-band.
1.2.1.1.5.Deve possuir memória RAM de no mínimo 16GB.
1.2.1.1.6.Deve possuir buffer de pacotes de no mínimo 32MB.
1.2.1.1.7.Deve possuir uma memória não volátil (flash, SSD ou equivalente técnico), com pelo menos 32GB, para armazenamento persistente de configuração, arquivos, bancos de dados, scripts, entre outras aplicações.
1.2.1.1.8.Deve possuir capacidade de encaminhamento de no mínimo 950 Mpps.
1.2.1.1.9.Deve possuir capacidade de comutação de no mínimo 1.280 Gbps.
1.2.1.1.10.A arquitetura deve permitir “Cluster” de Switches (par de switches) em que 2 (dois) switches interligados operem em conjunto, possibilitando a gerencia através de um endereço único (por exemplo, um IP virtual ou sincronismo de configurações). Deve implementar a solução de MC-LAG (MultiChassis Link Aggregation Group) ou tecnologia semelhante que possibilite funcionalidade idêntica, em que mesmo havendo conexões entre diferentes equipamentos pertencentes ao mesmo par de switches, seja disponibilizado somente um único caminho lógico e agregado de comunicação, eliminando desta forma a necessidade do uso do protocolo STP (Spanning Tree Protocol). Não serão aceitas soluções em condição de empilhamento ou em cascateamento.
1.2.1.1.10.1.Caso opere em cluster, o par de switches deve operar em alta-disponibilidade e possibilitar o

upgrade de software sem que haja a parada do ambiente, com a mudança de tráfego entre os switches, caso necessário.
1.2.1.1.11.Deve acompanhar todos os componentes necessários para sua fixação no rack 19”.
1.2.1.1.12.Deve possuir fonte de alimentação interna redundante de 100/240VAC.
1.2.1.1.13.Deve suportar fans redundantes e hot- swappable.
1.2.1.1.14.Deve possuir Certificado de Homologação na Anatel, de acordo com a Resolução nº 242.
1.2.1.1.15.Visando atender à padronização que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas, de que trata o inciso V do artigo 40 da lei 14.133, de 01 de abril de 2021, este item deve ser do mesmo fabricante dos demais switches descritos neste termo de referência.
1.2.1.1.16.Deve possuir garantia do fabricante na modalidade lifetime, ou seja, até 5 (cinco) anos após a data de término da venda do equipamento ofertado.
1.2.1.1.17.Deve possuir garantia do fabricante de pelo menos 3 anos, (extensível a pelo menos mais dois anos, a critério da contratante) por declaração do fabricante (ou Part Number específico para este item) para substituição de peças de hardware na modalidade NBD (next business day). Não será aceita garantia de terceiro (distribuidor, importador ou instalador).
1.2.1.1.18.A fim de garantir que os produtos ou serviços a serem adquiridos atendam aos padrões de qualidade e confiabilidade essenciais para o sucesso do projeto, é obrigatório que o fabricante esteja incluído no relatório do Gartner de 2022 intitulado "Magic Quadrant for Wired and Wireless LAN Access Infrastructure". É importante ressaltar que essa referência ao relatório do Gartner não visa restringir a competição, mas sim assegurar a excelência técnica e a eficácia da solução.
1.2.1.1.19.É obrigatório incluir na proposta a marca e o modelo específico do(s) equipamento(s) e/ou software(s) e demais componente(s) e acessório (s) ofertado(s) para atendimento das especificações contidas nesse Termo de Referência, juntamente ao(s) catálogo(s) e/ou manual(ais) que comprovem as características requisitadas.
1.2.1.2.Deve possuir no mínimo as seguintes funcionalidades de Camada 2:
1.2.1.2.1.Deve implementar VLAN 802.1Q.
1.2.1.2.2.Deve implementar o padrão IEEE 802.1AK.
1.2.1.2.3.Deve implementar jumbo packets de pelo menos 9000 bytes.
1.2.1.2.4.Deve implementar LACP IEEE 802.3ad com até 50 grupos e até 8 portas por grupo.
1.2.1.2.5.Deve implementar port mirroring com no mínimo 4 grupos de espelhamento.
1.2.1.2.6.Deve implementar funcionalidade que permita a detecção de links unidirecionais.
1.2.1.2.7.Deve suportar no mínimo 1000 VLANS configuradas simultaneamente.
1.2.1.2.8.Deve implementar VLAN Translation.
1.2.1.2.9.Deve implementar LLDP (IEEE 802.1ab).
1.2.1.2.10.Deve implementar RPVST+ ou protocolo compatível.
1.2.1.2.11.Deve implementar RSTP (802.1w).
1.2.1.2.12.Deve implementar MSTP (IEEE 802.1s).
1.2.1.2.13.Deve implementar ERPS (Ethernet Ring Protection Switching).
1.2.1.2.14.Deve possuir capacidade mínima da tabela MAC de 82.000 entradas
1.2.1.3.Deve possuir no mínimo as seguintes funcionalidades de Camada 3:
1.2.1.3.1.Deve implementar roteamento estático.
1.2.1.3.2.Deve suportar tunelamento de tráfego IPv6 em redes IPv4.
1.2.1.3.3.Deve suportar dual Stack.
1.2.1.3.4.Deve implementar OSPF.
1.2.1.3.5.Deve implementar OSPFv3.
1.2.1.3.6.Deve implementar OSPF com suporte a autenticação MD5.
1.2.1.3.7.Deve implementar Graceful OSPF Restart conforme RFC 3623.
1.2.1.3.8.Deve implementar BGP-4.
1.2.1.3.9.Deve implementar VXLAN com BGP-EVPN
1.2.1.3.10.Deve implementar MP-BGP (Multi-Protocol BGP).
1.2.1.3.11.Deve implementar Policy-based Routing.
1.2.1.3.12.Deve implementar VRRP.
1.2.1.3.13.Deve implementar funcionalidade que permita a detecção de encaminhamento bidirecionais.
1.2.1.3.14.Deve implementar servidor DHCP para IPv4 e IPv6.
1.2.1.3.15.Deve implementar DHCP relay.
1.2.1.3.16.Deve suportar no mínimo 24.000 rotas IPV4 e 12.000 rotas IPv6.
1.2.1.4.Deve possuir no mínimo as seguintes funcionalidades para multicast:

1.2.1.4.1.Deve implementar MLD v1 e v2.
1.2.1.4.2.Deve implementar IGMP v2 e v3.
1.2.1.4.3.Deve implementar Multicast Service Delivery Protocol (MSDP).
1.2.1.4.4.Deve implementar Protocol Independent Multicast Source-Specific Multicast (PIM-SSM), Protocol Independent Multicast Dense Mode (PIM-DM) e Protocol Independent Multicast Sparse Mode (PIM-SM) para IPv4 e IPv6.
1.2.1.4.5.Deve implementar Protocol Independent Multicast (PIM) Multicast Boundary.
1.2.1.5.Deve possuir no mínimo as seguintes para Software Defined Networking:
1.2.1.5.1.Deve possuir interface REST API e scripting via Python.
1.2.1.5.2.Deve possuir solução embarcada, customizável e programável para monitoramento e análise de eventos que possa auxiliar na identificação e correção de problemas de redes, aplicações e eventos de segurança da informação com pelo menos as seguintes características:
1.2.1.5.2.1.Deve ser acessada via sistema operacional, por meio de máquina virtual, container ou sandbox disponível diretamente no equipamento.
1.2.1.5.2.2.Deve conter dados históricos correlacionados a alterações de configuração, fornecendo assim a capacidade de capturar, arquivar e acessar rapidamente o estado da rede em torno de um evento de rede.
1.2.1.5.2.3.Deve possuir capacidade de tomar uma ação dependendo do acontecimento ou limiar definido, como por exemplo, configurar um DHCP server, reiniciar um serviço ou abrir um ticket no suporte.
1.2.1.5.2.4.Deve possuir capacidade de visibilidade do tráfego de aplicativos. Como por exemplo, acompanhar o desempenho de aplicativos em nuvem, como Microsoft 365 ou Google Suite.
1.2.1.5.2.5.Deve possuir visibilidade de aplicativos como a integridade da fila de aplicações VOIP, bem como estatísticas de retransmissão de DHCP.
1.2.1.5.2.6.A solução deve ser executada em uma "sandbox", impedindo assim de usar uma quantidade excessiva de recursos da CPU.
1.2.1.5.2.7.Caso o equipamento não possua este recurso é possível entregar uma ferramenta on-premisses ou em cloud com todo licenciamento necessário pelo período mínimo da garantia a ser contratada, sem prejuízo do prazo inicial de 36 meses.
1.2.1.6.Deve possuir no mínimo as seguintes funcionalidades para QoS (Quality of Service) e ACL (Access Control List):
1.2.1.6.1.Deve implementar controle de storm de broadcast e multicast.
1.2.1.6.2.Deve implementar IEEE 802.1p.
1.2.1.6.3.Deve implementar Strict priority (SP) queuing e Deficit Weighted Round Robin (DWRR).
1.2.1.6.4.Deve implementar Data Center Bridging (DCB).
1.2.1.6.5.Deve implementar IP SLA.
1.2.1.6.6.Deve implementar ACL IPv4 e desejável para IPv6.
1.2.1.7.Deve possuir no mínimo as seguintes funcionalidades para segurança:
1.2.1.7.1.Deve suportar controle de acesso baseado em perfis (Role Based Access Control).
1.2.1.7.2.Deve implementar EST (Enrollment over Secure Transport).
1.2.1.7.3.Deve implementar autenticação 802.1x.
1.2.1.7.4.Deve implementar autenticação baseada em endereço MAC.
1.2.1.7.5.Deve implementar TACACS+. Não serão aceitas soluções similares.
1.2.1.7.6.Deve implementar RADIUS. Não serão aceitas soluções similares.
1.2.1.7.7.Deve implementar SSHv2.
1.2.1.7.8.Deve possuir tecnologia para inicialização segura (secure boot ou equivalente técnico) através de uma raiz de confiança de nível de hardware (Root of Trust) ou através de um módulo de plataforma confiável integrado (Trusted Platform Module - TPM).
1.2.1.7.9.Deve suportar integração com ferramenta de controle de autenticação do mesmo fabricante que permita identificar automaticamente o tipo e sistema operacional dos equipamentos que se conectam a rede (device profiling) sem a necessidade de agentes instalados nos dispositivos.
1.2.1.7.10.Deve suportar integração com ferramenta de controle de autenticação do mesmo fabricante que permita verificar se a máquina está em conformidade com a política de segurança antes de entrar na rede, verificando, no mínimo serviços os serviços e antivírus das máquinas. Deve suportar os sistemas operacionais Microsoft Windows, macOS e Linux
1.2.1.8.Deve possuir no mínimo as seguintes funcionalidades para gerenciamento:
1.2.1.8.1.Deve implementar NTP.
1.2.1.8.2.Deve suportar duas imagens de software na memória flash.
1.2.1.8.3.Deve suportar múltiplos arquivos de configuração na memória flash.
1.2.1.8.4.Deve implementar sFlow.

1.2.1.8.5.Deve implementar Syslog.
1.2.1.8.6.Deve implementar Secure SFTP (SFTP).
1.2.1.8.7.Deve suportar RMON.
1.2.1.8.8.Deve implementar SNMP v2/v3.
1.2.1.8.9.Deve possuir bluetooth ou suportar a instalação de dongle USB Bluetooth para permitir a integração com o aplicativo mobile (Android e iPhone) com o objetivo de auxiliar os técnicos de campo para validar se os equipamentos foram configurados de forma correta. Este aplicativo deve possuir as funcionalidades para configurar, visualizar e gerenciar as configurações do equipamento. Poderão ser utilizadas soluções de terceiros para atendimento deste item.
1.2.1.9.Deve possuir no mínimo as seguintes características para licenciamento:
1.2.1.9.1.Deve ser fornecido com a versão de software mais completa disponível para o equipamento.
1.2.1.9.2.Deve ser fornecido devidamente licenciado para solução de gerenciamento unificada.
1.2.1.9.3.Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento

1.2.2.ITEM 02: SWITCH GERENCIADO DE ACESSO 48 PORTAS (PARA UNIDADES COM ALTO TRÁFEGO DE DADOS) -
1.2.2.1.Deve possuir no mínimo as seguintes características Gerais:
1.2.2.1.1.Deve possuir no mínimo 48 portas 10/100/1000BaseT Gigabit Ethernet BaseT.
1.2.2.1.2.Deve possuir 4 portas adicionais com velocidade de 1/10G SFP+.
1.2.2.1.3.Deve possuir 1 interface RJ-45, USB-C ou serial para acesso console local.
1.2.2.1.4.Deve possuir uma interface de gerenciamento out-of-band.
1.2.2.1.5.Deve possuir memória RAM de no mínimo 8GB.
1.2.2.1.6.Deve possuir buffer de pacotes de no mínimo 8MB.
1.2.2.1.7.Deve possuir uma memória não volátil (flash, SSD ou equivalente técnico), com pelo menos 16GB, para armazenamento persistente de configuração, arquivos, bancos de dados, scripts, entre outras aplicações.
1.2.2.1.8.Deve possuir capacidade de encaminhamento de no mínimo 130 Mpps.
1.2.2.1.9.Deve possuir capacidade de comutação de no mínimo 176 Gbps.
1.2.2.1.10.Deve possui capacidade de empilhamento com até 8 elementos na pilha, sendo gerenciados através de um único IP.
1.2.2.1.11.Deve ser possível realizar empilhamento em até 10Kms, utilizando transceivers de longa distância.
1.2.2.1.12.Deve ser fornecido com um cabo de empilhamento.
1.2.2.1.13.O switch deve ser do tipo empilhável, com altura máxima de 1U e instalação em rack (19”). Deve acompanhar todos os componentes necessários para sua fixação no rack.
1.2.2.1.14.Deve ser fornecido com fonte de alimentação interna 100/240VAC.
1.2.2.1.15.Deve possuir Certificado de Homologação na Anatel, de acordo com a Resolução nº 242.
1.2.2.1.16.Visando atender à padronização que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas, de que trata o inciso V do artigo 40 da lei 14.133, de 01 de abril de 2021, este item deve ser do mesmo fabricante dos demais switches descritos neste termo de referência.
1.2.2.1.17.Deve possuir garantia do fabricante na modalidade lifetime, ou seja, até 5 (cinco) anos após a data de término da venda do equipamento ofertado.
1.2.2.1.18.Deve possuir garantia do fabricante de pelo menos 3 anos, (extensível a pelo menos mais dois anos, a critério da contratante) por declaração do fabricante (ou Part Number específico para este item) para substituição de peças de hardware na modalidade NBD (next business day). Não será aceita garantia de terceiro (distribuidor, importador ou instalador).
1.2.2.1.19.A fim de garantir que os produtos ou serviços a serem adquiridos atendam aos padrões de qualidade e confiabilidade essenciais para o sucesso do projeto, é obrigatório que o fabricante esteja incluído no relatório do Gartner de 2022 intitulado "Magic Quadrant for Wired and Wireless LAN Access Infrastructure". É importante ressaltar que essa referência ao relatório do Gartner não visa restringir a competição, mas sim assegurar a excelência técnica e a eficácia da solução.
1.2.2.1.20.É obrigatório incluir na proposta a marca e o modelo específico do(s) equipamento(s) e/ou software(s) e demais componente(s) e acessório (s) ofertado(s) para atendimento das especificações contidas nesse Termo de Referência, juntamente ao(s) catálogo(s) e/ou manual(ais) que comprovem as características requisitadas.

1.2.2.2.Deve possuir no mínimo as seguintes funcionalidades de Camada 2:
1.2.2.2.1.Deve implementar VLAN 802.1Q.
1.2.2.2.2.Deve implementar 802.1V.
1.2.2.2.3.Deve implementar jumbo packets de no mínimo 9000 bytes.
1.2.2.2.4.Deve implementar LACP IEEE 802.3ad com até 32 grupos e até 8 portas por grupo.
1.2.2.2.5.Deve implementar port mirroring com no mínimo 4 grupos de espelhamento.
1.2.2.2.6.Deve implementar funcionalidade que permita a detecção de links unidirecionais.
1.2.2.2.7.Deve suportar pelo menos 1.000 VLANS configuradas simultaneamente.
1.2.2.2.8.Deve implementar MVRP (Multiple VLAN Registration Protocol).
1.2.2.2.9.Deve implementar LLDP (IEEE 802.1ab).
1.2.2.2.10.Deve implementar LLDP-MED.
1.2.2.2.11.Deve implementar RPVST+ ou protocolo compatível.
1.2.2.2.12.Deve implementar RSTP (802.1w).
1.2.2.2.13.Deve implementar MSTP (IEEE 802.1s).
1.2.2.2.14.Deve implementar MVRP.
1.2.2.2.15.Deve implementar IGMP.
1.2.2.2.16.Deve implementar túneis VxLAN
1.2.2.2.17.Deve possuir capacidade mínima da tabela MAC de 32.000 entradas.
1.2.2.3.Deve possuir no mínimo as seguintes funcionalidades de Camada 3:
1.2.2.3.1.Deve implementar roteamento estático IPv4 e IPv6.
1.2.2.3.2.Deve implementar OSPFv3.
1.2.2.3.3.Deve implementar servidor DHCP.
1.2.2.3.4.Deve implementar DHCP snooping
1.2.2.3.5.Deve implementar DHCP Relay.
1.2.2.3.6.Deve suportar DNS Client.
1.2.2.3.7.Deve suportar dual stack.
1.2.2.4.Deve possuir no mínimo as seguintes funcionalidades para multicast:
1.2.2.4.1.Deve implementar MLD snooping.
1.2.2.4.2.Deve implementar IGMP v2 e v3.
1.2.2.4.3.Deve implementar Protocol Independent Multicast (PIM) com Sparse Mode (SM), Source Specific Multicast (SSM) e Dense Mode (DM) para IPv4 e IPv6.
1.2.2.5.Deve possuir no mínimo as seguintes para Software Defined Networking:
1.2.2.5.1.Deve possuir interface REST API e scripting via Python.
1.2.2.5.2.Deve possuir solução embarcada, customizável e programável para monitoramento e análise de eventos que possa auxiliar na identificação e correção de problemas de redes, aplicações e eventos de segurança da informação com pelo menos as seguintes características:
1.2.2.5.2.1.Deve ser acessada via sistema operacional, por meio de máquina virtual, container ou sandbox disponível diretamente no equipamento.
1.2.2.5.2.2.Deve conter dados históricos correlacionados a alterações de configuração, fornecendo assim a capacidade de capturar, arquivar e acessar rapidamente o estado da rede em torno de um evento de rede.
1.2.2.5.2.3.Deve possuir capacidade de tomar uma ação dependendo do acontecimento ou limiar definido, como por exemplo, configurar um DHCP server, reiniciar um serviço ou abrir um ticket no suporte.
1.2.2.5.2.4.Deve possuir capacidade de visibilidade do tráfego de aplicativos. Como por exemplo, acompanhar o desempenho de aplicativos em nuvem, como Office 365 ou Google Suite.
1.2.2.5.2.5.Deve possuir visibilidade de aplicativos como a integridade da fila de aplicações VOIP, bem como estatísticas de retransmissão de DHCP.
1.2.2.5.2.6.A solução deverá ser executada em uma "sandbox", impedindo assim de usar uma quantidade excessiva de recursos da CPU.
1.2.2.5.2.7.Caso o equipamento não possua este recurso é possível entregar uma ferramenta on-premisses ou em cloud com todo licenciamento necessário pelo período mínimo de 36 meses.
1.2.2.6.Deve possuir no mínimo as seguintes funcionalidades para QoS (Quality of Service) e ACL (Access Control List):
1.2.2.6.1.Deve implementar controle de broadcast e multicast.
1.2.2.6.2.Deve implementar rate limiting para pacotes ICMP.
1.2.2.6.3.Deve implementar Strict priority (SP) queuing e Deficit Weighted Round Robin (DWRR).
1.2.2.6.4.Deve implementar priorização de tráfego em tempo real.
1.2.2.6.5.Deve suportar IP SLA.
1.2.2.6.6.Deve implementar priorização de tráfego com no mínimo os seguintes parâmetros: endereço IP,

Tipo de Serviço, número da porta TCP/UDP, porta de origem e Diffserv.
1.2.2.6.7.Deve suporta pelo no mínimo oito filas de priorização de tráfego
1.2.2.6.8.Deve suportar ACL para IPv4 e IPv6
1.2.2.6.9.Deve implementar ACL com base no IP de origem e destino, porta TCP e UDP de origem e destino baseada em VLAN e por porta
1.2.2.7.Deve possuir no mínimo as seguintes funcionalidades para segurança:
1.2.2.7.1.Deve suportar controle de acesso baseado em perfis (Role Based Access Control).
1.2.2.7.2.Deve implementar 802.1x.
1.2.2.7.3.Deve implementar autenticação baseada em web.
1.2.2.7.4.Deve implementar autenticação baseada em endereço MAC.
1.2.2.7.5.Deve permitir a utilização simultânea de autenticação 802.1x, WEB e MAC em uma mesma porta, com suporte a até 32 sessões simultâneas.
1.2.2.7.6.Deve implementar TACACS+. Não serão aceitas soluções similares.
1.2.2.7.7.Deve implementar proteção contra-ataques na CPU do switch para prevenção de desligamento do appliance.
1.2.2.7.8.Deve implementar SSHv2.
1.2.2.7.9.Deve possuir tecnologia para inicialização segura (secure boot ou equivalente técnico) através de uma raiz de confiança de nível de hardware (Root of Trust) ou através de um módulo de plataforma confiável integrado (Trusted Platform Module - TPM).
1.2.2.7.10.Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita identificar automaticamente o tipo e sistema operacional dos equipamentos que se conectam a rede (device profiling) sem a necessidade de agentes instalados nos dispositivos.
1.2.2.7.11.Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita verificar se a máquina está em conformidade com a política de segurança antes de entrar na rede, verificando, no mínimo serviços os serviços e antivírus das máquinas. Deve suportar os sistemas operacionais Microsoft Windows, macOS e Linux.
1.2.2.8.Deve possuir no mínimo as seguintes funcionalidades para gerenciamento:
1.2.2.8.1.Deve implementar NTP.
1.2.2.8.2.Deve suportar duas imagens de software na memória flash.
1.2.2.8.3.Deve suportar múltiplos arquivos de configuração na memória flash.
1.2.2.8.4.Deve suportar a autoconfiguração dos switches através de DHCP e software de gerenciamento, sem necessidade de nenhuma intervenção no switch (com configuração de fábrica).
1.2.2.8.5.deve suportar detecção de falha e link entre switches.
1.2.2.8.6.Deve implementar sFlow.
1.2.2.8.7.Deve possuir interface web para configuração.
1.2.2.8.8.Deve implementar Syslog.
1.2.2.8.9.Deve implementar Secure SFTP (SFTP).
1.2.2.8.10.Deve implementar SNMP v1/v2/v3.
1.2.2.8.11.Deve implementar compatibilidade com o protocolo CDP e/ou LLDP para provisionamento de telefones IP.
1.2.2.8.12.Deve possuir funcionalidade Zero Touch Provisioning, ou seja, provisionar automaticamente o equipamento baixando e instalando automaticamente um arquivo de firmware, um arquivo de configuração ou ambos.
1.2.2.8.13.Deve possuir bluetooth ou suportar a instalação de dongle USB Bluetooth para permitir a integração com o aplicativo mobile (Android e iPhone) com o objetivo de auxiliar os técnicos de campo para validar se os equipamentos foram configurados de forma correta. Este aplicativo deve possuir as funcionalidades para configurar, visualizar e gerenciar as configurações do equipamento. Poderão ser utilizadas soluções de terceiros para atendimento deste item.
1.2.2.9.Deve possuir no mínimo as seguintes características para licenciamento:
1.2.2.9.1.Deve ser fornecido com a versão de software mais completa disponível para o equipamento;
1.2.2.9.2.Deve ser fornecido devidamente licenciado para solução de gerenciamento unificada.
1.2.2.9.3.Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento.

1.2.3. ITEM 03: SWITCH GERENCIADO DE ACESSO 24 PORTAS POE (PARA UNIDADES COM BAIXO TRÁFEGO DE DADOS)
1.2.3.1. Deve possuir no mínimo as seguintes características gerais:

1.2.3.1.1. Deve possuir no mínimo 24 portas 10/100/1000BaseT Gigabit Ethernet BaseT.
1.2.3.1.2. Deve possuir no mínimo 4 portas SFP.
1.2.3.1.3. Deve implementar PoE e PoE+ (Power over Ethernet) de acordo com o padrão IEEE 803.3af e IEEE 802.3at.
1.2.3.1.4. Deve possuir no mínimo 370 watts destinados as portas com PoE+ ativo.
1.2.3.1.5. Deve implementar Energy Efficient Ethernet IEEE 802.3az.
1.2.3.1.6. Deve possuir 1 interface RJ-45 ou USB-C ou serial para acesso console local.
1.2.3.1.7. Deve possuir 1 interface USB para conexão com dispositivos externos.
1.2.3.1.8. Deve possuir memória RAM de no mínimo 4GB.
1.2.3.1.9. Deve possuir buffer de pacotes de no mínimo 1MB.
1.2.3.1.10. Deve possuir uma memória não volátil (flash, SSD ou equivalente técnico), com pelo menos 16GB, para armazenamento persistente de configuração, arquivos, bancos de dados, scripts, entre outras aplicações.
1.2.3.1.11. Deve possuir capacidade de encaminhamento de no mínimo 40 Mpps.
1.2.3.1.12. Deve possuir capacidade de comutação de no mínimo 56 Gbps.
1.2.3.1.13. Deve possuir altura máxima de 1RU e instalação em rack (19”). Deve acompanhar todos os componentes necessários para sua fixação no rack.
1.2.3.1.14. Deve possuir fonte de alimentação interna 100/240VAC.
1.2.3.1.15. Deve possuir Certificado de Homologação na Anatel, de acordo com a Resolução nº 242.
1.2.3.1.16. Visando atender à padronização que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas, de que trata o inciso V do artigo 40 da lei 14.133, de 01 de abril de 2021, este item deve ser do mesmo fabricante dos demais switches descritos neste termo de referência.
1.2.3.1.17. Deve possuir garantia do fabricante na modalidade lifetime, ou seja, até 5 (cinco) anos após a data de término da venda do equipamento ofertado.
1.2.3.1.18. Deve possuir garantia do fabricante de pelo menos 3 anos comprovado por declaração do fabricante (ou Part Number específico para este item) para substituição de peças de hardware na modalidade NBD (next business day). Não será aceita garantia de terceiro (distribuidor, importador ou instalador).
1.2.3.1.19. A fim de garantir que os produtos ou serviços a serem adquiridos atendam aos padrões de qualidade e confiabilidade essenciais para o sucesso do projeto, é obrigatório que o fabricante esteja incluído no relatório do Gartner de 2022 intitulado "Magic Quadrant for Wired and Wireless LAN Access Infrastructure". É importante ressaltar que essa referência ao relatório do Gartner não visa restringir a competição, mas sim assegurar a excelência técnica e a eficácia da solução.
1.2.3.1.20. É obrigatório incluir na proposta a marca e o modelo específico do(s) equipamento(s) e/ou software(s) e demais componente(s) e acessório (s) ofertado(s) para atendimento das especificações contidas nesse Termo de Referência, juntamente ao(s) catálogo(s) e/ou manual(ais) que comprovem as características requisitadas
1.2.3.2. Deve possuir no mínimo as seguintes funcionalidades de Camada 2:
1.2.3.2.1. Deve implementar VLAN 802.1Q.
1.2.3.2.2. Deve implementar jumbo packets de pelo menos 9000 bytes.
1.2.3.2.3. Deve implementar LACP IEEE 802.3ad com até 8 grupos e até 8 portar por grupo.
1.2.3.2.4. Deve implementar port mirroring com no mínimo 4 grupos de espelhamento.
1.2.3.2.5. Deve implementar funcionalidade que permita a detecção de links unidirecionais.
1.2.3.2.6. Deve implementar 4000 VLAN IDs.
1.2.3.2.7. Deve suportar 512 VLANS configuradas simultaneamente.
1.2.3.2.8. Deve implementar MVRP (Multiple VLAN Registration Protocol).
1.2.3.2.9. Deve implementar LLDP (IEEE 802.1ab).
1.2.3.2.10. Deve implementar LLDP-MED.
1.2.3.2.11. Deve implementar RPVST+ ou protocolo compatível.
1.2.3.2.12. Deve implementar RSTP (802.1w).
1.2.3.2.13. Deve implementar MSTP (IEEE 802.1s).
1.2.3.2.14. Deve implementar tabela ARP com até 1000 entradas.
1.2.3.2.15. Deve possuir capacidade mínima da tabela MAC de 8.000 entradas
1.2.3.3. Deve possuir no mínimo as seguintes funcionalidades de Camada 3:
1.2.3.3.1. Deve implementar roteamento estático para IPv4 e IPv6.
1.2.3.3.2. Deve suportar dual Stack.
1.2.3.3.3. Deve implementar DHCP snooping.

1.2.3.3.4. Deve implementar DHCP Relay.
1.2.3.3.5. Deve suportar DNS Client.
1.2.3.3.6. Deve suportar DHCP Client para IPv4 e IPv6.
1.2.3.3.7. Deve possuir no mínimo as seguintes funcionalidades para multicast:
1.2.3.3.7.1. Deve implementar MLD snooping.
1.2.3.3.7.2. Deve implementar MLD v1 e v2.
1.2.3.3.7.3. Deve implementar IGMP v2 e v3.
1.2.3.3.8. Deve possuir no mínimo as seguintes para Software Defined Networking:
1.2.3.3.8.1. Deve possuir interface REST API.
1.2.3.3.9. Deve possuir no mínimo as seguintes funcionalidades para QoS (Quality of Service) e ACL (Access Control List):
1.2.3.3.9.1. Deve implementar controle de storm de broadcast e multicast.
1.2.3.3.9.2. Deve implementar rate limiting.
1.2.3.3.9.3. Deve implementar Strict priority (SP) queuing.
1.2.3.3.9.4. Deve implementar priorização de tráfego em tempo real.
1.2.3.3.9.5. Deve implementar priorização de tráfego com no mínimo os seguintes parâmetros: endereço IP, Tipo de Serviço, número da porta TCP/UDP, porta de origem e Diffserv.
1.2.3.3.9.6. Deve suporta pelo no mínimo oito filas de priorização de tráfego.
1.2.3.3.9.7. Deve suportar ACL para IPv4 e IPv6.
1.2.3.3.9.8. Deve implementar ACL com base no IP de origem e destino, porta TCP e UDP de origem e destino baseada em VLAN e por porta.
1.2.3.3.10. Deve possuir no mínimo as seguintes funcionalidades para segurança:
1.2.3.3.10.1. Deve suportar controle de acesso baseado em perfis (Role Based Access Control).
1.2.3.3.10.2. Deve implementar autenticação 802.1x.
1.2.3.3.10.3. Deve implementar autenticação baseada em web.
1.2.3.3.10.4. Deve implementar autenticação baseada em endereço MAC.
1.2.3.3.10.5. Deve permitir a utilização simultânea de autenticação 802.1x, WEB e MAC em uma mesma porta com suporte até 32 sessões simultâneas.
1.2.3.3.10.6. Deve implementar TACACS+. Não serão aceitas soluções similares.
1.2.3.3.10.7. Deve implementar RADIUS. Não serão aceitas soluções similares.
1.2.3.3.10.8. Deve implementa proteção contra-ataques na CPU do switch para prevenção de desligamento do appliance.
1.2.3.3.10.9. Deve implementar SSHv2.
1.2.3.3.10.10. Deve possuir tecnologia para inicialização segura (secure boot ou equivalente técnico) através de uma raiz de confiança de nível de hardware (Root of Trust) ou através de um módulo de plataforma confiável integrado (Trusted Platform Module - TPM).
1.2.3.3.10.11. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita identificar automaticamente o tipo e sistema operacional dos equipamentos que se conectam a rede (device profiling) sem a necessidade de agentes instalados nos dispositivos.
1.2.3.3.10.12. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita verificar se a máquina está em conformidade com a política de segurança antes de entrar na rede, verificando, no mínimo serviços os serviços e antivírus das máquinas. Deve suportar os sistemas operacionais Microsoft Windows, macOS e Linux.
1.2.3.3.11. Deve possuir no mínimo as seguintes funcionalidades para gerenciamento:
1.2.3.3.11.1. Deve implementar NTP.
1.2.3.3.11.2. Deve suportar duas imagens de software na memória flash.
1.2.3.3.11.3. Deve suportar múltiplos arquivos de configuração na memória flash.
1.2.3.3.11.4. Deve implementar sFlow.
1.2.3.3.11.5. Deve possuir interface web e via linha de comando para configuração.
1.2.3.3.11.6. Deve implementar Syslog.
1.2.3.3.11.7. Deve implementar Secure SFTP (SFTP).
1.2.3.3.11.8. Deve suportar RMON.
1.2.3.3.11.9. Deve suportar ping e traceroute para IPv4 e IPv6.
1.2.3.3.11.10. Deve implementar SNMP v2/v3.
1.2.3.3.11.11. Deve implementar compatibilidade com o protocolo CDP para provisionamento de telefones IP.
1.2.3.3.11.12. Deve possuir funcionalidade Zero Touch Provisioning, ou seja, provisionar automaticamente o equipamento baixando e instalando automaticamente um arquivo de firmware, um arquivo de

configuração ou ambos.
1.2.3.3.11.13. Poderão ser utilizadas soluções de terceiros para atendimento deste item.
1.2.3.3.12. Deve possuir no mínimo as seguintes características para licenciamento:
1.2.3.3.12.1. Deve ser fornecido com a versão de software mais completa disponível para o equipamento.
1.2.3.3.12.2. Deve ser fornecido devidamente licenciado para solução de gerenciamento unificada.
1.2.3.3.12.3. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento

1.2.4. ITEM 04: SWITCH GERENCIADO DE ACESSO 48 PORTAS POE (PARA UNIDADES COM BAIXO TRÁFEGO DE DADOS)
1.2.4.1. Deve possuir no mínimo as seguintes características gerais:
1.2.4.1.1. Deve possuir no mínimo 48 portas 10/100/1000BaseT Gigabit Ethernet BaseT.
1.2.4.1.2. Deve possuir no mínimo 4 portas SFP.
1.2.4.1.3. Deve implementar PoE e PoE+ (Power over Ethernet) de acordo com o padrão IEEE 803.3af e IEEE 802.3at.
1.2.4.1.4. Deve possuir no mínimo 370 watts destinados as portas com PoE+ ativo.
1.2.4.1.5. Deve implementar Energy Efficient Ethernet IEEE 802.3az.
1.2.4.1.6. Deve possuir 1 interface RJ-45 ou USB-C ou serial para acesso console local.
1.2.4.1.7. Deve possuir 1 interface USB para conexão com dispositivos externos.
1.2.4.1.8. Deve possuir memória RAM de no mínimo 4GB.
1.2.4.1.9. Deve possuir buffer de pacotes de no mínimo 1MB.
1.2.4.1.10. Deve possuir uma memória não volátil (flash, SSD ou equivalente técnico), com pelo menos 16GB, para armazenamento persistente de configuração, arquivos, bancos de dados, scripts, entre outras aplicações.
1.2.4.1.11. Deve possuir capacidade de encaminhamento de no mínimo 77 Mpps.
1.2.4.1.12. Deve possuir capacidade de comutação de no mínimo 104 Gbps.
1.2.4.1.13. Deve possuir altura máxima de 1RU e instalação em rack (19”). Deve acompanhar todos os componentes necessários para sua fixação no rack.
1.2.4.1.14. Deve possuir fonte de alimentação interna 100/240VAC.
1.2.4.1.15. Deve possuir Certificado de Homologação na Anatel, de acordo com a Resolução nº 242.
1.2.4.1.16. Visando atender à padronização que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas, de que trata o inciso V do artigo 40 da lei 14.133, de 01 de abril de 2021, este item deve ser do mesmo fabricante dos demais switches descritos neste termo de referência.
1.2.4.1.17. Deve possuir garantia do fabricante na modalidade lifetime, ou seja, até 5 (cinco) anos após a data de término da venda do equipamento ofertado.
1.2.4.1.18. Deve possuir garantia do fabricante de pelo menos 3 anos comprovado por declaração do fabricante (ou Part Number específico para este item) para substituição de peças de hardware na modalidade NBD (next business day). Não será aceita garantia de terceiro (distribuidor, importador ou instalador).
1.2.4.1.19. A fim de garantir que os produtos ou serviços a serem adquiridos atendam aos padrões de qualidade e confiabilidade essenciais para o sucesso do projeto, é obrigatório que o fabricante esteja incluído no relatório do Gartner de 2022 intitulado "Magic Quadrant for Wired and Wireless LAN Access Infrastructure". É importante ressaltar que essa referência ao relatório do Gartner não visa restringir a competição, mas sim assegurar a excelência técnica e a eficácia da solução.
1.2.4.1.20. É obrigatório incluir na proposta a marca e o modelo específico do(s) equipamento(s) e/ou software(s) e demais componente(s) e acessório (s) ofertado(s) para atendimento das especificações contidas nesse Termo de Referência, juntamente ao(s) catálogo(s) e/ou manual(ais) que comprovem as características requisitadas.
1.2.4.2. Deve possuir no mínimo as seguintes funcionalidades de Camada 2:
1.2.4.2.1. Deve implementar VLAN 802.1Q.
1.2.4.2.2. Deve implementar jumbo packets de pelo menos 9000 bytes.
1.2.4.2.3. Deve implementar LACP IEEE 802.3ad com até 8 grupos e até 8 portar por grupo.
1.2.4.2.4. Deve implementar port mirroring com no mínimo 4 grupos de espelhamento.
1.2.4.2.5. Deve implementar funcionalidade que permita a detecção de links unidirecionais.
1.2.4.2.6. Deve implementar 4000 VLAN IDs.
1.2.4.2.7. Deve suportar 512 VLANS configuradas simultaneamente.
1.2.4.2.8. Deve implementar MVRP (Multiple VLAN Registration Protocol).

1.2.4.2.9. Deve implementar LLDP (IEEE 802.1ab).
1.2.4.2.10. Deve implementar LLDP-MED.
1.2.4.2.11. Deve implementar RPVST+ ou protocolo compatível.
1.2.4.2.12. Deve implementar RSTP (802.1w).
1.2.4.2.13. Deve implementar MSTP (IEEE 802.1s).
1.2.4.2.14. Deve implementar tabela ARP com até 1000 entradas.
1.2.4.2.15. Deve possuir capacidade mínima da tabela MAC de 8.000 entradas
1.2.4.3. Deve possuir no mínimo as seguintes funcionalidades de Camada 3:
1.2.4.3.1. Deve implementar roteamento estático para IPv4 e IPv6.
1.2.4.3.2. Deve suportar dual Stack.
1.2.4.3.3. Deve implementar DHCP snooping.
1.2.4.3.4. Deve implementar DHCP Relay.
1.2.4.3.5. Deve suportar DNS Client.
1.2.4.3.6. Deve suportar DHCP Client para IPv4 e IPv6.
1.2.4.4. Deve possuir no mínimo as seguintes funcionalidades para multicast:
1.2.4.4.1. Deve implementar MLD snooping.
1.2.4.4.2. Deve implementar MLD v1 e v2.
1.2.4.4.3. Deve implementar IGMP v2 e v3.
1.2.4.5. Deve possuir no mínimo as seguintes para Software Defined Networking:
1.2.4.5.1. Deve possuir interface REST API.
1.2.4.6. Deve possuir no mínimo as seguintes funcionalidades para QoS (Quality of Service) e ACL (Access Control List):
1.2.4.6.1. Deve implementar controle de storm de broadcast e multicast.
1.2.4.6.2. Deve implementar rate limiting.
1.2.4.6.3. Deve implementar Strict priority (SP) queuing.
1.2.4.6.4. Deve implementar priorização de tráfego em tempo real.
1.2.4.6.5. Deve implementar priorização de tráfego com no mínimo os seguintes parâmetros: endereço IP, Tipo de Serviço, número da porta TCP/UDP, porta de origem e Diffserv.
1.2.4.6.6. Deve suporta pelo no mínimo oito filas de priorização de tráfego.
1.2.4.6.7. Deve suportar ACL para IPv4 e IPv6.
1.2.4.6.8. Deve implementar ACL com base no IP de origem e destino, porta TCP e UDP de origem e destino baseada em VLAN e por porta.
1.2.4.7. Deve possuir no mínimo as seguintes funcionalidades para segurança:
1.2.4.7.1. Deve suportar controle de acesso baseado em perfis (Role Based Access Control).
1.2.4.7.2. Deve implementar autenticação 802.1x.
1.2.4.7.3. Deve implementar autenticação baseada em web.
1.2.4.7.4. Deve implementar autenticação baseada em endereço MAC.
1.2.4.7.5. Deve permitir a utilização simultânea de autenticação 802.1x, WEB e MAC em uma mesma porta com suporte até 32 sessões simultâneas.
1.2.4.7.6. Deve implementar TACACS+. Não serão aceitas soluções similares.
1.2.4.7.7. Deve implementar RADIUS. Não serão aceitas soluções similares.
1.2.4.7.8. Deve implementa proteção contra-ataques na CPU do switch para prevenção de desligamento do appliance.
1.2.4.7.9. Deve implementar SSHv2.
1.2.4.7.10. Deve possuir tecnologia para inicialização segura (secure boot ou equivalente técnico) através de uma raiz de confiança de nível de hardware (Root of Trust) ou através de um módulo de plataforma confiável integrado (Trusted Platform Module - TPM).
1.2.4.7.11. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita identificar automaticamente o tipo e sistema operacional dos equipamentos que se conectam a rede (device profiling) sem a necessidade de agentes instalados nos dispositivos.
1.2.4.7.12. Deve suportar integração com ferramenta de controle de acesso do mesmo fabricante que permita verificar se a máquina está em conformidade com a política de segurança antes de entrar na rede, verificando, no mínimo serviços os serviços e antivírus das máquinas. Deve suportar os sistemas operacionais Microsoft Windows, macOS e Linux.
1.2.4.8. Deve possuir no mínimo as seguintes funcionalidades para gerenciamento:
1.2.4.8.1. Deve implementar NTP.
1.2.4.8.2. Deve suportar duas imagens de software na memória flash.
1.2.4.8.3. Deve suportar múltiplos arquivos de configuração na memória flash.

1.2.4.8.4. Deve implementar sFlow.
1.2.4.8.5. Deve possuir interface web e via linha de comando para configuração.
1.2.4.8.6. Deve implementar Syslog.
1.2.4.8.7. Deve implementar Secure SFTP (SFTP).
1.2.4.8.8. Deve suportar RMON.
1.2.4.8.9. Deve suportar ping e traceroute para IPv4 e IPv6.
1.2.4.8.10. Deve implementar SNMP v2/v3.
1.2.4.8.11. Deve implementar compatibilidade com o protocolo CDP para provisionamento de telefones IP.
1.2.4.8.12. Deve possuir funcionalidade Zero Touch Provisioning, ou seja, provisionar automaticamente o equipamento baixando e instalando automaticamente um arquivo de firmware, um arquivo de configuração ou ambos.
1.2.4.9. Deve possuir no mínimo as seguintes características para licenciamento:
1.2.4.9.1. Deve ser fornecido com a versão de software mais completa disponível para o equipamento.
1.2.4.9.2. Deve ser fornecido devidamente licenciado para solução de gerenciamento unificada.
1.2.4.9.3. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento.

1.2.5.ITEM 05: INTERFACE 10G ETHERNET CURTA DISTÂNCIA
1.2.5.1.Deve ser fornecido interface óptica compatível com SFP+ para conexão de fibras ópticas multimodo.
1.2.5.2.Deve ser compatível com o padrão 10GBASE-SR para fibras ópticas de pelo menos 300 metros.
1.2.5.3.Deve possuir conector LC duplex.
1.2.5.4.Velocidade de 10GbE.
1.2.5.5.Deve ser compatível com os switches que possuem portas SFP+ deste lote.

1.2.6.ITEM 06: INTERFACE 10G ETHERNET LONGA DISTÂNCIA
1.2.6.1.Deve ser fornecido interface óptica compatível com SFP+ para conexão de fibras ópticas monomodo.
1.2.6.2.Deve ser compatível com o padrão 10GBASE-LR para fibras ópticas de até 10.000 metros.
1.2.6.3.Deve possuir conector LC duplex.
1.2.6.4.Velocidade de 10GbE.
1.2.6.5.Deve ser compatível com os switches que possuem portas SFP+ deste lote.

1.2.7.ITEM 07: INTERFACE 40G ETHERNET
1.2.7.1.Deve ser fornecido interface óptica compatível com fibras ópticas multimodo de pelo menos 100 metros.
1.2.7.2.Deve possuir conector LC duplex.
1.2.7.3.Velocidade de 40GbE;
1.2.7.4.Deve ser compatível com os switches de distribuição

1.2.8.ITEM 08: INTERFACE 100G ETHERNET
1.2.8.1.Deve ser fornecido interface óptica compatível com fibras ópticas multimodo de até 100 metros.
1.2.8.2.Deve possuir conector LC duplex.
1.2.8.3.Velocidade de 100GbE;
1.2.8.4.Deve ser compatível com os switches de distribuição deste projeto, especialmente.

1.2.9.ITEM 9: SOLUÇÃO PARA CONTROLE DE ACESSO
1.2.9.1.As especificações a seguir visam apresentar os requisitos necessários e funcionalidades para a solução para controle de acesso de usuários e dispositivos e demais funções necessárias para atendimento do projeto e desta forma complementam as que estao previstas no inicio deste documento, especialmente as previstas no item 1.1. deste documento.
1.2.9.2.Deve ser fornecida uma máquina virtual para implementar a solução para autenticação de usuários e dispositivos.
1.2.9.3.Deve ser compatível com VMWare ESXi, Amazon EC2 e CentOS KVM.
1.2.9.4.O servidor para instalação da solução será de responsabilidade da CONTRATANTE, no qual a CONTRATADA deve informar as especificações mínimas recomendadas pelo fabricante, assim como sistemas operacionais e software complementares para a completa instalação do sistema.
1.2.9.5.Deve ser uma plataforma unificada que combina AAA, NAC, BYOD e acesso de convidado incorporando identidade, integridade, informações físicas / de dispositivo e elementos condicionais em um conjunto de políticas.
1.2.9.6.Deve implementar as seguintes fontes para autenticação:

1.2.9.6.1.Microsoft Active Directory;
1.2.9.6.2.Kerberos;
1.2.9.6.3.LDAP-compliant directory;
1.2.9.6.4.ODBC-compliant SQL server;
1.2.9.6.5.Token servers;
1.2.9.6.6.Base SQL interna;
1.2.9.6.7.RADIUS;
1.2.9.6.8.Microsoft Azure Active Directory;
1.2.9.6.9.Google G Suite;
1.2.9.6.10.HTTP;
1.2.9.6.11.Lista estática de endereços MAC.
1.2.9.7.Deve implementar Single Sign-on (SSO) através de SAML v2.0.
1.2.9.8.Deve implementar gerenciamento e aplicação de políticas de autorização de acesso de usuários com base em:
1.2.9.8.1. Atributos do usuário autenticado;
1.2.9.8.2.Hora do dia, dia da semana;
1.2.9.8.3.Tipo de dispositivo utilizado;
1.2.9.8.4.Localização do usuário;
1.2.9.8.5.Tipo de autenticação utilizado.
1.2.9.9.Deve permitir a visualização de todas informações relativas a cada transação/autenticação em uma única tela, como Data e Hora, MAC Address do dispositivo, classificação do dispositivo, Usuário, equipamento que requisitou a autenticação (origem), Método de autenticação utilizado, fonte de autenticação utilizada para validação, perfil de acesso aplicado, todos atributos de entrada do protocolo utilizados na requisição (ex. RADIUS), informações de resposta da solução para o elemento de rede, alertas em caso de falha, e exibição dos Log já filtrados para a requisição em análise.
1.2.9.10.Deve possuir Dashboard customizável, onde deve permitir a visualização de no mínimo as seguintes informações:
1.2.9.10.1.Lista com os últimos Alertas do sistema;
1.2.9.10.2.Gráfico com todas as requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ e Web Authetication;
1.2.9.10.3.Gráfico com o status das autenticações aceitas e rejeitadas nos últimos 7 dias;
1.2.9.10.4.Para soluções compostas por mais de um servidor, deve apresentar o Status de cada elemento dos sistemas, com informações como endereço IP e data da última replicação dos dados;
1.2.9.10.5.Gráfico com a categorização dos dispositivos classificados pela solução, divididos de acordo com as categorias de classificação;
1.2.9.10.6.Últimas falhas de autenticação;
1.2.9.10.7.Lista com as últimas autenticações;
1.2.9.10.8.Lista com as últimas autenticações com sucesso;
1.2.9.10.9.Utilização de CPU do sistema, no mínimo nos últimos 30 minutos.
1.2.9.11.Deve implementar funcionalidade de classificação automática de dispositivos (“Device profiling”), de forma a descobrir, classificar e agrupar os dispositivos conectados na rede.
1.2.9.12.Deve categorizar os dispositivos em pelo menos 3 níveis, por tipo de dispositivo (ex. Computador, SmartDevice, impressora, entre outros), por sistema operacional (ex. Windows, Linux, MacOS) e versão do sistema (ex. Windows, Windows Server).
1.2.9.13.Deve implementar a coleta de informações, para classificação, usando no mínimo DHCP, HTTP User-Agent, MAC OUI, ActiveSync plugin, SNMP, Subnet Scanner, IF-MAP, Cisco Device Sensor, MDM e TCP Fingerprinting.
1.2.9.14.Deve possuir base de regras e categorias de dispositivos pré-configurada.
1.2.9.15.Deve implementar mecanismo de atualização das regras e categorias pré-configuradas.
1.2.9.16.Deve implementar os serviços de autenticação, profiling e autorização para 4500 usuários ou dispositivos simultaneamente.
1.2.9.17.Caso exista licenciamento distinto para usuários ou dispositivos da rede sem fio (wireless) e usuários/dispositivos da rede cabeada (wired), deverão ser fornecidas as duas licenças para o número total de usuários solicitados.
1.2.9.18.Deve permitir que cada dispositivo receba uma chave pré-compartilhada exclusiva durante o registro do dispositivo.
1.2.9.19.Deve implementar RADIUS CoA, Web authentication e SAML v2.0.
1.2.9.20.Deve implementar no mínimo os seguintes métodos de autenticação:

1.2.9.20.1.-EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS);
1.2.9.20.2.-PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD);
1.2.9.20.3.-TTLS (EAP-MSCHAPv2, EAP-GTC, EAP- TLS, EAP-MD5, PAP, CHAP);
1.2.9.20.4.-EAP-TLS;
1.2.9.20.5.-PAP, CHAP, MSCHAPv1, MSCHAPv2, and EAP-MD5;
1.2.9.20.6.-Windows machine authentication;
1.2.9.20.7.-SMB v2/v3;
1.2.9.20.8.-WPA3 – MPSK;
1.2.9.20.9.-RADSec;
1.2.9.20.10.-Online Certificate Status Protocol (OCSP);
1.2.9.20.11.-TACACS+;
1.2.9.20.12.-WEB Authentication;
1.2.9.21.Deve implementar a verificação de vulnerabilidade através de varredura de portas (NMAP).
1.2.9.22.Deve implementar a aplicação de políticas em ambiente multivendor de Wireless, cabeado e VPN.
1.2.9.23.Deve implementar a integração nativa com soluções de MDM (Mobile Device Management), com no mínimo 5 (cinco) fabricantes distintos no mercado.
1.2.9.24.Deve implementar a integração nativa com soluções de segurança, com no mínimo 5 (cinco) fabricantes distintos no mercado, dentre eles Palo Alto implementado atualmente no TJPI.
1.2.9.25.Deve implementar a integração nativa com provedores de identidade (Identity Provider), com no mínimo 10 (dez) fabricantes distintos no mercado, dentre eles Google, Facebook, Instagram, LinkedIn e Twitter.
1.2.9.26.Deve permitir configurar um meio para proteger a comunicação entre clientes RADIUS / TCP na camada de transporte, utilizando TLS para encriptação da comunicação.
1.2.9.27.Deve suportar EDUROAM.
1.2.9.28.Deve possuir integração com plataforma de terceiros usando HTTP/RESTful API.
1.2.9.29.Deve permitir que a solução faça consultas em bases SQL, com o objetivo de buscar informação a serem utilizadas durante o processo de autenticação dos usuários.
1.2.9.30.Deve implementar seguintes recursos através de IPv6:
1.2.9.30.1.Administração via WEB e CLI;
1.2.9.30.2.Servidores de autenticação e autorização com endereçamento IPv6;
1.2.9.30.3.IPv6 Accounting Proxy;
1.2.9.30.4.Acesso a servidores com endereçamento IPv6 para contexto de endpoints;
1.2.9.30.5.Syslog, DNS, NTP;
1.2.9.30.6.Endereçamento IPv6 para VIP (Virtual IP) de alta disponibilidade;
1.2.9.30.7.Fontes de Syslog para processamento de eventos.
1.2.9.31.Deve permitir configuração em alta disponibilidade com no mínimo 2 (dois) elementos, sendo que ambos devem permanecer ativos para o processamento das requisições.
1.2.9.32.Deve permitir a configuração centralizada de políticas em ambientes distribuídos, no qual as políticas serão configuradas em um único elemento para serem distribuídas aos demais que pertençam a mesma zona/área.
1.2.9.33.Deve permitir a geração e o envio através de e-mail de alertas relativos as seguintes atividades anormais detectadas na rede:
1.2.9.34.Autenticações;
1.2.9.35.Acesso a dispositivos de rede;
1.2.9.36.Tentativa de execução de comandos em dispositivos de rede por usuários sem privilégios;
1.2.9.37.Atividades irregulares nos servidores da solução.
1.2.9.38.Deve possuir ferramenta para geração de relatórios de maneira centralizada, permitindo o agendamento e envio por e-mail em formato HTML e PDF.
1.2.9.39.Deve possuir ferramenta para geração de relatórios de maneira centralizada, permitindo o agendamento e envio por e-mail em formato HTML e PDF.
1.2.9.40.Deve possuir suporte técnico e atualizações de software pelo fabricante de pelo menos 3 (três) anos comprovado por declaração do fabricante ou fornecimento de PN do suporte técnico ofertado.

1.2.10.ITEM 10: INSTALAÇÃO DE SWITCH GERENCIADO
1.2.10.1.Os equipamentos deverão observar integralmente os requisitos de implantação, instalação e fornecimento descritos a seguir:
1.2.10.1.1.As atividades de instalação deverão ser realizadas dentro do horário comercial e nas dependências da Contratante.

1.2.10.1.2.Deve ser devidamente desembalado e todos os seus componentes devem ser montados conforme as instruções do fabricante.
1.2.10.1.3.Deve ser fixado de forma segura no rack padrão 19" fornecido pela contratante, seguindo as especificações e normas adequadas.
1.2.10.1.4.Deve ser corretamente conectado à rede à alimentação elétrica fornecida pela contratante.
1.2.10.1.5.Deve ser corretamente conectado à rede de dados (uplinks) utilizando cabos e conectores apropriados ofertados pela contratante.
1.2.10.1.6.Deve ser realizada a atualização para a versão de firmware mais recente disponibilizada pelo fabricante, a fim de garantir que o dispositivo esteja com as últimas melhorias de desempenho e segurança.
1.2.10.1.7.Deve ser realizada a configuração inicial do switch de acordo com as diretrizes e recomendações do fabricante, incluindo a atribuição de um endereço IP para gerenciamento, configuração de protocolos de gerenciamento (como SNMP e SSH) e definição de senhas de acesso.
1.2.10.1.8.Deve ser configurado para suportar a segmentação da rede por meio de VLANs, conforme o planejamento técnico fornecido pela contratante, garantindo uma organização lógica eficiente da infraestrutura de rede.
1.2.10.1.9.Devem ser configurados protocolos de redundância e resiliência (como STP, RSTP entre outros) visando garantir a disponibilidade contínua da rede e prevenção de loops de tráfego indesejados.
1.2.10.1.10.Caso seja necessário, deverão ser realizadas as configurações de recursos de segurança adequados ao ambiente, como listas de controle de acesso (ACLs) para filtragem de tráfego, autenticação de porta (802.1X) para controle de acesso baseado em identidade, entre outros recursos.
1.2.10.1.11.Caso seja necessário, deverão ser realizadas as configurações para protocolos de roteamento, como OSPF (Open Shortest Path First) ou BGP (Border Gateway Protocol), para garantir a conectividade e o roteamento eficiente entre as diferentes redes.
1.2.10.1.12.Deve ser configurado alertas e notificações no software de gerenciamento para receber notificações em tempo real sobre eventos críticos na rede, como falhas de link, quedas de dispositivos ou violações de segurança.
1.2.10.1.13.Deve ser personalizado os alertas de acordo com as necessidades da contratante.
1.2.10.1.14.Após as configurações dos switches deverão ser realizados testes de conectividade para verificar o correto funcionamento do equipamento, garantindo a comunicação adequada entre os dispositivos de rede e o tráfego de dados conforme as especificações exigidas.
1.2.10.1.15.Após as configurações do gerenciamento dos switches deverão ser realizados testes de monitoramento para verificar o correto funcionamento da solução, garantindo a comunicação adequada entre os dispositivos de rede, testes de funcionalidades de monitoramento e relatórios para validação das informações coletadas.
1.2.10.1.16.Ao final da implantação do projeto, deve ser fornecida à contratante toda a documentação detalhada referente às configurações aplicadas ao switch, incluindo endereços IP, configurações de VLAN, protocolos de gerenciamento, protocolos de redundância e resiliência, chaves de licenças, entre outros, para fins de registro e manutenção futura da rede.
1.2.10.1.17. As instalações a serem feitas no município sede da Contratante serão presenciais e as que forem em municípios do interior poderão ser feitas de forma remota.

1.2.11.ITEM 11: INSTALAÇÃO DA SOLUÇÃO PARA CONTROLE DE ACESSO
1.2.11.1.A solução deverá observar integralmente os requisitos de implantação, instalação e fornecimento descritos a seguir:
1.2.11.1.1.As atividades de instalação deverão ser realizadas dentro do horário comercial e nas dependências da Contratante, com repasse de conhecimento conhecido como hands on.
1.2.11.1.2.Deve ser realizada a instalação da versão de software mais recente disponibilizada pelo fabricante, a fim de garantir que esteja com as últimas melhorias de segurança, correções de bugs e recursos aprimorados.
1.2.11.1.3.A instalação deverá ser realizada em equipamento ofertado pela contratante, no qual a contratada deverá informar quais são as especificações de hardware, sistema operacional e recursos necessários.
1.2.11.1.4.Deve ser realizada a aplicação das licenças da solução para controle de acesso à rede, garantindo que estejam devidamente registradas, documentadas e atualizadas.
1.2.11.1.5.Antes da implementação a equipe técnica da contratada e equipe técnica da contratante deverão elaborar e definir as seguintes atividades:
1.2.11.1.5.1.Definir a solução de autenticação de rede mais adequada para atender as necessidades da contratante.

1.2.11.1.5.2.Definir a configuração do servidor de autenticação, no qual deve possuir as políticas de autenticação, criação contas de usuário e definir as opções de segurança apropriadas.
1.2.11.1.5.3.Definir a configuração dos equipamentos ofertados para direcionar os pedidos de autenticação ao servidor de autenticação.
1.2.11.1.5.4.Caso necessário definir a integração com os sistemas existentes como diretórios LDAP (Lightweight Directory Access Protocol) ou Active Directory, para simplificar a administração de usuários e garantir a sincronização adequada das informações de autenticação.
1.2.11.1.5.5.Definir as políticas de acesso baseadas em papéis ou grupos de usuários para determinar quais recursos de rede são acessíveis por diferentes usuários ou grupos.
1.2.11.1.5.6.Definir as configurações para restrições de acesso, como restrições de horário ou limites de largura de banda, caso seja necessário.
1.2.11.1.6.Após a etapa de planejamento a contratada deverá realizar as configurações e cronograma acordado.
1.2.11.1.7.Deve ser realizado testes abrangentes de autenticação para garantir que a solução esteja funcionando corretamente, verificando a autenticação de diferentes tipos de usuários, dispositivos diversos e usuários convidados, para garantir uma experiência de autenticação consistente e segura.
1.2.11.1.8.Deve ser realizado o monitoramento e registro de eventos da solução de controle de acesso à rede para acompanhar atividades de autenticação, detectar possíveis violações de segurança e facilitar a investigação de incidentes de segurança.
1.2.11.1.9.Ao final da implantação do projeto, deve ser fornecida à contratante toda a documentação detalhada referente às configurações aplicadas à solução, incluindo endereços IP, protocolos de gerenciamento, chaves de licenças de software entre outros, para fins de registro e manutenção futura da rede.

1.2.12.ITEM 12: BANCO DE HORAS PARA SERVIÇOS AVANÇADOS
1.2.12.1.1.Compreende o fornecimento de 1 (uma) hora de serviços técnicos especializados na área de Tecnologia da Informação, para atividades de suporte técnico remoto, diagnóstico, implementação de serviços, site survey passivo, repasse de conhecimento e/ou execução de procedimentos periódicos (atualizações) da infraestrutura de rede LAN/WLAN contratada.
1.2.12.1.2.Os serviços deverão ser prestados por profissional devidamente certificado pelo fabricante da solução.

1.2.13.ITEM 13: TREINAMENTO OFICIAL DO FABRICANTE
1.2.13.1.1.Compreende o fornecimento de 1 (uma) turma com até 6 participantes para o treinamento oficial do fabricante para a plataforma de gerenciamento unificada e deverá ser ministrado por instrutor certificado.
1.2.13.1.2.O treinamento deve possuir pelo menos 16h de treinamento a serem cumpridas em 02 ou mais dias de aula.
1.2.13.1.3.O treinamento poderá de forma presencial nas dependências do TJPI quando disponíveis e no interesse da Administração ou nas dependências do fornecedor ou em centro de treinamento/instrução disponibilizado em território nacional. O tratamento deverá ser voltado à certificação, em nível básico ou acima deste, na solução adquirida.
1.2.13.1.4.Deve possuir apresentações e laboratórios práticos, de modo com que a equipe técnica do TJPI possa ter um melhor aproveitamento dos benefícios da solução para o gerenciamento abrangente de alertas, a conectividade de dispositivos, a integridade da rede e a atividade dos usuários.
1.2.13.1.5. Será admitido o treinamento mediante fornecimento de voucher para treinamento oficial para a quantidade mínima de participantes prevista, desde que atendidos os demais requisitos e prestado em centro de formação ou congênere, em território nacional, com fornecimento de datas previstas com antecedência mínima de 01 mês de modo a permitir o planejamento da contratante. Neste caso, apenas as despesas de deslocamento e de diárias dos treinandos correrão por conta da Contratante.
1.2.13.1.6. Todas as despesas relativas à organização do treinamento, espaço físico, diárias do instrutor, material didático incluindo laboratórios e coffe break correrão às expensas da Contratada.

ANEXO II - LOCAIS DE EXECUÇÃO DOS SERVIÇOS

Unidades da Capital	**Endereço**

Tribunal Arnoldo Péres	Av. André Araújo, s/nº - Aleixo. CEP 69.060-000.
Centro Adm. José de Jesus	Av. André Araújo, s/nº - Aleixo. CEP 69.060-000.
Fórum Henoch Reis	Rua Paraíba, s/n – Adrianópolis – Aleixo CEP: 69.061-970
Fórum Mário Verçosa	Rua Comendador Alexandre Amorim, 285 – Aparecida – CEP: 69010-300
Fórum Lúcio Fonte	Av. Noel Nutels s/nº Cidade Nova I – CEP: 69.093-771.
Fórum Azarias Menescal	Av. Autaz Mirim, s/n – Jorge Teixeira – CEP 69085-000
Juizado Infracional	Rua Des. João Machado, s/n - Alvorada I, Manaus - AM – 69.043-360
Fórum Euza de Vasconcelos	R. Valério Botelho de Andrade, 32 -188 - São Francisco, Manaus - AM, 69079-260
Juizado Especial Nilton Lins	Rua Marquês de Monte Alegre, 1400, Pq das Laranjeiras, Manaus - AM, 69.058-040
Arquivo Geral	Av. Constantino Nery, 2575 - Flores, Manaus - AM, 69058-795
Casa da Justiça e Cidadania - Shopping São José	Alam. Cosme Ferreira, 8047, 2º piso, Shopping São José, Manaus - AM, 69.083–000
Casa da Justiça e Cidadania - Shopping Pq. 10 Mall	Av. Tancredo Neves, 654, 1º piso, Parque 10, Manaus - AM, 69054-700
Central de Transportes	Av. André Araújo, s/nº - Aleixo. CEP 69.060-000.

ANEXO III - INFRAÇÕES, GRAUS, MULTAS E PENALIDADES

Tabela 1 - Infrações, Graus e Multas

Item	**Infração**	**Grau da Infração**	**Tipo de Multa**
1	Descumprimento de quaisquer outras obrigações contratuais, não explicitadas nos demais itens, que sejam consideradas leves	1	Moratória
2	Não entreqa de documentação simples solicitada pelo CONTRATANTE	1	Moratória
3	Atraso parcialmente justificado na entrega até 30 dias.	1	Moratória
4	Atraso parcialmente justificado na entrega acima de 30 dias até 60 dias.	2	Moratória
5	Atraso parcialmente justificado ou injustificado na entrega acima de 60 dias.	2	Compensatória

6	Descumprimento de outros prazos, previstos do TR	2	Moratória
7	Erros de execução do objeto	2	Moratória
8	Desatendimento às solicitações do CONTRATANTE	3	Moratória
9	Descumprimento de quaisquer outras obrigações contratuais, não explicitadas nos demais anteriores, que seriam consideradas médias	3	Moratória
10	Execução imperfeita do objeto	3	Moratória
11	Não manutenção das condições de habilitação e de licitar e contratar com a Administração Pública durante a vigência contratual	4	Compensatória
12	Não entrega de documentação importante solicitada pelo CONTRATANTE	4	Compensatória
13	Descumprimento de quaisquer outras obrigações contratuais, não explicitadas nos demais itens, que seriam consideradas graves	4	Compensatória
14	Inexecução parcial do Contrato	4	Compensatória
15	Descumprimento da legislação (legais e infralegais) afeta à execução do objeto (direta ou indireta)	5	Compensatória
16	Cometimento de atos protelatórios durante a execução visando adiamento dos prazos contratados	5	Compensatória
17	Inexecução total do Contrato	5	Compensatória

Tabela 2 - Penalidades

Grau	**Advertência - 1ª Ocorrência**	**Mora Moratória Valor Mensal**	**Multa Compensatória**
1	Sim	Não	Não
2	Não	1% a 4,9% por ocorrência ou contrato	1,5% a 4,9% por ocorrência ou contrato
3	Não	5% a 8,9% por ocorrência ou contrato	8,0% a 14,9% por ocorrência ou contrato
4	Não	9% a 11,9% por ocorrência ou contrato	15,0% a 24,9% por ocorrência ou contrato
5	Não	12% a 15% por ocorrência ou contrato	25% a 30% por ocorrência ou contrato

Documento assinado eletronicamente por **Karla Rozeana Bau Zarth**, **Servidor**, em 03/12/2024, às 11:35, conforme art. 1º, III, "b", da Lei 11.419/2006.