ESTUDO TÉCNICO PRELIMINAR

INTRODUÇÃO

O presente documento visa analisar a viabilidade da presente contratação, bem como levantar os elementos essenciais que servirão para compor o Termo de Referência, de forma a melhor atender às necessidades da Administração.

Porém, cabe ressaltado que o presente ETP, como o próprio título sugere (preliminar) não se constitui em documento acabado, devendo a Administração da FEMA complementar e ou atualizar as informações, de forma a atender as normas legais vigentes.

1. DADOS DO PROCESSO

Memorando 6.072/2024

Setor Requisitante: Centro de Pesquisa em Informática – CEPEIN – FEMA

Objeto: CONTRATAÇÃO DE EMPRESA ESPECIALIZADA NA PRESTAÇÃO DE SERVIÇOS GERENCIADOS DE TECNOLOGIA DA INFORMAÇÃO PARA REALIZAÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO, SERVIÇO DE PROTEÇÃO PARA ESTAÇÕES DE TRABALHO E SERVIÇO DE SUPORTE TÉCNICO E MONITORAMENTO DE REDES E WI-FI.

EQUIPE DE PLANEJAMENTO PARA ESTA CONTRATAÇÃO

Servidor	Cargo
Nivaldo Aparecido de Melo	Coordenador Administrativo
Luiz Ricardo Begosso	Coordenador do CEPEIN
Eduardo Aparecido de Souza	Chefe de Seção
Juliana Santos De Nigris Batista	Chefe de Seção
Isadora Pelizone de Lima Cintra	Assistente Administrativo

2. OBJETIVO

2.1. O objetivo de uma contratação de segurança da informação é proteger os ativos de informação de uma organização contra ameaças e vulnerabilidades. Isso inclui

garantir a confidencialidade, integridade e disponibilidade dos dados, bem como assegurar que a empresa esteja em conformidade com regulamentações e normas de segurança.

3. NORMATIVOS QUE DISCIPLINAM OS SERVIÇOS A SEREM CONTRATADOS OU MATERIAIS A SEREM ADQUIRIDOS

3.1. A contratação objeto deste estudo terá como base a Lei 14.133/2021.

3.2. Para a contratação de empresa para prestação de serviços de tecnologia da informação, incluindo serviços de proteção para estações de trabalho, suporte técnico e monitoramento de redes Wu-Fi, a modalidade de licitação mais adequada, conforme a Lei nº 14.133/21, é o Pregão Eletrônico, por menor preço.

3.3. Esta escolha é fundamentada pelo o Art. 28 da Lei 14.133/2021 que estabelece o pregão deve ser utilizado sempre que possível, dada a sua eficiência em termos de custo e tempo e Art. 11 da Lei, que estabelece que a licitação é o procedimento administrativo destinado a selecionar a proposta mais vantajosa para a administração, sendo o menor preço uma das modalidades previstas para a escolha da proposta.

3.4. A escolha do Pregão Eletrônico também está alinhada com os princípios de transparência, competitividade e economicidade do processo licitatório, essenciais para a administração pública e destacados no Art. 5º da Lei 14.133/2021. Este procedimento assegura que a Fundação Educacional do Município de Assis possa adquirir serviços tecnicamente adequados e economicamente vantajosos, respeitando a legislação vigente e garantindo a melhor aplicação dos recursos públicos.

3.5. Portanto, a utilização do Pregão Eletrônico para a contratação dos serviços descritos é a mais indicada, proporcionando um processo licitatório justo, competitivo e transparente, em conformidade com a Lei nº 14.133/2021.

4. JUSTIFICATIVAS DA NECESSIDADE DA CONTRATAÇÃO

4.1. A contratação de uma empresa especializada na prestação de serviços

gerenciados de tecnologia da informação, especificamente para serviços de segurança da informação, proteção para estações de trabalho, e suporte técnico e monitoramento de redes e Wi-Fi, é essencial para a Fundação Educacional do Município de Assis (FEMA). Esta necessidade surge do crescente volume de dados operacionalizados, da diversidade do parque tecnológico e da alta dependência do negócio em relação à disponibilidade e qualidade dos serviços de TIC. A segurança robusta é crucial para proteger as atividades da FEMA contra ameaças cibernéticas, garantindo a integridade e a confidencialidade dos dados manipulados.

4.2. A contratação de profissionais qualificados e com experiência na área de proteção de dados permitirá uma segurança maior devido ao aumento de ameaças cibernéticas, o que poderia resultar em perdas financeiras significativas.

4.3. A segurança da informação não é uma tarefa única. A contratação de serviços externos garante que a segurança seja continuamente avaliada e aprimorada, respondendo rapidamente a novas ameaças.

4.4. Diante do exposto, a contratação de uma empresa especializada em serviços de segurança da informação não é apenas uma necessidade, mas um compromisso da FEMA com os dados de todos os alunos da instituição.

5. REFERÊNCIA A OUTROS INSTRUMENTOS DE PLANEJAMENTO DO ÓRGÃO

5.1. A contratação de empresa especializada na prestação de serviços gerenciados de tecnologia da informação para realização de serviços gerenciados de segurança da informação, serviço de proteção para estações de trabalho e serviço de suporte técnico e monitoramento de redes e Wi-Fi pela Fundação Educacional do Município de Assis está alinhada com o planejamento estratégico da instituição. A necessidade de contratação é justificada pela crescente demanda por segurança em sistemas de TIC, proteção contra ameaças cibernéticas e a importância de manter a disponibilidade e qualidade dos serviços tecnológicos. A contratação está prevista para ser realizada em regime de 24 horas por dia, durante 12 meses, podendo ser

prorrogada conforme a Lei 14.133/2021.

6. REQUISITOS DA CONTRATAÇÃO

6.1. Natureza da Contratação:

6.1.1. A natureza da necessidade de contratação dos serviços especializados de Tecnologia da Informação, incluindo serviços gerenciados de segurança da informação, proteção para estações de trabalho, e suporte técnico e monitoramento de redes e Wi-Fi, é de natureza comum, pois se trata de um serviço que não exige especialização técnica exclusiva, sendo acessível a diversas empresas qualificadas no mercado. O objetivo dessa contratação reflete a necessidade garantir a segurança e eficiência das operações de TI da Fundação Educacional do Município de Assis, protegendo as atividades contra ameaças cibernéticas, conforme justificado no Documento de Formalização de Demanda e neste Estudo Técnico Preliminar, que são parte do planejamento desta contratação

6.2. Os requisitos necessários à contratação, conforme a Lei nº 14.133/21, incluem:

6.2.1. Modalidade de Licitação e critério de julgamento por Menor Preço:

a. Lei 14.133/2021, Art. 28, I - estabelece que o pregão deve ser utilizado sempre que possível, dada a sua eficiência em termos de custo e tempo;

a.1. Justificativa: A escolha da modalidade visa promover a transparência, competitividade e economicidade do processo licitatório

b. Lei nº 14.133/21, Art. 11: A licitação é o procedimento administrativo destinado a selecionar a proposta mais vantajosa para a administração, sendo o menor preço um dos critérios previstos para a escolha da proposta mais vantajosa para a Administração;

b1. Justificativa: A escolha por menor preço é adequada devido à natureza do serviço, onde o custo é um fator determinante e a economicidade e eficiência são necessárias**.**

6.2.2. Compatibilidade do Valor Estimado com o Mercado:

a. Lei nº 14.133/21, Art. 23: O valor estimado para a contratação deve ser compatível

com os valores de mercado;

a1. Justificativa: Essencial para garantir que a Fundação não pague por serviços acima do valor de mercado, mantendo a contratação dentro de parâmetros econômicos razoáveis.

6.2.3. Habilitação dos Licitantes:

a. Lei nº 14.133/21, Art. 62: A habilitação é a fase da licitação em que se verifica a capacidade do licitante de realizar o objeto da licitação, dividindo-se em habilitação jurídica, técnica, fiscal, social e trabalhista, e econômico-financeira.

a1. Justificativa: Garantir que a empresa escolhida possua a capacidade jurídica, técnica e econômico-financeira necessária para fornecer o serviço de seguro de vida em grupo de forma eficaz e conforme as normas legais e regulatórias.

6.2.4. Apresentação de Propostas e Lances:

a. Lei nº 14.133/21, Art. 55: A apresentação de propostas e lances deve ser realizada de forma a garantir a seleção da proposta mais vantajosa.

a.1. Justificativa: A modalidade de menor preço facilita a comparação direta entre as propostas, simplificando o processo de seleção e garantindo transparência e justiça no processo licitatório.

6.3. Esses requisitos são fundamentais para assegurar que a contratação dos serviços de tecnologia FEMA/IMESA, com foco na proteção sejam realizados de maneira eficiente, transparente e ao menor custo possível, alinhada com os princípios de economicidade e eficiência que regem as contratações públicas conforme estabelecido pela Lei nº 14.133/21.

6.4. Duração Inicial do Contrato:

6.4.1. A duração inicial do contrato para a prestação de serviços deve ser estabelecida conforme a Lei 14.133/21, que permite contratos de até cinco anos para serviços contínuos, com possibilidade de prorrogação. O contrato será executado na Fundação Educacional do Município de Assis, localizada na Av. Getúlio Vargas, 1200 – Vila Nova Santana – Assis – SP. O pagamento será realizado mensalmente, em até 15 dias úteis após a apresentação da nota fiscal pela contratada, através do sistema bancário.

6.5. Critérios de Sustentabilidade:

6.5.1. Para a contratação dos serviços especializados de Tecnologia de Informação da FEMA/IMESA, com foco na proteção da rede interna, é essencial incorporar critérios de sustentabilidade, especialmente considerando a dimensão ambiental. Estes critérios incluem a descrição de possíveis impactos ambientais e medidas mitigadoras, requisitos de baixo consumo de energia e de outros recursos, além de logística reversa para desfazimento e reciclagem de bens e refugos, quando aplicável. Seguem os critérios de sustentabilidade e medidas mitigadoras:

6.5.2. Energia e Recursos: Exigir que a empresa prestadora dos serviços implemente práticas de baixo consumo de energia em seus escritórios e operações, equipamentos com alta eficiência energética e incentivo ao trabalho remoto para reduzir o consumo de energia e emissões relacionadas ao transporte dos funcionários. As medidas mitigadoras incluem a redução da pegada de carbono e menor impacto ambiental das operações diárias.

6.5.3. Logística Reversa e Reciclagem: Estabelecer políticas de logística reversa para o descarte e reciclagem de materiais eletrônicos e de escritório usados pela empresa de seguros. Isso inclui a reciclagem de equipamentos eletrônicos e a disposição adequada de materiais não recicláveis. A medida mitigadora é a minimização do impacto ambiental dos resíduos gerados.

6.5.4. Educação e Conscientização: Promover programas de educação e conscientização sobre sustentabilidade para os funcionários da empresa prestadora de serviços. Isso pode incluir treinamentos sobre práticas sustentáveis no local de trabalho e em casa.

6.5.5. Esses critérios e medidas não apenas contribuem para a proteção ambiental, mas também alinham a contratação do serviço pretendido com as disposições da Lei 14.133/21, que incentiva a adoção de práticas sustentáveis nas contratações públicas. A implementação dessas práticas pode ser monitorada e avaliada regularmente para garantir sua eficácia e ajustar as políticas conforme necessário.

6.6. Transição Contratual:

6.6.1. O objeto do contrato é a contratação de empresa especializada na prestação de serviços gerenciados de tecnologia da informação, incluindo serviços gerenciados de segurança da informação, serviço de proteção para estações de trabalho e serviço de suporte técnico e monitoramento de redes e Wi-Fi. A necessidade de contratação surge da importância de proteger as atividades da FEMA contra ameaças cibernéticas, garantindo segurança, alta disponibilidade, eficiência, escalabilidade e desempenho na operacionalização de dados. Os prazos para a transição devem ser estabelecidos em acordo com a contratada, assegurando que todas as obrigações legais e contratuais sejam cumpridas antes da finalização do contrato atual e início do novo. Os possíveis riscos da transição incluem atrasos na transferência de conhecimento, falhas na configuração dos sistemas de segurança, e interrupções no serviço durante a mudança de fornecedor, o que pode afetar a operação da FEMA

6.7. Relevância dos requisitos estipulados:

6.7.1. Os requisitos especiais para a contratação dos serviços de Tecnologia da Informação para a Fundação Educacional do Município de Assis não são restritivos, pois se enquadram na natureza de serviços comuns dentro do campo da Tecnologia da Informação, cujos padrões de desempenho e qualidade são objetivamente definidos e usuais no mercado. A relevância da contratação destes serviços especializados é alta, considerando que são essenciais para garantir a segurança e eficiência das operações de TI da Fundação, protegendo as atividades contra ameaças cibernéticas. Esta necessidade justifica a escolha do pregão como modalidade de licitação, conforme o Art. 29 da Lei 14.133/21, que é apropriada para a aquisição de bens e serviços comuns.

6.7.2. A relevância da contratação está em proporcionar um ambiente seguro para trabalho e ensino de alunos e funcionários. Este objetivo alinha-se com os princípios de eficiência e efetividade, garantindo que os recursos públicos sejam utilizados de maneira a maximizar o bem-estar dos estagiários.

6.7.3. A transparência e imparcialidade são asseguradas pela Lei nº 14.133/21, Art. 55, que exige a apresentação de propostas e lances de forma clara e justa, permitindo

uma seleção objetiva baseada no menor preço. A legalidade é observada ao seguir todos os requisitos legais e regulatórios para a habilitação dos licitantes, conforme Art. 62 da mesma lei, garantindo que apenas empresas capacitadas participem do processo.

6.7.4. A publicidade é garantida pela divulgação do processo licitatório, permitindo o conhecimento e a participação de várias empresas, promovendo a competitividade. A moralidade e o interesse público são atendidos ao buscar um serviço que proteja os estagiários, uma ação alinhada com os deveres da Fundação para com seus beneficiários.

6.7.5. A celeridade e economicidade são observadas ao escolher a modalidade de Menor Preço, simplificando o processo de seleção e garantindo que não se pague mais do que o valor de mercado pelo seguro, conforme Art. 23 da Lei nº 14.133/21. A sustentabilidade, embora menos diretamente relacionada, pode ser considerada na escolha de empresas que ofereçam condições de seguro responsáveis e sustentáveis.

6.7.6. A competitividade é fomentada pela ausência de requisitos especiais restritivos, permitindo a participação de um número maior de licitantes. A motivação para a contratação é claramente justificada pela necessidade de atenção na saúde mental dos alunos, propiciando um ambiente saudável para o aprendizado, e a segurança jurídica é mantida ao cumprir rigorosamente as disposições da Lei nº 14.133/21.

6.7.7. Portanto, a contratação está alinhada com os princípios administrativos e legais, garantindo um processo justo, competitivo e benéfico para a comunidade envolvida.

7. LEVANTAMENTO DE MERCADO

7.1. Após análise detalhada do Documento de Formalização de Demanda e considerando as necessidades da Fundação Educacional do Município de Assis (FEMA) para a contratação de serviços de empresa especializada na prestação de serviços gerenciados de tecnologia da informação, incluindo serviços gerenciados de segurança da informação, serviço de proteção para estações de trabalho e serviço de

suporte técnico e monitoramento de redes e Wi-Fi, foi realizado um levantamento de mercado para identificar as melhores soluções disponíveis que atendam às especificações técnicas e operacionais requeridas.

7.2. Para realizar o levantamento de mercado, foram consideradas as seguintes fontes: a) Orçamentos recebidos de potenciais fornecedores;

7.3. A estimativa de valores foi baseada na média dos preços obtidos por meio de orçamento recebido de potenciais fornecedores.

7.4. Os valores foram considerados compatíveis com o mercado, garantindo conformidade legal e eficiência na aquisição, afastando qualquer possibilidade de superfaturamento ou de preço inexequível.

8. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

8.1. A descrição da solução como um todo abrange a prestação dos serviços de empresa especializada na prestação de serviços gerenciados de tecnologia da informação, incluindo serviços gerenciados de segurança da informação, serviço de proteção para estações de trabalho e serviço de suporte técnico e monitoramento de redes e Wi-Fi.

8.2. A prestação do serviço se dará 7 (sete) dias por semana, 24 (vinte e quatro) horas por dia.

8.3. Esta necessidade é justificada pelo aumento do volume de dados, diversidade tecnológica e alta dependência dos serviços de TIC, essenciais para a integridade e confidencialidade dos dados da FEMA. A não contratação desses serviços pode expor a instituição a riscos significativos de ataques cibernéticos e perda de dados, comprometendo sua operacionalidade e reputação.

8.4. A solução proposta deve incluir manutenção contínua e assistência técnica para garantir a eficácia dos serviços ao longo do tempo, com exigências claras de desempenho e qualidade definidas no edital, conforme os padrões usuais de mercado.

8.5. De acordo com a legislação vigente, há a possibilidade de prorrogação contratual por tratar-se de serviço de natureza contínua, onde é necessário a manutenção do

presente contrato para que não ocorra interrupção dos serviços.

9. ESTIMATIVA DAS QUANTIDADES A SEREM CONTRATADAS

9.1. O tempo de contratação é de 12 meses podendo ser renovado por sucessivos períodos nos termos da lei.

9.2. A prestação de serviços especializados na prestação de serviços gerenciados de tecnologia da informação, incluindo serviços gerenciados de segurança da informação, serviço de proteção para estações de trabalho e serviço de suporte técnico e monitoramento de redes e Wi-Fi deve ser prestado sete dias por semana, vinte e quatro horas por dia.

9.3. Não deve haver limites para aberturas de chamados, sejam dúvidas, configurações ou resoluções de problemas.

10. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

10.1. Foi estimado uma despesa mensal de R$ 26.100,00 (vinte e seis mil e cem reais) e total anual de R$ 313.200,00 (trezentos e treze mil e duzentos reais), para contratação completa do objeto, valor esse não será sigiloso e constará no edital da licitação.

10.2. Vislumbra-se que os valores obtidos são compatíveis com o praticado no mercado correspondente, tendo em vista que, a estimativa de custo foi realizada considerando a média dos preços obtidos por meio de orçamentos recebidos de potenciais fornecedores do objeto pretendido, garantindo assim conformidade legal e eficiência na aquisição, afastando qualquer possibilidade de superfaturamento ou de preço inexequível, conforme planilha de estimativa de custos acostado ao processo.

10.3. Justificativa da Pesquisa de Mercado e da Escolha do Fornecedor:

10.3.1. A contratação de serviços especializados na tecnologia da informação, demanda a seleção de fornecedores especializados no mercado. Esta medida visa garantir que o serviço oferecido atenda de forma precisa às necessidades específicas da instituição, resguardando os direitos e a segurança e sigilo de dados, conforme previsto na legislação vigente, incluindo a Lei 14.133/2021.

10.3.2. Dado que o objeto da contratação envolve um serviço especializado e com peculiaridades, tais como proteção de dados internos, é essencial realizar a pesquisa de preços com empresas que possuam expertise consolidada na oferta desse tipo de serviço. A escolha dessas empresas especializadas proporciona os seguintes benefícios:

10.3.2.1. Adequação técnica: Empresas do ramo possuem amplo conhecimento das exigências legais e contratuais para os atendimentos, garantindo que o aluno seja atendido em sua especificidade e singularidade.

10.3.2.2. Competitividade e atualização de mercado: O levantamento de preços junto a fornecedores do ramo assegura que os valores estimados estejam alinhados às práticas e padrões atualizados do mercado, evitando distorções orçamentárias e maximizando o uso eficiente dos recursos públicos.

11. CONDIÇÕES DE PAGAMENTO

11.1. Os pagamentos serão efetuados em parcelas mensais, com prazo de até 15 (quinze) dias úteis após o recebimento da Nota Fiscal devidamente preenchida.

12. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

12.1. Esta prestação de serviço se caracteriza como um serviço contínuo, com vigência normalmente anual.

12.2. A natureza integrada e interdependente desses serviços sugere que a contratação por lote único é mais apropriada, pois permite uma gestão unificada e eficiente, minimizando interfaces de coordenação entre diferentes fornecedores e garantindo uma abordagem holística à segurança e ao suporte técnico.

12.3. A decisão de contratar por lote único é apoiada pelo inciso VIII do § 1° do art. 18 da Lei 14.133/21, que permite a contratação integrada quando a divisão do objeto em lotes puder comprometer a segurança e a eficácia da contratação pretendida. Além disso, o art. 7° da mesma lei estabelece que a licitação deve ser processada e julgada

com observância dos princípios de legalidade, impessoalidade, moralidade, igualdade, publicidade, probidade administrativa, vinculação ao instrumento convocatório, julgamento objetivo e dos que lhes são correlatos, assegurando a escolha da proposta mais vantajosa para a administração.

13. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

13.1. Não há contratações correlatas ou interdependentes, deste serviço, nesta fundação.

14. RESULTADOS ESPERADOS

14.1. A contratação de serviços gerenciados de tecnologia da informação, especificamente para segurança da informação, proteção de estações de trabalho, e suporte técnico e monitoramento de redes e Wi-Fi, visa alcançar resultados significativos em termos de economicidade e eficiência operacional para a Fundação Educacional do Município de Assis (FEMA). A necessidade de tais serviços é impulsionada pelo crescente volume de dados e pela complexidade do parque tecnológico da instituição, que requerem soluções avançadas para garantir a segurança contra ameaças cibernéticas e a continuidade das operações acadêmicas e administrativas.

14.2. Os resultados esperados com essa contratação incluem a melhoria na proteção dos dados e sistemas da FEMA, garantindo alta disponibilidade e desempenho dos sistemas de TI, o que é crucial para a operacionalização eficiente da instituição. Além disso, espera-se que a implementação de soluções de segurança de última geração e o suporte técnico contínuo contribuam para a prevenção de interrupções causadas por ataques cibernéticos, minimizando riscos e potenciais prejuízos.

14.3. Em termos de desenvolvimento nacional sustentável, a contratação alinha-se com as diretrizes de promover tecnologias que suportem a segurança e a eficiência das operações, contribuindo para a formação de um ambiente acadêmico mais seguro e propício ao desenvolvimento de pesquisas e à formação de profissionais

qualificados na área de tecnologia da informação.

14.4. Para a medição dos resultados e desempenho do contrato, os indicadores podem incluir a redução no número de incidentes de segurança, a melhoria no tempo de resposta a incidentes, a eficácia das soluções de proteção implementadas, e a satisfação dos usuários com a infraestrutura de TI. Estes indicadores ajudarão a garantir que o contrato esteja cumprindo seus objetivos e agregando valor à instituição conforme previsto na Lei 14.133/2021.

15. PRAZO DE VIGÊNCIA CONTRATUAL

15.1. O prazo de vigência contratual será de 12 (doze) meses, contados a partir da assinatura do contrato, podendo ser prorrogado na forma e condições estabelecidas na Lei nº 14.133/2024.

15.1.1. Caso o contrato venha a ser prorrogado os valores poderão ser corrigidos pelo Índice Nacional de Preços ao Consumidor Amplo – IPCA.

16. POSSÍVEIS IMPACTOS AMBIENTAIS

16.1. Entende-se que a contratação pretendida não traz possíveis impactos ambientais.

17. CONTROLE E FISCALIZAÇÃO

17.1. A fiscalização do contrato seguirá os padrões estabelecidos no artigo 117 da Lei nº 14.133/2021, garantindo o cumprimento de todas as especificações técnicas e normas regulatórias aplicáveis.

18. ANÁLISE DE RISCO

18.1. Não foram identificados riscos substanciais fora os comuns a toda contratação semelhante, tais como: a inexecução total ou parcial do ajuste pactuado; o não cumprimento de obrigações, especificações e prazos; bem como a ocorrência de caso fortuito ou de força maior.

18.2. Entende - se que as ações, de iniciativa da Administração, necessárias para

reduzir a ocorrência dos riscos identificados, já estão previstas nos normativos aos quais à contratação do presente serviço deverá estar devidamente fundamentada, representadas pelas sanções administrativas a serem definidas, observando- se os aspectos e características do seu objeto.

19. VIABILIDADE OU NÃO DA CONTRATAÇÃO

19.1. O estudo preliminar traz evidência com base na solução proposta e nos benefícios produzidos pela contratação ora descrita, ou seja, a contratação de uma empresa especializada em Tecnologia da Informação, incluindo serviços gerenciados de segurança da informação, proteção para estações de trabalho, e suporte técnico e monitoramento de redes e Wi-Fi, mostra-se tecnicamente possível e fundamentadamente necessária, tendo em vista também a alta relevância destes serviços para a FEMA.

Diante do exposto, declara-se ser viável a contratação pretendida.

Assis, 30 de outubro de 2024

Luiz Ricardo Begosso
Coordenador do CEPEIN

Eduardo Aparecido de Souza
Chefe de Seção

Nivaldo Aparecido de Melo
Coordenador Administrativo

Juliana Santos De Nigris Batista
Chefe de Seção

Isadora Pelizone de Lima Cintra
Assistente Administrativo

TERMO DE REFERÊNCIA

OBJETO: Contratação de empresa especializada na prestação de serviços gerenciados de tecnologia da informação como serviços gerenciados de segurança da informação, serviço de proteção para estações de trabalho e serviço de suporte técnico e monitoramento de redes e Wi-Fi devidamente descritos e caracterizados nas especificações técnicas presente abaixo:

LOTE - SERVIÇOS GERENCIADOS DE TECNOLOGIA DA INFORMAÇÃO		
ITEM	**DESCRIÇÃO**	**QTDE**
1	SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO	12 meses
2	SERVIÇO DE PROTEÇÃO PARA ESTAÇÕES DE TRABALHO	12 meses
3	SERVIÇO DE SUPORTE TÉCNICO E MONITORAMENTO DE REDES E WI-FI	12 meses
4	SERVIÇO DE INSTALAÇÃO	1

- Os equipamentos utilizados pela contratada para prestação dos serviços deverão ser novos, ainda em linha de produção em pleno funcionamento, e cobertos por garantia pelo respectivo fabricante durante toda a vigência do contrato.
- Deverão ser apresentados juntamente com a proposta comercial CATÁLOGOS, ENCARTES, FOLHETOS TÉCNICOS E MANUAIS dos equipamentos, softwares e serviços ofertados, onde constem as especificações técnicas e a caracterização deles, permitindo a consistente avaliação dos itens.
- O prazo para implantação e ativação dos serviços do presente certame é de até 30 (trinta) dias corridos.
- Deverá ser prestado o serviço de forma interrupta, 24 horas por dia, sem intervalos, durante 12 meses podendo ser prorrogado por iguais períodos nos termos da lei.

ITEM 1 - SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO:

1.1. Next-Generation Firewall (NGFW) para proteção de informação perimetral e de rede interna que inclui stateful firewall com capacidade para operar em alta disponibilidade (HA) em modo ativo-ativo para controle de tráfego de dados por identificação de usuários e por camada 7, com controle de aplicação, administração de largura de banda (QoS), VPN IPsec e SSL, IPS, prevenção contra ameaças de vírus, *malwares* e Filtro de URL.

1.2. Deverá ser fornecida console de gerenciamento dos equipamentos e centralização de logs em nuvem ou hardware do mesmo fabricante.

1.3. A console de gerenciamento em nuvem, deve estar no hospedada no Brasil;
1.4. A console de gerenciamento deve ser possível atribuir configurações de concentradores de SD-WAN;
1.5. A console de gerenciamento deve dispor de configurações globais para replicação nos firewalls;
1.6. Deverão ser fornecidas as licenças que ativem a modalidade do firewall como ativo-ativo para atualização de todos os componentes de software sem custo adicional, pelo período mínimo de 12 (doze) meses.
1.7. Para os itens que representem bens materiais, a CONTRATADA deverá fornecer produtos novos, sem uso anterior.
1.8. Por cada appliance físico que compõe a plataforma de segurança, entende-se o hardware, software e as licenças necessárias para o seu funcionamento.
1.9. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico.
1.10. Deve possuir processadores próprios e para fins específicos, desenvolvidos exclusivamente pelo fabricante da solução, com a finalidade de processar tráfegos de redes e acelerar o processamento destes pacotes de redes, permitindo o uso de diversas funcionalidades de segurança ao mesmo tempo sem diminuir a performance do equipamento.
1.11. Todos os equipamentos de rede deverão possuir certificado de homologação expedido pela Agência Nacional de Telecomunicações (ANATEL).
1.12. Por alta disponibilidade (HA) entende-se que a solução deverá ser composta ao menos por dois *appliances*, licenciados para funcionamento em redundância no formato ativo-ativo.
1.13. A solução deverá contemplar a totalidade das capacidades exigidas, sendo permitido o uso de mais de um equipamento (sempre em modo de alta disponibilidade HA) para complementar a solução, caso o fabricante não possua todas as funções em um único equipamento.
1.14. Caso a solução ofertada ofereça link dedicado para gerenciamento de HA, deverá suportar interfaces LAG e VLAN para o link HA dedicado e interfaces VLAN para links monitorados;
1.15. Cada *appliance* deverá ser capaz de executar a totalidade das capacidades exigidas para cada função, não sendo aceitos somatórias para atingir os limites mínimos.
1.16. O hardware e o software fornecidos não podem constar, no momento da apresentação da proposta, em listas de *end-of-sale, end-of-support, end-of-engineering-support* ou *end-of-life* do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante.
1.17. CARACTERÍSTICAS DE DESEMPENHO E HARDWARE
1.18. Performance mínima de 39 Gbps de *throughput* para firewall.
1.19. Performance mínima de 7 Gbps de *throughput* de IPS.
1.20. Performance mínima de 6.3 Gbps de *throughput* para controle de NGFW.
1.21. Performance mínima de 20.5 Gbps de *throughput* de IPsec VPN.
1.22. Suporte a, no mínimo, 6.500,000 de conexões simultâneas.
1.23. Suporte a, no mínimo, 148.000 novas conexões por segundo.
1.24. Possuir o número irrestrito quanto ao máximo de usuários licenciados.

1.25. Não será aceito soluções que tenham limite de VPN via software.
1.26. Possuir armazenamento interno de no mínimo 1 disco de 120 GB SATA-III SSD para sistema operacional, quarentena local, logs e relatórios.
1.27. Possuir no mínimo 8 GB (2400mhz) DDR4 de memória RAM ECC (Error Correction Code) para o processador principal
1.28. Possuir processador de Fluxo do tipo NPU para aceleração de pacotes;
1.29. Possuir no mínimo 4 GB de memória RAM ECC (Error Correction Code) dedicada ao processador de rede NPU;
1.30. Possuir no mínimo 8 (oito) interfaces de rede GbE;
1.31. Possuir no mínimo 2 (duas) interfaces SFP;
1.32. Possuir no mínimo 1 slots para adição de módulos de interfaces de rede;
1.33. Deve ser compatível com módulos do mesmo fabricante com as seguintes opções:
1.34. 8 port GbE copper;
1.35. 8 port GbE SFP fiber;
1.36. 4 port 10 GbE SFP+ fiber;
1.37. 4 port GbE copper bypass (2 pairs);
1.38. 4 port GbE copper PoE +;
1.39. 4 port GbE Copper;
1.40. 4 port 2.5 GbE copper PoE;
1.41. port GbE Fiber (LC) bypass;
1.42. + 4 port GbE SFP Fiber.
1.43. Possuir 1 (uma) interface do tipo console ou similar.
1.44. Interruptor Elétrico.
1.45. CARACTERÍSTICAS DO SERVIÇO ESPECIALIZADO DE SEGURANÇA DE PERIMETRO.
1.46. A solução deve consistir de *appliance* de proteção de rede com funcionalidades de *Next Generation Firewall* (NGFW), e console de gerência, monitoração e logs.
1.47. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões.
1.48. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos *appliances* desde que obedeçam a todos os requisitos desta especificação.
1.49. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.
1.50. O software deverá ser fornecido em sua versão mais atualizada.
1.51. O HA (modo de alta disponibilidade) deve suportar o uso de dois equipamentos em modo ativo-passivo ou modo ativo-ativo e deve possibilitar monitoração de falha de link.
1.52. Uma interface completa de comando de linha (*CLI command-line-interface*) deverá ser acessível através da interface gráfica e via porta serial.
1.53. A atualização de software deverá enviar avisos de atualização automáticos.
1.54. O sistema de objetos deverá permitir a definição de redes, serviços, *hosts* períodos de tempos, usuários e grupos, clientes e servidores.
1.55. As notificações deverão ser realizadas via e-mail e SNMP.
1.56. Suportar SNMPv3 e Netflow.
1.57. O firewall deverá ser *stateful*, com inspeção profunda de pacotes.

1.58. As zonas deverão ser divididas pelo menos em WAN, LAN e DMZ, sendo necessário que as zonas LAN e DMZ possam ser customizáveis.

1.59. As políticas de NAT deverão ser customizáveis para cada regra.

1.60. A proteção contra *flood* deverá ter proteção contra DoS (*Denial of Service*), DdoS (*Distributed DoS*).

1.61. Proteção contra *anti-spoofing*.

1.62. Suportar IPv4 e IPv6.

1.63. Possuir certificação IPv6 Ready;

1.64. IPv6 deve suportar os tunelamentos 6in4, 6to4, 4in6 e *IPv6 Rapid Deployment (6rd)* de acordo com a RFC 5969.

1.65. Suporte aos roteamentos estáticos, dinâmico (RIP, BGP e OSPF, OSPFv3) e multicast (PIM-SM e IGMP).

1.66. Deve suportar Roteamento BGP com uso de IPv6;

1.67. Suportar Delegação de Prefixo IPV6 (DHCP PD);

1.68. O firewall deve possuir integração com a plataforma de ZTNA do mesmo fabricante ou integrar de terceiros;

1.69. Deve possuir tecnologia de conectividade SD-WAN;

1.70. A funcionalidade SD-WAN deve suportar conectividade com o Secure SD-WAN oferecido no serviço Microsoft Azure Virtual WAN;

1.71. Deve suportar perfis de SD-WAN para balancear a carga das conexões entre as interfaces,

1.72. Deve possuir métodos de balanceamento: round-robin e persistência de sessão com as seguintes opções de conexão:

a) IP de origem;

b) IP de destino;

c) IP de origem e destino.

1.73. Os links podem ser ponderados para determinar como o tráfego é distribuído entre eles, podendo usar o SLA para selecionar quais links serão incluídos no balanceamento de carga.

1.74. Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SDWAN;

1.75. Deve suportar o uso de, no mínimo, 3 (três) links;

1.76. Deve suportar o uso de links de interfaces físicas, sub-interfaces lógicas de VLAN e túneis IPSec;

1.77. Deve gerar log de eventos que registrem alterações no estado dos links do SD-WAN, monitorados pela checagem de saúde;

1.78. A solução deverá ser capaz de medir o status de saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de Theshold para cada um destes itens, onde será utilizado como fator de decisão nas regras de SD-WAN;

1.79. A solução de SD-WAN deve ser capaz de apresentar de forma gráfica, todos os dados de análise da saúde dos links, contendo gráficos que apresentam no mínimo os critérios descritos acima;

1.80. Os gráficos devem ser apresentados em tempo real e possibilitar a visualização histórica de pelo menos 24 horas, 48 horas, 1 semana e 1 mês;

1.81. A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, para avaliação mais precisa de links que possuem QoS configurado

1.82. A solução deve possuir funcionalidade de criação da malha SD-WAN em diversos firewalls em um único concentrador;
1.83. Esta funcionalidade deve facilitar a configuração do SD-WAN de múltiplos firewalls, criando automaticamente todas as informações necessárias para que o SD-WAN aconteça, como pelo menos, mas não se limitando a: criação de rotas, regras de firewall, objetos e túneis VPNs necessárias;
1.84. A mesma console do concentrador de SD-WAN deve monitorar os links de cada dispositivo implementado, garantindo uma visualização única de todos os dispositivos implementados;
1.85. Deve possibilitar o roteamento baseado em VPNs;
1.86. Deve suportar criar políticas de roteamento;
1.87. Para as políticas de roteamento, devem ser permitidas pelo menos as seguintes condições:
1.88. Interface de entrada do pacote;
1.89. IPs de origem;
1.90. IPs de destino;
1.91. Portas de destino;
1.92. Usuários ou grupos de usuários;
1.93. Aplicação em camada 7
1.94. Deve ser possível escolher um gateway primário e um gateway de backup para as políticas de roteamento.
1.95. Deve suportar a definição de VLANs no firewall conforme padrão IEEE 802.1q e *tagging* de VLAN.
1.96. Deve suportar Extended VLAN;
1.97. O balanceamento de link WAN deve permitir múltiplas conexões de links Internet, checagem automática do estado de links, *failover* automático e balanceamento por peso.
1.98. A solução deverá permitir port-aggregation de interfaces de firewall suportando o protocolo 802.3ad, para escolhas entre aumento de throughput e alta disponibilidade de interfaces;
1.99. Deve permitir a configuração de jumbo frames nas interfaces de rede;
1.100. Deve permitir a criação de um grupo de portas layer2;
1.101. A Solução física deverá apresentar compatibilidade com modens USB (3G/4G), onde apenas seja acionado na eventualidade de falha no link principal;
1.102. A solução deverá permitir configurar os serviços de DNS, *Dynamic* DNS, DHCP e NTP;
1.103. O *traffic shapping (QoS)* deverá ser baseado em rede ou usuário.
1.104. A solução deve permitir o tráfego de cotas baseados por usuários para upload/download e pelo tráfego total, sendo cíclicas ou não-cíclicas.
1.105. Deve possuir otimização em tempo real de voz sobre IP.
1.106. Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).
1.107. Não deverá existir limite de conexões VPN's através da limitação do software do equipamento evitando limitações de carga de trabalho futuras e necessidade de novas aquisições.
1.108. CONTROLE POR POLÍTICAS DE FIREWALL
1.109. Deve suportar controles por: porta e protocolos TCP/UDP, origem/destino e

identificação de usuários.
1.110. O controle de políticas deverá monitorar as políticas de redes, usuários, grupos e tempo, bem como identificar as regras não-utilizadas, desabilitadas, modificadas e novas políticas.
1.111. As políticas deverão ter controle de tempo de acesso por usuário e grupo, sendo aplicadas por zonas, redes e por tipos de serviços.
1.112. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.
1.113. Controle de políticas por países via localização por IP.
1.114. Suporte a objetos e regras IPv6.
1.115. Suporte a objetos e regras *multicast*.

1.6. PREVENÇÃO DE AMEAÇAS

1.6.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e *Anti-Malware* integrados no próprio *appliance* de Firewall ou entregue em múltiplos *appliances* desde que obedeçam a todos os requisitos desta especificação.
1.6.2. Deve realizar a inspeção profunda de pacotes para prevenção de intrusão (IPS) e deve incluir assinaturas de prevenção de intrusão (IPS).
1.6.3. As assinaturas de prevenção de intrusão (IPS) devem ser customizadas. Exceções por usuário, grupo de usuários, IP de origem ou de destino devem ser possíveis nas regras;
1.6.4. Deve suportar granularidade nas políticas de IPS Antivírus e *Anti-Malware*, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens, com customização completa;
1.6.5. A solução contratada deve realizar a emulação de malwares desconhecidos em ambientes de sandbox em nuvem;
1.6.6. Para a eficácia da análise de malwares Zero-Day, a solução de Sandbox deve possuir algoritmos de inteligência artificial, como algoritmos baseados em machine learning;
1.6.7. A funcionalidade de sandbox deve atuar como uma camada adicional ao motor de antimalware, e ao fim da análise do artefato, deverá gerar um relatório contendo o resultado da análise, bem como os screenshots das telas dos sistemas emulados pela plataforma;
1.6.8. Deve permitir configuração da exclusão de tipos de arquivos para que não sejam enviados para o sandbox em nuvem;
1.6.9. A proteção *Anti-Malware* deverá bloquear todas as formas de vírus, *web malwares*, *trojans* e *spyware* em HTTP e HTTPS, FTP e *web-emails*.
1.6.10. A proteção Anti-Malware deverá realizar a proteção com emulação *JavaScript*.
1.6.11. Deve ter proteção em tempo real contra novas ameaças criadas.
1.6.12. Deve possuir pelo menos duas *engines* de anti-vírus independentes e de diferentes fabricantes para a detecção de *malware*, podendo ser configuradas isoladamente ou simultaneamente.
1.6.13. Deve permitir o bloqueio de vulnerabilidades.
1.6.14. Deve permitir o bloqueio de *exploits* conhecidos.
1.6.15. Deve detectar e bloquear o tráfego de rede que busque acesso a *command and control* e servidores de controle utilizando múltiplas camadas de DNS, *AFC* e

firewall.
1.6.16. Deve incluir proteção contra-ataques de negação de serviços.
1.6.17. Ser imune e capaz de impedir ataques básicos como: *SYN flood, ICMP flood, UDP Flood*, etc.
1.6.18. Suportar bloqueio de arquivos por tipo.
1.6.19. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.
1.6.20. Os eventos devem identificar o país de onde partiu a ameaça.
1.6.21. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas de segurança considerando uma das opções ou a combinação de todas elas: usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por usuários, grupos de usuários, origem, destino, zonas de segurança.
1.6.22. Deve possuir pelo menos duas *engines* de anti-vírus independentes e de diferentes fabricantes para a proteção da aplicação Web, podendo ser configuradas isoladamente ou simultaneamente.
1.6.23. Proteção pelo menos contra os seguintes ataques, mas não limitado a: *SQL injection* e *Cross-site scripting*.
1.7. CONTROLE E PROTEÇÃO DE APLICAÇÕES
1.7.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações por assinaturas e camada 7, utilizando portas padrões (80 e 443), portas não padrões, *port hopping* e túnel através de tráfego SSL encriptado.
1.7.2. Deve ser possível inspecionar os pacotes criptografados com os algoritmos SSL 2.0, SSL 3.0, TLS 1.2 e TLS 1.3.
1.7.3. O motor de análise de tráfego criptografado deve reconhecer, mas não limitado a, pelo menos os seguintes algorítimos: curvas elipticas (ECDH, ECDHE, ECDSA), DH, DHE, Authentication, RSA, DSA, ANON, Bulk ciphers, RC4, 3DES, IDEA, AES128, AES256, Camellia, ChaCha20-Poly1305, GCM, CCM, CBC, MD5, SHA1, SHA256, SHA384.
1.7.4. O motor de inspeção dos pacotes criptografados deve ser configurável e permitir definir ações como não descriptografar, negar o pacote e criptografar para determinadas conexões criptografadas
1.7.5. Reconhecer pelo menos 2.300 aplicações diferentes, classificadas por nível de risco, características e tecnologia, incluindo, mas não limitado a tráfego relacionado a *peer-to-peer*, redes sociais, acesso remoto, *update* de software, serviços de rede, VoIP, streaming de mídia, proxy e tunelamento, mensageiros instantâneos, compartilhamento de arquivos, web e-mail e update de softwares.
1.7.6. Reconhecer pelo menos as seguintes aplicações: *4Shared File Transfer, Active Directory/SMB, Citrix ICA, DHCP Protocol, Dropbox Download, Easy Proxy, Facebook Graph API, Firefox Update, Freegate Proxy, FreeVPN Proxy, Gmail Video, Chat* Streaming, Gmail WebChat, Gmail WebMail, Gmail-Way2SMS WebMail, Gtalk Messenger, Gtalk Messenger File Transfer, Gtalk-Way2SMS, HTTP Tunnel Proxy, HTTPort Proxy, LogMeIn Remote Access, NTP, Oracle database, RAR File Download, Redtube Streaming, RPC over HTTP Proxy, Skydrive, Skype, Skype Services, skyZIP,

SNMP Trap, TeamViewer Conferencing e File Transfer, TOR Proxy, Torrent Clients P2P, Ultrasurf Proxy, UltraVPN, VNC Remote Access, VNC Web Remote Access, WhatsApp, WhatsApp File Transfer e WhatsApp Web.

1.7.7. Deve realizar o escaneamento e controle de *micro app* incluindo, mas não limitado a: *Facebook (Applications, Chat, Commenting, Events, Games, Like Plugin, Message, Pics Download e Upload, Plugin, Post Attachment, Posting, Questions, Status Update, Video Chat, Video Playback, Video Upload, Website), Freegate Proxy, Gmail (Android Application, Attachment), Google Drive (Base, File Download, File Upload), Google Earth Application, Google Plus, LinkedIN (Company Search, Compose Webmail, Job Search, Mail Inbox, Status Update), SkyDrive File Upload e Download, Twitter (Message, Status Update, Upload, Website), Yahoo (WebMail, WebMail File Attach) e Youtube (Video Search, Video Streaming, Upload, Website)*

1.7.8. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de *payload* para checagem de assinaturas de aplicações conhecidas pelo fabricante.

1.7.9. Atualizar a base de assinaturas de aplicações automaticamente.

1.7.10. Reconhecer aplicações em IPv6.

1.7.11. Limitar a banda usada por aplicações (*traffic shaping*).

1.7.12. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory e Azure AD, sem a necessidade de instalação de agente no *Domain Controller*, nem nas estações dos usuários.

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

1.7.14. Deve permitir o uso individual de diferentes aplicativos para usuários que pertencem ao mesmo grupo de usuários, sem que seja necessária a mudança de grupo ou a criação de um novo grupo. Os demais usuários deste mesmo grupo que não possuem acesso a estes aplicativos devem ter a utilização bloqueada.

1.8. CONTROLE E PROTEÇÃO WEB

1.8.1. Deve permitir especificar política de navegação Web por tempo, ou seja, a definição de regras para um determinado dia da semana e horário de início e fim, permitindo a adição de múltiplos dias e horários na mesma definição de política por tempo. Esta regra de tempo pode ser recorrente ou em uma única vez.

1.8.2. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs e redes;

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

1.8.4. Deve permitir autenticação em 2 fatores em conjunto com a autenticação Radius;

1.8.5. Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

1.8.6. Possuir pelo menos 90 categorias de URLs;

1.8.7. Suportar a capacidade de criação de políticas baseadas no controle por URL e

Categoria de URL;
1.8.8. Deve ser capaz de forçar o uso da opção Safe Search em sites de busca;
1.8.9. Deve ser capaz de forçar as restrições do Youtube
1.8.10. Deve ser capaz de categorizar as URLs a partir de base ou cache de URLs locais ou através de consultas dinâmicas na nuvem do fabricante, independentemente do método de classificação a categorização não deve causar atraso na comunicação visível ao usuário;
1.8.11. Suportar a criação categorias de URLs customizadas;
1.8.12. Suportar a opção de bloqueio de categoria HTTP e liberação da categoria apenas em HTTPS.
1.8.13. Deve ser possível reconhecer o pacote HTTP independentemente de qual porta esteja sendo utilizada
1.8.14. Suportar a inclusão nos logs do produto de informações das atividades dos usuários;
1.8.15. Deve salvar nos logs as informações adequadas para geração de relatórios indicando usuário, tempo de acesso, bytes trafegados e site acessado.
1.8.16. Deve permitir realizar análise flow dos pacotes, entendendo exatamente o que aconteceu com o pacote em cada checagem;
1.8.17. Deve ser possível realizar *caching* do conteúdo web;
1.8.18. Deve realizar filtragem por mime-type, extensão e tipos de conteúdo ativos, tais como, mas não limitado a*: ActiveX, applets* e *cookies*.
1.8.19. Deve ser possível realizar a liberação de cotas de navegação para os usuários, permitindo que os usuários tenham tempos pré-determinados para acessar sites na internet.
1.8.20. A console de gerenciamento deve possibilitar a visualização do tempo restante para cada usuário, bem como reiniciar o tempo restante com o intuito de zerar o contador.
1.8.21. Deve possuir capacidade de alguns usuários previamente selecionados realizarem um bypass temporário na política de bloqueio atual.
A solução deve permitir o enforce dos domínios do Google e Office365 a fim de determinar em quais domínios os usuários poderão se autenticar;

1.9. IDENTIFICAÇÃO DE USUÁRIOS

1.9.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticando via LDAP, *Active Directory, Azure AD, Radius, eDirectory, TACACS+* e via base de dados local, para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários.
1.9.2. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (*Captive Portal*).
1.9.3. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços.
1.9.4. Deve permitir autenticação em modos: transparente, autenticação proxy

(explicito, NTLM e Kerberos) e autenticação via clientes nas estações com os sistemas operacionais Windows, macOS e Linux 32/64.

1.9.5. Ao se utilizar da opção de proxy explicito, deve permitir a autenticação por cada conexão, a fim de garantir que usuários logados em servidores de multisessão sejam identificados corretamente pelo firewall, mesmo quando utilizando-se apenas 1 IP de origem;

1.9.6. Deve possuir a autenticação Single sign-on para, pelo menos, os sistemas de diretórios *Active Directory*, Azure AD e *eDirectory*.

1.9.7. Dever suportar a configuração de logon único (Single sign-on) para que os administradores façam logon no console da Web usando o Azure AD

1.9.8. Deve possuir portal do usuário para que os usuários tenham acesso ao uso de internet pessoal, troquem senhas da base local e façam o download de softwares para as estações presentes na solução.

1.10. QUALIDADE DE SERVIÇO - QoS

1.10.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações.

1.10.2. A solução deverá suportar *Traffic Shaping* (Qos) e a criação de políticas baseadas em categoria web e aplicação por: endereço de origem; endereço de destino; usuário e grupo do LDAP/AD.

1.10.3. Deve ser configurado o limite e a garantia de upload/download, bem como ser priorizado o tráfego total e *bitrate* de modo individual ou compartilhado.

1.10.4. Suportar priorização *Real-Time* de protocolos de voz (VoIP).

1.10.5. Deve permitir aplicar prioridade mesmo após o roteamento, utilizando o protocolo DSCP;

1.11. REDES VIRTUAIS PRIVADAS - VPN

1.11.1. Suportar VPN *Site-to-Site e Cliente-to-Site*.

1.11.2. Suportar IPsec VPN.

1.11.3. Suportar SSL VPN.

1.11.4. Suportar L2TP e PPTP.

1.11.5. Suportar acesso remoto SSL, IPSec e VPN Client para Android e iPhone/iPAD.

1.11.6. Deve ser disponibilizado o acesso remoto ilimitado, até o limite suportado de túneis VPN pelo equipamento, sem a necessidade de aquisição de novas licenças e sem qualquer custo adicional para o licenciamento de clientes SSL.

1.11.7. Deve possuir o acesso via o portal de usuário para o download e configuração do cliente SSL para Windows.

1.11.8. Deve possuir opção de VPN IPSEC com client nativo do fabricante.

1.11.9. Deve possuir um portal encriptado baseado em HTML5 para suporte pelo menos a: RDP, SSH, Telnet e VNC, sem a necessidade de instalação de clientes VPN nas estações de acesso.

1.11.10. A VPN IPsec deve suportar: DES, 3DES, GCM, Suite-B, Autenticação MD5 e SHA-1; *Diffie-Hellman Group 1, Group 2, Group 5 e Group 14*; Algoritmo Internet Key Exchange (IKE); AES 128, 192 e 256 (*Advanced Encryption Standard*); SHA 256, 384 e 512; Autenticação via certificado PKI (X.509) e *Pre-shared key* (PSK).

1.11.11. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, SonicWALL, Fortinet, Huawei, Juniper, Palo Alto Networks e Sophos.
1.11.12. Deve suportar nativamente a integração com a Amazon, a fim de estabelecer um túnel seguro entre os appliances e o VPN da AWS.
1.11.13. Deve permitir criar políticas de controle de aplicações, IPS, Antivírus, *Anti-Malware* e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
1.11.14. Suportar autenticação via AD/LDAP, *Token* e base de usuários local;
1.11.15. Permitir estabelecer um túnel SSL VPN com uma solução de autenticação via LDAP, *Active Directory, Azure AD, Radius, eDirectory, TACACS+* e via base de dados local;

1.12. GERÊNCIA ADMINISTRATIVA CENTRALIZADA

1.12.1. Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos através de uma única console central, com administração de privilégios e funções.
1.12.2. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.
1.12.3. Estar licenciada para gerenciar as soluções de firewall de próxima geração**.**
1.12.4. Devem ser fornecidas soluções virtuais ou via *appliances* desde que obedeçam a todos os requisitos desta especificação.
1.12.5. Deve ser centralizada a gerência de todas as políticas do firewall e configurações para as soluções de firewall de próxima geração, sem necessidade de acesso direto aos equipamentos.
1.12.6. Deve permitir a criação de Templates para configurações.
1.12.7. Deve possuir indicadores do estado de equipamentos e rede.
1.12.8. Deve emitir alertas baseados em *thresholds* customizáveis, incluindo também alertas de expiração de subscrição, mudança de *status* de *gateways*, uso excessivo de disco, eventos ATP, IPS, ameaças de vírus, navegação, entre outros.
1.12.9. Deve permitir a criação de grupos de equipamentos por nome, modelo, *firmware* e regiões.
1.12.10. Deve ter controle de privilégios administrativos, com granularidade de funções (VPN admin, App e Web admin, IPS admin, etc);
1.12.11. Deve ter controle das alterações feitas por usuários administrativos, comparar diferentes versões de configurações e realizar o processo de *roll back* de configurações para mudanças indesejadas;
1.12.12. Deve ter logs de auditoria de uso administrativo e atividades realizadas nos equipamentos.
1.12.13. Deve ter integração com a solução de logs e relatórios, habilitando o provisionamento automático de novos equipamentos e a sincronização dos administradores da centralização da gerência com a centralização de logs e relatórios. Deve possibilitar o envio dos logs via syslog com conexão segura (TLS)

1.13. GERÊNCIA DE LOGS E RELATÓRIOS CENTRALIZADOS

1.13.1. Deve possuir solução de logs e relatórios centralizados, possibilitando a consolidação total de todas as atividades da solução através de uma única console central.
1.13.2. Estar licenciada para gerenciar as soluções de firewall de próxima geração**.**
1.13.3. Devem ser fornecidas soluções virtuais, ou em nuvem ou via *appliances* desde

que obedeçam a todos os requisitos desta especificação, com armazenamentomínimo de 200GB de dados.
1.13.4. Deverá prover relatórios baseados em usuários, com visibilidade sobre acesso a aplicações, navegação, eventos ATP, downloads e consumo de banda, independente em qual rede ou IP o usuário esteja se conectando.
1.13.5. Deve possibilitar a identificação de ataques como a identificação de malware identificados pelos eventos ATP, usuários suspeitos, tráfegos anômalos incluindo tráfego ICMP e consumo não-usual de banda.
1.13.6. Deve conter relatórios pré-configurados, pelo menos de: aplicações, navegação, web server (WAF), IPS, ATP e VPN;
1.13.7. Deve fornecer relatórios históricos para análises de mudanças e comportamentos.
1.13.8. Deve conter customizações dos relatórios para inserção de logotipos próprios.
1.13.9. Deve fornecer relatórios de *compliance* SOX, HIPAA, GLBA, FISMA, PCI, CIPA
1.13.10. Deve permitir a exportação via PDF ou Excel.
1.13.11. Deve fornecer relatórios sobre os acessos de procura no Google, Yahoo, Bing e Wikipedia.
1.13.12. Deve fornecer relatórios de tendências.
1.13.13. Deve fornecer logs em tempo real, de auditoria e arquivados.
1.13.14. Deve possuir mecanismo de procura de logs arquivados.

1.14 GERÊNCIA DE BACKUPS

1.14.1 A CONTRATADA deverá disponibilizar a unidade de armazenamento dos backups dos equipamentos de Firewall.
1.14.2 Será de responsabilidade da CONTRATADA implementar e configurar a transferência de backup no repositório em nuvem segura.
1.14.3 O licenciamento e operação do ambiente em nuvem é de total responsabilidade da CONTRATADA;
1.14.4 O armazenamento de dados da CONTRATANTE deverá estar localizado no estado de São Paulo - Brasil, mantendo assim uma menor latência na comunicação e transferência de dados;
1.14.5 A CONTRATADA deverá garantir a segurança da informação dos dados e estrutura em nuvem que irá hospedar os dados de backup da CONTRATANTE. se responsabilizando por qualquer dano causado a eles;
1.14.6 O backup e o reestabelecimento de configuração deverão ser feitos localmente, via FTP ou e-mail com frequência diária, semanal ou mensal, podendo também ser realizado por demanda.

2. SERVIÇO DE SEGURANÇA PARA ESTAÇÕES DE TRABALHO

2.1. Possuir console central única de gerenciamento. As configurações do Antivírus, AntiSpyware, Firewall, Detecção de intrusão controle de Dispositivos e Controle de Aplicações deverão ser realizadas através da mesma console;
2.2. O Produto deverá ter a capacidade de remoção do software de antivírus já instalado e ser instalado de forma remota pela console de gerenciamento;
2.3. O produto deverá possuir no mínimo os seguintes módulos:

2.4. Console de Gerenciamento fornecendo funcionalidades de gestão;
2.5. Módulos para estações físicas, laptops e servidores;
2.6. Módulo para ambientes virtualizados, sendo criado especialmente para ambientes virtuais;
2.7. Utilizar o conceito de heurística;
2.8. Oferecer tecnologia onde a solução explore vulnerabilidades de softwares instalados no intuito de reduzir o risco
de infecções (anti-exploit);
2.9. Oferecer tecnologia nativa no intuito de eliminar ameaças do tipo Ransomware;
2.10. Oferecer inventário de softwares;
2.11. Oferecer tecnologia onde a solução teste arquivos potencialmente perigosos em ambiente isolado antes da execução do mesmo no ambiente de produção;
2.12. Oferecer proteção por base de assinaturas;
2.13. Instalação e configuração
2.14. Deve ser fornecido como um appliance virtual ou executável para instalação em servidores Windows ou Console com Gerenciamento na nuvem (Cloud).
2.15. Deverá suportar no mínimos os seguintes Hypervisors: VMWare vSphere, Citrix XenServer; XenDesktop, VDI-ina-
Box;
2.16. Microsoft Hyper-V, Red hat Enterprise Virtualization, Kernel-based Virtual Machine ou KVM, Oracle VM;
2.17. Deverá ser fornecido com base de dados embutido na Console em Nuvem, sem a necessidade de baixar para
máquina do administrador da Console;
2.18. Permitir instalação remota via console WEB de gerenciamento para ambientes virtual VMWare ou Citrix;
2.19. O mecanismo de varredura deverá estar disponível para download separadamente;
2.20. A solução deverá permitir a inclusão de um modulo de balanceamento para casos em vários servidores tenham a
mesma função (para alta disponibilidade, recuperação de desastres, performance entre outras);
2.21. Deve ser totalmente em português.
2.22. Arquitetura simples de atualização, com botão único para acesso a todas as funções e serviços serem
atualizados;
2.23. Permitir que o administrador escolha qual o pacote será atualizado;
2.24. As notificações devem ser destacadas como item não lida, enviar e-mail para o administrador;
2.25. No mínimo enviar notificações:

- Problemas com licenças,
- Alertas de Surto de vírus,
- Máquinas desatualizadas,
- Eventos de antimalware,

2.26. Painel para Monitoramento baseado em "portlets" configuráveis com no mínimo as seguintes especificações:
Nome; Tipo de relatório; Alvo do relatório;
2.27. Deverá disponibilizar "portlets" para qualquer serviço de segurança, máquinas físicas, virtuais, dispositivos
móveis;
2.28. Inventário da Rede
2.29. Possuir no mínimo as integrações abaixo: Múltiplos domínios do Active Directory, Múltiplos VMWare vCenters,
Múltiplos Citrix Xen Servers;
2.30. Possuir a possibilidade de definição de sincronização com o Active Directory em horas;
2.31. Deverá ser compatível com Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM;
2.32. Descoberta de rede para máquinas em grupo de trabalho;
2.33. Possuir busca em tempo real pelo menos com os seguintes filtros: Nome, Sistema Operacional e Endereço IP;
2.34. Possibilitar a instalação remota e desinstalação remota do antivírus;
2.35. Possibilitar a configuração de pacotes de instalação do produto de antivírus;
2.26. Possuir tarefas remotas e configuráveis de Scan;
2.37. Possuir tarefa de reinicialização remota de estação ou servidor;
2.38. Assinar políticas para no mínimo os níveis: Computador, Máquina Virtual ou Possuir a propriedade detalhada
de objetos gerenciados para: Nome, IP, Sistema Operacional, Grupo, Política Assinada, último status de malware;
2.39. Modelo único para todos os equipamentos, seja físico ou virtual;
2.40. Cada serviço de segurança deve ter seu modelo configurável de política com opções específicas de
ativar/desativar;
2.41. Deverá configurar as funcionalidades como escaneamento do Antivírus, firewall de duas vias de detecção de
intrusão, controle de acesso a rede, controle de aplicação, controle de acesso web, autenticação e ações para
serem aplicadas em caso de vírus e dispositivos em não conformidade;
2.42. Relatório para cada serviço de segurança;
2.43. Facilidade de usar e visualização simplificada;

2.44. Agendamento, com opção de envio por e-mail para qualquer destinatário conforme escolha do administrador;
2.45. Filtros de agendamento de relatórios;
2.46. Arquivo com todas as instâncias de relatório agendados;
2.47. Exportar o relatório nos formatos .pdf e/ou .csv;
2.48. Oferecer possibilidade de criar relatórios de maneira dinâmica no painel administrativo da solução.
2.49. Restauração remota, com configuração de localidade e deleção;
2.50. Criação e exclusão para arquivos restaurados;
2.51. Administração baseada em regras;
2.52. Disponibilizar tipos de usuários pré-definidos como no mínimo: Administrador - Gerente dos componentes da
solução, Administrador de rede - Gerente dos serviços de segurança;
2.53. Relatório - Monitora e cria relatórios;
2.54. Deverá ser possível customizar um tipo de usuário;
2.55. Deverá permitir a integração do usuário com o Active Directory para autenticação da console de gerenciamento;
2.56. Logs de utilização;
2.57. Registrar as ações do usuário na console de gerenciamento;
2.58. Detalhar cada ação do usuário;
2.59. Permitir busca complexa baseada em ações do usuário, intervalos de tempo;
2.60. Deverá prover o acesso via HTTPS;
2.61. Deverá permitir a importação de certificados digitais;
2.62. O gerenciamento e a comunicação com dispositivos móveis devem ser feitos de forma segura utilizando certificados digitais;
2.63. Deverá permitir a configuração do scan do antivírus do cliente como: Scan local, Scan Hibrido, Scan Central;
2.64. Deverá permitir a instalação customizada do antivírus com no mínimo: Instalar o antivírus sem o controle de
acesso a internet; Instalar o antivírus sem o módulo de firewall;
2.65. Deverá suportar no mínimo os seguintes sistemas operacionais para estação de trabalho: Windows 10 32 e
64Bits, Windows 7 32 e 64Bits.
2.66. Deverá suportar no mínimo os seguintes sistemas operacionais para servidores: Windows Server 2022 Windows Server 2019 Core Windows Server 2019,Windows Server 2019 Core, Windows Server 2016, Windows Server 2016 Core, Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Server 2008 R2.
2.67. Deverá suportar no mínimo os seguintes sistemas operacionais para distribuição Linux: Ubuntu 14.04 LTS ou superior, Red Hat Enterprise Linux /

CentOS 6.0 ou superior, SUSE Linux Enterprise Server 11 SP4 ou superior, OpenSUSE Leap 42.x, Fedora 25 ou superior, Debian 8.0 ou superior, Oracle Linux 6.3 ou superior, Amazon Linux AMI 2016.09 ou superior;

2.68. Deverá permitir ao administrador customizar a instalação;

2.69. A instalação deverá ser possível executar com no mínimo das seguintes maneiras: Executar o pacote de
antivírus diretamente na estação de trabalho, instalar remotamente, distribuído via console de gerencia web;

2.70. Deverá ser possível ter um relatório com as estações instaladas e as faltantes da instalação;

2.71. A console de gerenciamento deve incluir informações detalhadas sobre as estações e servidores com no
mínimo as seguintes informações: Nome, IP, Sistema Operacional, Política Aplicada;

2.72. Através da console, o administrador poderá enviar uma política única para configurar o antivírus;

2.73. A console de gerenciamento deverá incluir sessão de log com as seguintes informações: Login, Edição, Criação,
Log-out, ter a capacidade de criar um único pacote independente ser for para 32 bits ou 64 bits, deverá permitir
ao administrador criar grupos e subgrupos para mover as estações de trabalho;

2.74. O agente utilizado na sincronização deve ser incluído no cliente do antivírus e não ser necessário à distribuição
em um agente separado;

2.74. Proteção de antivírus dedicado para ambientes virtuais;

2.75. Deverá ter a disponibilidade de ser integrado com o VMWare e oferecer a escaneamento sem instalar o
produto na máquina virtual;

2.76. A console de gerenciamento central da solução deverá ter a possibilidade de integrar com múltiplos vCenters
da VMWare;

2.77. Deverá proteger em tempo real e agendado as máquinas virtuais Linux;

2.78. O produto deverá oferecer agente para virtualização dos seguintes produtos: Citrix Xen Server, Microsoft
Hyper-V, Red Hat Virtualization, Oracle KVM, KVM;

2.79. Deverá ter métodos de detecção de vírus, Spyware, rootkits e outros mecanismos de segurança;

2.80. Deverá reportar o estado atual das VMs no mínimo, protegida/desprotegida;

2.81. Plataformas de Virtualização:

- VMware vSphere and vCenter Server versão 6.5;

- VMware vSphere and vCenter Server version 6.7, incluindo update 1, update 2a e update 3;
- VMware vSphere and vCenter Server version 7.0, incluindo update 1, update 2, update 2b, update 2c e update 2d;
- VMware vSphere and vCenter Server version 8.0, incluindo update 1, update 2.
- VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x
- VMware Workstation 11.x, 10.x, 9.x, 8.0.6
- VMware Player 7.x, 6.x, 5.x
- Citrix Xen Hypervisor: 7.1 (with the XS71ECU2060 hotfix), 8.2.
- Citrix Virtual Apps e Desktops 7 1808, 7 1811, 7 1903, 7 1906
- Citrix XenApp e XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR
- Citrix VDI-in-a-Box 5.x
- Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2, 2016, 2019 or Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019 (incluindo Hyper-V Hypervisor).
- Red Hat Enterprise Virtualization 3.0 (incluindo KVM Hypervisor).
- Oracle VM 3.0.
- Oracle VM VirtualBox 5.2, 5.1
- Nutanix Prism com AOS 5.6, 5.5, 5.20 LTS, 5.18 STS, 5.15 LTS, 5.11, 5.10 (Enterprise Edition)
- Nutanix Prism with AHV 20170830.115, 20170830.301, 20170830.395 e 20190916.294 (Community Edition)

2.82. Sistemas Operacionais desktops (32 e 64 Bits): Windows 7, Windows 10

2.83. Sistemas Operacionais Servidores: Windows Server 2022 Windows Server 2019 Core Windows Server 2019, Windows Server 2019 Core, Windows Server 2016, Windows Server 2016 Core, Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Server 2008 R2,
Ubuntu 14.04 LTS ou superior, Red Hat Enterprise Linux / CentOS 6.0 ou superior, SUSE Linux Enterprise Server 11 SP4 ou superior, OpenSUSE Leap 42.x, Fedora 25 ou superior, Debian 8.0 ou superior, Oracle Linux 6.3 ou superior, Amazon Linux AMI 2016.09 ou superior;

2.84. Deverá fazer scan em tempo real automático;

2.85. Deverá ser configurável para não escanear arquivos conforme necessidade do administrador, ou seja, por
tamanho ou por tipo de extensão;

2.86. Escaneamento de comportamento heurístico;

2.87. Deverá escanear em tempo real qualquer informação localizadas em mídias de armazenamento como:

CD/DVD, Discos Externos, Pen-Drivers, Deverá permitir a escolha e configuração de pastas a serem escaneada;
2.88. Para melhor proteção, o antivírus deverá ter no mínimo 3 tipos de detecção: Baseada em Assinaturas, Baseada
em Heurística, Baseada em monitoramento contínuo de processos;
2.89. Deverá ter a capacidade de escaneamento nos protocolos HTTP e SSL na Estações de trabalho;
2.90. O cliente do antivírus deverá ter o módulo de Antiphishing que deverá ter a opção de verificar links
pesquisados com os sites de pesquisas Search Advisor na Estações de trabalho;
2.91. Deverá possuir módulo de firewall que de acordo com o administrador poderá ou não ser
instalado/desinstalado nas estações de trabalho;
2.92. O módulo de firewall deverá ser possível configurar o modo invisível tanto a nível de rede local ou Internet nas
estações de trabalho;
2.93. Deverá permitir o envio automático de arquivos da quarentena para o laboratório de vírus;
2.94. Deverá fazer a remoção automática de arquivos antigos, pré-definidos pelo administrador;
2.95. Deverá permitir a movimentação do arquivo da quarentena para seu local original ou outro destino que o
administrador definir;
2.96. Deverá de forma automática criar exclusão para arquivos restaurados da quarentena;
2.97. Deverá permitir escanear a quarentena após a atualização das atualizações de assinaturas;
2.98. Deverá ter módulo de controle de usuário integrando com as seguintes características: Bloqueio de acesso a
internet, Bloqueio de acesso a aplicações definidas pelo administrador;
2.99. Deverá ser possível a instalação do módulo de controle de dispositivos através da console de gerenciamento;
2.100. Através do módulo de controle de dispositivo deverá ser possível controlar: Bluetooth, CDROM/DVDROM, IEEE
1284.4, IEEE 1394, Windows Portable, Adaptadores de Rede, Adaptadores de rede Wireless, Discos Externos;
2.101. Deverá permitir regras de definição de bloqueio/desbloqueio;
2.102. Deverá permitir regras de exclusão;
2.103. Após a atualização o administrador deverá ter a capacidade de adiar uma reinicialização;

2.104. Possibilidade de utilizar um servidor local para efetuar as atualizações das estações de trabalho;
2.105. Permitir atualizações de assinatura de hora em hora;
2.106. Permitir motor de varredura local, no servidor de rede ou em nuvem afim de aumentar o desempenho da
estação de trabalho quando a mesma estiver sendo escaneada.
2.107. Fornecer proteção para ambiente Exchange
2.108. Oferecer tecnologia para proteção contra spam;
2.109. Oferecer análise comportamental e proteção para zero-day;
2.110. Oferecer proteção contra vírus e tentativas de phishing;
2.111. Possibilidade de criptografia de disco através da console de gerenciamento seja em nuvem ou on-premise com
módulo de Criptografia presente na mesma Console do Antivirus.
2.112. Deverá utilizar quando necessários serviços de criptografia através agentes nativos da estação de trabalho
baseada em Windows (BitLocker) ou Mac (FileVault);
2.113. Deverá solicitar autenticação quando iniciado o sistema operacional do equipamento;
Deverá ser compatível com:

- macOS Sonoma (14.x)
- macOS Ventura (13.x)
- macOS Monterey (12.x)
- macOS Big Sur (11.x)

2.114. Detectar e bloquear todos os tipos de ameaças sofisticadas e malwares desconhecidos bem como eliminar
malwares desconhecidos e ameaças avançadas que ignoram as soluções tradicionais de proteção de endpoints, incluindo o ransomware. Detectar e bloquear ataques avançados, como os ataques do PowerShell, baseados em scripts, ataques sem arquivos e malware sofisticado, devendo ser detectados e bloqueados antes de serem executados.
2.115. Detectar e parar, bloquear e interromper malwares sem arquivos.
2.116. Parar os ataques com base em macros e scripts. Analisar scripts, como Powershell, WMI, intérpretes de Javascript, etc, bem como adicionar técnicas de analisador de linha de comando para interceptar e proteger scripts, enquanto alerta os administradores e bloqueia a execução de scripts no caso de executar comandos maliciosos.
2.117. Reparo e resposta automatizada a ameaças
2.118. Quando uma ameaça é detectada, a ferramenta deve neutralizá-la imediatamente por meio de ações que

incluem a conclusão do processo, a quarentena, a exclusão e a reversão de alterações mal intencionadas.
Compartilhar as informações sobre ameaças em tempo real com a GPN, o serviço de inteligência contra
ameaças baseadas na nuvem do fabricante, para impedir ataques semelhantes.
2.119. Obter visibilidade e contexto sobre ameaças devendo identificar e reportar atividades suspeitas alertando
antecipadamente para comportamentos maliciosos, como ações suspeitas do sistema operacional.
2.120. Operar com um único agente e console integrados bem como personalizar automaticamente o pacote de instalação e minimizar o carregamento do agente.
2.121. Deverá ter um nível de proteção na fase de pré-execução com modelos locais de aprendizado de máquina e heurística avançada e treinada para detectar ferramentas de hackers, explorações e técnicas de ocultação de malware, a fim de bloquear ameaças sofisticadas antes que elas sejam executadas. Também deverá detectar técnicas de propagação e sites que hospedam kits de exploração, além de bloquear tráfego suspeito na web.
2.122. Deverá permite que os administradores de segurança ajustem a proteção para combater os riscos.
2.123. As técnicas de Machine Learning devem utilizar modelos e algoritmos extensamente treinados para prever e bloquear os ataques avançados.
2.124. A ferramenta de Machine Learning deve se basear em características estáticas e dinâmicas, e se treinarem
continuamente com bilhões de amostras de arquivos legítimos e maliciosas devendo melhorar significativamente a efetividade da detecção de malware e minimizar os falsos positivos. ações evasivas e conexões a centros de comando e controle.
2.125. Sandbox integrado nos terminais que deverá analisar arquivos suspeitos em profundidade, acionar ações destrutivas em um ambiente virtual isolado, hospedado pelo fabricante, analisando seu comportamento e informando sobre intenções maliciosas. O Sandbox deve ser integrado com o agente e encaminhar automaticamente os arquivos suspeitos para análise. Ao retornar uma análise com resultado "malicioso", o Sandbox deverá bloquear automaticamente o arquivo malicioso em sistemas em toda rede imediatamente. O recurso de envio automático deve permitir que os administradores de segurança da empresa escolham o modo de monitoramento ou bloqueio, o que impede o acesso a um arquivo até que um resultado seja emitido. Os administradores também podem enviar arquivos manualmente para análise. As informações forenses devem
fornecem um contexto claro das ameaças e ajudar a entender o comportamento delas.

2.125. Deverá conter antiexploit avançado para prevenção de exploração e proteção a memória e aplicativos vulneráveis, como navegadores, leitores de documentos, arquivos multimídia e tempo de execução (ou seja:Flash ou Java). Os ecanismos avançados devem observar a rotina de acesso na memória para detectar e bloquear técnicas de exploração, como verificação de chamadas de API, pivotamento de pilha, ROP (returnoriented programming), etc.

2.126. O Inspetor de Processos deverá operar em um modo de confiança zero, monitorando continuamente todos os processos em execução no sistema operacional. Deverá procurar atividades suspeitas ou comportamentos anormais de processos, como tentativas de ocultar o tipo de processo, executar código no espaçode outro processo (seqüestro de memória do processo para escalonamento de privilégios), replicar, descartar arquivos, ocultar para processar aplicativos de listagem etc. Tomar as medidas de reparação adequadas, incluindo o encerramento do processo e a reversão das alterações efetuadas. Deverá detectar de malwares desconhecidos, avançados e ataques sem arquivos, incluindo ransomware.

2.127. Deverá realizar a correlação entre terminais, conhecida como EDR, levando a detecção de ameaças bem como aplicar funcionalidades de XEDR para detectar ataques avançados em vários terminais em infraestruturas híbridas (estações de trabalho ou servidores executando vários sistemas operativos)

2.128. Deverá analisar continuamente os riscos usando centenas de fatores para descobrir e priorizar os riscos de configuração para todos os seus terminais, permitindo ações automáticas de fortalecimento. Identificar ações e comportamentos dos usuários que representam um risco de segurança para a organização, como o uso de páginas web não criptografadas para fazer login em sites, gerenciamento de senhas inadequado, uso de USBs comprometidos, infecções recorrentes, etc.

3. SERVIÇO DE SUPORTE TÉCNICO E MONITORAMENTO DE REDES E WI-FI

3.1. O atendimento de suporte técnico e monitoramento deverá atuar com todas as soluções propostas nesse termo de referência, itens 1, 2 e 3, adicionando também os itens da tabela a seguir:

TABELA DE EQUIPAMENTOS		
QTDE	**FABRICANTE E MODELO**	**TIPO**
29	Aruba 2930F	Switch
2	HPE OfficeConnect 1820	Switch
1	Aruba 7205 Controller	Controladora Wi-Fi

134	Aruba AP-305 Access Point	Ponto de Acesso Wi-Fi
4	Aruba AP-365 Access Point	Ponto de Acesso Wi-Fi

3.2. O suporte técnico completo se refere a toda e qualquer demanda ocasionada de impacto produtivo do ambiente computacional da FUNDAÇÃO EDUCACIONAL DO MUNICÍPIO DE ASSIS com o escopo de atendimento dos itens 1, 2, 3 e TABELA DE EQUIPAMENTOS.

3.3. Em casos que envolva o hardware ou software proprietário dos fabricantes, se possível, a **CONTRATADA** será a responsável pela abertura de chamados, acompanhamento e atendimento diretamente com o fabricante.

3.4. O monitoramento deverá cobrir todos os itens destacados na TABELA DE EQUIPAMENTOS e nos itens 1, 2 e 3 desse Termo de Referências.

3.5. Registrar, diagnosticar e solucionar problemas no escopo de serviço mencionado neste termo de referência.

3.6. Correlacionar incidentes a fim de identificar sua causa-raiz, solucioná-la e prevenir novas ocorrências.

3.7. Executar ações correlatas, que demandem maior esforço ou complexidade (ex: instalações e ou atualizações de software em grande quantidade de equipamentos, elaboração de roteiro específico etc.), solicitadas diretamente pelo Gestor do Contrato por parte da **CONTRATANTE** e devidamente registradas no Sistema de atendimento técnico.

3.8. CHAMADOS E ATENDIMENTO TÉCNICO

3.9. A **CONTRATANTE** deverá abrir chamados de manutenção através de chamada telefônica, central de atendimento via navegador (Web) ou e-mail, sem a necessidade prévia de consulta e/ou qualquer liberação por parte da fornecedora da solução sem nenhum custo adicional.

Prioridade	Descrição	Início do Atendimento
1	Serviço completamente indisponível	Até 1 hora
2	Serviço operando parcialmente	Até 4 horas

3	Serviço com degradação de qualidade	Até 8 horas
4	Problemas que não impactam no funcionamento do serviço, dúvidas e solicitações em geral	Programada

Descrição das Prioridades	
1 (Crítica)	O serviço está fora de operação ou há um impacto crítico nas operações dos negócios.
2 (Alta)	O serviço está degradado, ou aspectos significativos das operações de negócio sofreram impactos negativos pelo desempenho inadequado.
3 (Média)	Serviço funcionando com pequenos problemas sem impacto direto na operação.
4 (Baixa)	Manutenção preventiva e gestão de melhorias

3.10. O atendimento técnico deverá ocorrer de 24x7x365 (Vinte e quatro horas por dia, sete dias da semana e nos trezentos e sessenta e cinco dias no ano) de forma interrupta.
3.11. Não deve haver limites para aberturas de chamados, sejam dúvidas, configurações ou resolução de problemas.
3.12. A equipe de suporte técnico deverá buscar, no escopo de serviços, prevenir a ocorrência de problemas e seus incidentes resultantes, eliminando incidentes recorrentes correlacionando-os e identificando a causa-raiz e sua solução, além de minimizar o impacto dos incidentes que não podem ser prevenidos.
3.13. Todos os atendimentos deverão estar registrados em central de atendimento técnico e gestão de chamados.
3.14. Deve haver realização de otimizações nas configurações para melhor do desempenho, quando observadas quedas de desempenho ou indisponibilidades pela **CONTRATANTE** ou **CONTRATADA.**
3.15. CENTRAL DE ABERTURA DE CHAMADOS:
3.16. A **CONTRATADA** deverá disponibilizar e gerenciar os atendimentos técnicos da **CONTRATANTE** através de portal de gerenciamento de atendimentos com acesso através de navegador web.
3.17. Mesmo os chamados sendo abertos através de ligação telefônica ou correio eletrônico, os chamados deverão ser registrados na central.
3.18. A solução deverá ser aderente aos processos do ITIL para gerenciamento de incidentes e requisições.
3.19. A solução deverá contar com perfis de usuários, sendo possível a criação de acessos somente leitura.

3.20. A solução deverá permitir a exportação dos chamados em .PDF e .CSV.

3.21. MONITORAMENTO DO AMBIENTE:

3.22. O serviço de monitoramento deverá ser composto de tecnologia que seja apartada do ambiente computacional da **CONTRATANTE**.

3.23. A fonte de carregamento de energia deverá ser conectada através da porta tipo-C com uma tomada do rack com o tipo padrão NBR 14136 de três pinos, sendode voltagem 100/240 VA, 5V de 3000mA, com fio que não deverá ser superior a 100cm.

3.24. A **CONTRATANTE** não disponibilizará recursos computacionais para a instalação do sistema de monitoramento.

3.25. Deverá possuir uma entrada do tipo RJ-45 com a velocidade de 10/100/1000 Mbps.

3.26. Deverá possuir entradas USB 2.0.

3.27. Deverá possuir entradas de USB 3.0.

3.28. Deverá possuir entradas Micro HDMI 2.0.

3.29. A entrada Micro HDMI deverá possuir o suporte de resolução em 4Kp60.

3.30. Deverá possuir uma entrada A/V habilitado para TV out.

3.31. Deverá possuir 1 entrada categorizada como tipo-C.

3.32. O recurso tecnológico de monitoramento deverá ter suporte para sistema operacional Windows.

3.33. O recurso tecnológico deverá ser um dispositivo para que seja monitorado toda a infraestrutura **CONTRATADA** pela **CONTRATANTE**.

3.34. A comunicação entre cliente e servidor de monitoramento com o datacenter deverá ser feita através do protocolo de comunicação TCP.

3.35. O recurso tecnológico deverá possuir um cooler para que ele consiga realizar a dissipação de calor assim evitando qualquer tipo de impacto no serviço de monitoramento.

3.36. O recurso tecnológico deverá dispor de 4 borrachas de proteção na parte inferior;

3.37. O recurso tecnológico deverá possuir furação para que a dissipação de calor seja mais eficiente;

3.38. O recurso tecnológico deverá possuir o armazenamento em MicroSD deno mínimo128GB;

3.39. A **CONTRATADA** ficará responsável em realizar a entrega do recurso tecnológico juntamente com as respectivas licenças do sistema operacional e softwares de segurança como licença contra-ataques cibernéticos, backup do sistema operacional e até mesmo monitoramento do sistema tecnológico.

3.40. O dispositivo tecnológico deverá possuir uma proteção contra ameaças cibernéticas instalado no recurso tecnológico de monitoramento.

3.41. O dispositivo deverá ter a possibilidade de criptografia de disco através da console de gerenciamento, seja em nuvem ou on-premise com módulo de Criptografia.

3.42. Deverá utilizar quando necessários serviços de criptografia através agentes nativos do recurso tecnológico baseado em Windows;

3.43. Deverá solicitar autenticação quando iniciado o sistema operacional do equipamento;

3.44. Detectar e bloquear todos os tipos de ameaças sofisticadas e malwares desconhecidos bem como eliminar malwares desconhecidos e ameaças avançadas que ignoram as soluções tradicionais de proteção de endpoints, incluindo o ransomware.
3.45. Detectar e bloquear ataques avançados, como os ataques do PowerShell, baseados em scripts, ataques sem arquivos e malware sofisticado, devendo ser detectados e bloqueados antes de serem executados.
3.46. Detectar e parar, bloquear e interromper malwares sem arquivos.
3.47. Parar os ataques com base em macros e scripts. Analisar scripts, como Powershell, WMI, intérpretes de Javascript, etc, bem como adicionar técnicas de analisador de linha de comando para interceptar e proteger scripts, enquanto alerta os administradores e bloqueia a execução de scripts no caso de executar comandos maliciosos.
3.48. Quando uma ameaça é detectada, a ferramenta deve neutralizá-la imediatamente por meio de ações que incluem a conclusão do processo, a quarentena, a exclusão e a reversão de alterações mal-intencionadas.
3.49. Compartilhar as informações sobre ameaças em tempo real com a GPN, o serviço de inteligência contra ameaças baseadas na nuvem do fabricante, para impedir ataques semelhantes.
3.50. Obter visibilidade e contexto sobre ameaças devendo identificar e reportar atividades suspeitas alertando antecipadamente para comportamentos maliciosos, como ações suspeitas do sistema operacional.
3.51. Operar com um único agente e console integrados bem como personalizar automaticamente o pacote de instalação e minimizar o carregamento do agente.
3.52. Deverá ter um nível de proteção na fase de pré-execução com modelos locais de aprendizado de máquina e heurística avançada e treinada para detectar ferramentas de hackers, explorações e técnicas de ocultação de malware, a fim de bloquear ameaças sofisticadas antes que elas sejam executadas.
3.53. Também deverá detectar técnicas de propagação e sites que hospedam kits de exploração, além de bloquear tráfego suspeito na web.
3.54. Deverá permite que os administradores de segurança ajustem a proteção para combater os riscos.
3.55. As técnicas de Machine Learning devem utilizar modelos e algoritmos extensamente treinados para prever e bloquear os ataques avançados.
3.56. A ferramenta de Machine Learning deve se basear em características estáticas e dinâmicas, e se treinarem continuamente com bilhões de amostras de arquivos legítimos e maliciosas devendo melhorar significativamente a efetividade da detecção de malware e minimizar os falsos positivos. ações evasivas e conexões a centros de comando e controle.
3.57. Sandbox integrado no terminal que deverá analisar arquivos suspeitos em profundidade, acionar ações destrutivas em um ambiente virtual isolado, hospedado pelo fabricante, analisando seu comportamento e informando sobre intenções maliciosas.
3.58. O Sandbox deve ser integrado com o agente e encaminhar automaticamente os arquivos suspeitos para análise.
3.59. Ao retornar uma análise com resultado "malicioso", o Sandbox deverá bloquear

automaticamente o arquivo malicioso em sistemas em toda rede imediatamente.

3.60. O recurso de envio automático deve permitir que os administradores de segurança da empresa escolham o modo de monitoramento ou bloqueio, o que impede o acesso a um arquivo até que um resultado seja emitido.

3.61. Os administradores também podem enviar arquivos manualmente para análise. As informações forenses devem fornecem um contexto claro das ameaças e ajudar a entender o comportamento delas.

3.62. Deverá conter antiexploit avançado para prevenção de exploração e proteção a memória e aplicativos vulneráveis, como navegadores, leitores de documentos, arquivos multimídia e tempo de execução (ou seja:Flash ou Java).

3.63. Os mecanismos avançados devem observar a rotina de acesso na memória para detectar e bloquear técnicas de exploração, como verificação de chamadas de API, pivotamento de pilha e ROP (returnoriented programming).

3.64. O Inspetor de Processos deverá operar em um modo de confiança zero, monitorando continuamente todos os processos em execução no sistema operacional.

3.65. Deverá procurar atividades suspeitas ou comportamentos anormais de processos, como tentativas de ocultar o tipo de processo, executar código no espaço de outro processo (sequestro de memória do processo para escalonamento de privilégios), replicar, descartar arquivos e ocultar para processar aplicativos de listagem.

3.66. Tomar as medidas de reparação adequadas, incluindo o encerramento do processo e a reversão das alterações efetuadas.

3.67. Deverá detectar de malwares desconhecidos, avançados e ataques sem arquivos, incluindo ransomware.

3.68. Deverá realizar a correlação entre terminais, conhecida como EDR, levando a detecção de ameaças bem como aplicar funcionalidades de XEDR para detectar ataques avançados em vários terminais em infraestruturas híbridas (estações de trabalho ou servidores executando vários sistemas operativos)

3.69. Deverá analisar continuamente os riscos usando centenas de fatores para descobrir e priorizar os riscos de configuração para todos os seus terminais, permitindo ações automáticas de fortalecimento. Identificar ações e comportamentos dos usuários que representam um risco de segurança para a organização, como o uso de páginas web não criptografadas para fazer login em sites e gerenciamento de senhas inadequadas.

3.70. A **CONTRATADA** deverá monitorar o ambiente 24x7x365 (Vinte e quatro horas por dia, sete dias da semana e nos trezentos e sessenta e cinco dias no ano) de forma interrupta;

3.71. O monitoramento deve contemplar o ambiente de infraestrutura, apresentado nos itens 1, 2, 3 e TABELA DE EQUIPAMENTOS.

3.72. Deverá ter SLA de disponibilidade da console de gerenciamento de no mínimo 99,98%;

3.73. A solução de monitoramento deverá estar hospedada em datacenter com a classificação mínima de Tier III;

3.74. A solução de monitoramento deverá ter portal de acesso de visualização WEB disponibilizada para a **CONTRATANTE**;

3.75. Deverá ser capaz de enviar alertas de alteração de status de sensores através de correio eletrônico;
3.76. Ser capaz de executar áudio pré-definido em caso de alteração de sensores de monitoramento;
3.77. Possuir pelo menos os seguintes status para os sensores de monitoramento: Estado normal, estado de alerta e estado de erro;
3.78. Possuir a possibilidade para criação de interface WEB com mapa de distribuição de arquitetura com o monitoramento, podendo ter acesso público e/ou autenticado através de contas de usuários internas da solução de monitoramento;
3.79. O monitoramento deverá ser compatível com os principais serviços de nuvem pública;
3.80. O sistema de monitoramento deverá contar com aplicativo de administração instalável e homologado para o sistema operacional Microsoft Windows;
3.81. A solução deverá ser compatível com os seguintes protocolos:
   a. SNMPvl;
   b. SNMPv2;
   c. SNMPv3;
   d. WMI;
   e. SSH;
   f. Netflow
   g. jFlow
   h. Http
   i. sFlow
   j. ftp
3.82. Deverá ter intervalo mínimo de verificação de 30 (trinta) segundos para os sensores monitorados;
3.83. A solução deverá alertar sobre medições incomuns de sensores do ambiente, ou seja, deverá analisar padrões alertando quando houver um estado incomum no monitoramento;
3.84. Disponibilizar informações sobre interrupções ou inoperâncias por meio de cores e/ou formato de ícones, informando se os elementos estão ou não ativos, e se os paramentos estão ou não dentro dos limites preestabelecidos;
3.85. Deve permitir o monitoramento da performance com detecção de gargalos e outros problemas da rede, incluindo aqueles relacionados com carga de CPU, uso da memória, utilização de banda, status operacional de interface de rede, tempo de resposta dos dispositivos e eventos de erros;
3.86. Possuir um centro de mensagens único para todos os alertas de eventos em dispositivos e/ou serviços de maneira a permitir correlação desses eventos;
3.87. Permitir a configuração ou agendamento de descobrimento automático na rede;
3.88. Permitir a criação de relatórios de rede personalizados que possam ser exportados para pdf., impresso ou visualizado via HTTP;
3.89. Deve suportar IPV4 e IPV6;
3.90. Deve permitir interação na configuração do dispositivo através de SNMP v1, v2 e v3;
3.91. A solução de monitoramento deverá armazenar dados históricos armazenados

em seu banco de dados interno pelo período de 90 (noventa dias);

3.92. A solução deverá permitir a personalização de disparadores para sensores, tais como: intervalo de tempo de monitoramento, intervalo de tempo entre erros e alertas e quantidade de alertas consecutivos;

3.93. Deverá ser capaz de efetuar detecções automáticas no ambiente da **CONTRATANTE**;

3.94. A solução de monitoramento deverá ser capaz de entregar e-mails utilizando Relay autenticado;

3.95. Deverá ser possível o monitoramento de todas as portas das soluções (hardware) deste termo de referência, mostrando através de tabela de dados e gráficos sua disponibilidade e largura de banda com o intervalo mínimo de 30 (trinta) segundos;

3.96. A solução deverá monitorar características físicas das soluções (hardware) desta solução, tais como: temperatura do hardware, utilização de memória volátil, utilização de armazenamento, utilização e processamento e carga total do equipamento;

3.97. Deverá ter sensor com a informação de quantidade de tempo ligado dos equipamentos (hardwares) das soluções;

3.98. A solução de monitoramento deverá abrir chamado de maneira automática junto a **CONTRATANTE**, após a alteração de um sensor para o estado de alerta ou erro;

3.99. Deverá ser possível a geração de relatórios com dados de tabela e gráficos para quaisquer sensores que compõem a solução;

3.100. Deverá ser possível a criação de templates de relatórios de monitoramento;

3.101. A solução deverá conter sensor de "Sniffing de Pacotes" para monitoramento de tráfego incluindo: tráfego por porta e endereço IP, tráfego total, tráfego web (http/https), tráfego de e-mail (IMAP/POP/SMTP), tráfego de transferência de arquivos (FTP e P2P), tráfego de infraestrutura (DHCP, DNS, ICMP e SNMP) e tráfego de acesso remoto (RDP, SSH e VNC);

3.102. Deverá suportar monitoramento de tráfego sFlow e Netflow;

3.103. Deverá suportar monitoramento nativo incluindo: status, tráfego inbond e outbound para LAN e WLAN, eventos, atualizações, protocolos mais utilizados (Netflow) e conexões mais utilizadas (Netflow);

3.104. Deverá suportar o monitoramento da LAN, WAN e VPNs através de de SNMP, sFLOW, Netflow, Ping e Packet Sniffing;

3.105. Deverá suportar o monitoramento da rede WLAN incluindo: Tráfego, intensidade do sinal, status dos dispositivos e último acesso;

3.106. Deverá suportar o monitoramento dos seguintes Sistemas Operacionais: Microsoft Windows, Linux e MAC OS X

3.107. Deverá suportar o monitoramento das seguintes aplicações: Microsoft Active Directory, SQL Server, Hyper-V e VMWare

3.108. Deverá ser capaz de detectar automaticamente sobrecargas de largura de banda em equipamentos de rede gerenciáveis;

3.109. A solução deverá ser capaz de monitorar a qualidade de serviço da rede inciuindo: jitter, QoS, latência, perda de pacotes, e MOS (mean opinion score);

3.110. Deverá ser capaz de monitorar a latência de um dispositivo;

3.111. A solução deverá ser capaz de importar arquivos ".MIB", interpreta-los e integra-los ao sistema de monitoramento;

3.112. RELÁTORIOS

3.113. Deverá ser fornecido relatórios mensais de chamados e monitoramento de recursos dos componentes do serviço, com:

3.114. Relatório de Chamados (referente ao serviço descrito nesse lote):

3.115. Categoria do chamado;

3.116. Usuário;

3.117. Ativos relacionados;

3.118. Data de abertura e fechamento;

3.119. Status;

3.120. Relatório de Monitoramento de recursos (referente ao serviço descrito nesse lote):

3.121. Disponibilidade;

3.122. Consumo de hardware (CPU, memória, disco, consumo de banda);

3.123. Alertas e erros;

ITEM 4: SERVIÇO DE INSTALAÇÃO

4.1. Todo o processo de instalação das tecnologias deverá ser feito de forma presencial.

4.2. O Endereço de instalação será **Av. Getúlio Vargas, 1200 - Vila Nova Santana, Assis - SP, CEP: 19807-130.**

4.3. O serviço de instalação e configuração local deverá ser aplicado para todos os itens deste edital.

4.4. O serviço deverá contemplar a implementação de toda a solução, com prazo de 30 (trinta) dias após a entrega da ordem de compras;

4.5. **CONTRATADA** deverá instalar e configurar os itens físicos e lógicos seguindo os padrões, melhores práticas e especificações acordadas com a **CONTRATANTE**;

4.6. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, em observância às normas legais e regulamentares aplicáveis e às recomendações aceitas pela boa técnica;

4.7. Prestar todos os esclarecimentos que lhe forem solicitados pelo **CONTRATANTE**, atendendo prontamente a quaisquer reclamações;

4.8. Elaborar um plano de implantação com: Descrição de atividades a serem desenvolvidas; Relatórios e diagramas com dados relevantes para efeito decisório; responsáveis pelas atividades, e; cronograma da implantação. Compondo assim um documento denominado "Projeto Executivo" com visibilidade completa do projeto e seus respectivos informes de status;

4.9. Elaborar e apresentar de maneira antecipada um documento com o planejamento de implantação com informações técnicas relevantes para efeito decisório, para os responsáveis pelo projeto por parte da **CONTRATANTE**;

4.10. A **CONTRATADA** deverá apresentar em reunião a conclusão do projeto com a entrega do documento "Projeto Executivo" completo, contendo todas as informações da operação e visão estratégia;

4.11. As senhas configuradas pela **CONTRATADA** no ambiente durante a

instalação deverão ter requisito mínimo de 08 (oito) caracteres contendo letras maiúsculas, minúsculas e caracteres especiais;

4.12. O projeto deverá ser acompanhado por um gerente de projetos juntamente com a equipe técnica qualificada, onde a equipe precisa ser apresentada junto com o projeto executivo na primeira reunião organizacional.

4.13. A **CONTRATADA** se responsabiliza por todo o cabeamento, conectores, fibras, G BICS, DIO e todos os equipamentos que se fizerem necessários para compor o projeto e executar o serviço de instalação.

4.14. A equipe da **CONTRATADA** que executará o projeto deve possuir as ferramentas de segurança para se conectar no ambiente da **CONTRATANTE** com configurações mínimas como, solução de antivírus ativa, que deverá possuir solução criptografia, duplo fator de autenticação, Data Loss Prevention, identificação de acessos a arquivos confidenciais, detectar e interromper as violações regulatórias pré-determinadas pela **CONTRATANTE**, controle de arquivos acessados, visibilidade das ações do que foi feito e alterado caso seja necessário a auditoria pela**CONTRATANTE** para manter o nível de qualidade de segurança exigido na universidade.

5. JUSTIFICATIVAS PARA CONTRATAÇÃO

5.1. Da necessidade da contratação:

Diante do crescente volume de dados operacionalizados em sistema, da amplitude e diversidade do parque tecnológico da FEMA e da grande dependência do negócio, a disponibilidade e qualidade dos serviços de TIC faz-se importante e necessário para proteger as atividades da FEMA contra eventuais ameaças cibernéticas mediante monitoramento de ambiente tecnológico, além de resposta imediata a segurança da informação.

5.1.1. A FEMA necessita da contratação de serviços especializados em segurança para proteção de seus servidores e rede de dados com solução de antivírus e firewall de última geração.

5.1.2. A contratação se alinha aos objetivos citados na medida em que requerem cada vez mais ferramentas e soluções que proporcionem segurança, alta disponibilidade, eficiência, escalabilidade e ganho de desempenho na operacionalização de dados em sistemas com segurança contra eventuais ataques cibernéticos.

5.2. Da escolha da modalidade e tipo de licitação:

5.2.1. **Modalidade de Licitação**: A contratação será realizada por meio de Pregão Eletrônico, conforme os princípios da Lei 14.133/2021, que assegura a transparência, competitividade e economicidade do processo licitatório. A modalidade de Pregão Eletrônico é preferencial para a contratação de bens e serviços comuns, garantindo a

ampla participação de interessados e a transparência necessária para a administração pública.

5.3.2. Tipo de licitação: para julgamento e classificação das propostas, será adotado o critério de menor preço, em conformidade com a Lei 14.133/2021, art.33, I.

6. DA FORMA E LOCAL DE EXECUÇÃO DO SERVIÇO

6.1. A prestação dos serviços especializados em tecnologia da informação para renovação de garantia para ativos de tecnologia, realização de serviço de estruturação e realização de serviço especializado de segurança para a Fundação Educacional do Município de Assis deverão ser realizados na sede da instituição localizada na Avenida Getúlio Vargas, nº 1200, Vila Nova Santana, na cidade de Assis/SP.

6.2. O prazo para execução dos serviços, desde o planejamento até a migração final, é de 30 (trinta) dias corridos, a contar da data de assinatura do contrato e emissão da ordem de serviço.

6.3. Caso não seja possível a entrega no prazo mencionado, a empresa deverá comunicar as razões respectivas com pelo menos 5 (cinco) dias de antecedência para que qualquer tipo de prorrogação de prazo seja analisado, ressalvadas as situações de caso fortuito ou força maior.

7. DO RECEBIMENTO DOS SERVIÇOS

7.1. Os serviços serão recebidos nos termos do art. 140, inciso I da Lei Federal nº 14.133/2021:

a) provisoriamente, pelo responsável por seu acompanhamento e fiscalização, mediante termo detalhado, quando verificado o cumprimento das exigências decaráter técnico;

b) definitivamente, por servidor ou comissão designada pela autoridade competente, mediante tremo detalhado que comprove o atendimento das exigências contratuais.

7.2. O objeto poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o contrato.

7.3. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança da obra ou serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato, nos limites estabelecidos pela lei ou pelo contrato.

7.4. Os prazos e dos métodos para realização dos recebimentos provisórios e definitivos serão definidos em contrato.

8. PRAZO DA VIGÊNCIA CONTRATUAL

8.1. O prazo de vigência contratual será de 12 (doze) meses, contados a partir da assinatura do contrato, podendo ser prorrogado na forma e condições estabelecidas na Lei nº 14.133/2021.

8.2. Caso venha a ser prorrogado os valores poderão ser corrigidos pelo Índice Nacional de Preços ao Consumidos Amplo – IPCA.

9. DO PREÇO ESTIMADO

9.1. O valor unitário e total estimado para os serviços de Contratação de empresa especializada na prestação de Serviços Gerenciados de Tecnologia da Informação e Segurança da Informação pela Fundação Educacional do Município de Assis, visando a renovação de garantia para ativos de tecnologia, serviços de estruturação e serviços especializados de segurança é demonstrado na tabela a seguir:

LOTE - SERVIÇOS GERENCIADOS DE TECNOLOGIA DA INFORMAÇÃO				
ITEM	**DESCRIÇÃO**	**VALOR UNITÁRIO**	**QTD.**	**VALOR TOTAL**
1	SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO	R$ 10.080,00	12	R$ 120.960,00
2	SERVIÇO DE PROTEÇÃO PARA ESTAÇÕES DE TRABALHO	R$ 7.840,00	12	R$ 94.080,00
3	SERVIÇO DE SUPORTE TÉCNICO E MONITORAMENTODE REDES E WI-FI	R$ 8.180,00	12	R$ 98.160,00
4	SERVIÇO DE INSTALAÇÃO	R$ 63.600,00	1	R$ 63.600,00

9.2. Este valor foi determinado com base em uma pesquisa de mercado que considerou orçamentos recebidos de potenciais fornecedores.

9.3 Justificativa do Preço:

9.3.1. A justificativa para o preço estabelecido baseia-se na necessidade de garantir a eficiência, economicidade e isonomia nas contratações públicas, conforme preconizado pela Lei 14.133/2021. A pesquisa de mercado é um instrumento fundamental para assegurar que os valores obtidos são compatíveis com o praticado no mercado correspondente, evitando superfaturamento ou preços inexequíveis. A estimativa de custo foi realizada considerando a média dos preços obtidos por meio de orçamentos recebidos de potenciais fornecedores que enviaram preços semelhantes para os serviços. Assim, vislumbra-se que os preços obtidos são compatíveis com os praticados nesse tipo de trabalho.

9.3.2. Os fornecedores selecionados para a coleta de orçamento são empresas especializadas no serviço a ser contratado, com plena capacidade de fornecer as licenças e os serviços de maneira adequada e dentro dos prazos estabelecidos em contrato e no edital. Além disso, é fundamental que as licenças sejam originais e compatíveis com os computadores da instituição, garantindo a segurança da rede interna da faculdade e evitando quaisquer riscos associados. Ademais, a pesquisa de preço foi feita com base em orçamentos de empresas especializadas e reconhecidas por prestarem esse tipo de serviço com maestria.

10. CRITÉRIOS DE AVALIAÇÃO

10.1. Os serviços serão avaliados com base na qualidade técnica das soluções propostas, no cumprimento dos prazos estabelecidos e na conformidade com as especificações do CEPEIN.

11. CONTROLE E FISCALIZAÇÃO

11.1. A fiscalização do contrato seguirá os padrões estabelecidos no artigo 117 da Lei nº 14.133/2021, garantindo o cumprimento de todas as especificações técnicas e normas regulatórias aplicáveis.

12. REQUISITOS DE HABILITAÇÃO

O fornecedor será selecionado por meio da realização de procedimento de licitação, na modalidade Pregão, sob a forma eletrônica, com adoção do critério de julgamento

de menor preço.

12.1. Para fins de habilitação, deverá a licitante comprovar os requisitos:

12.2. Habilitação Jurídica:

12.2.1. Registro comercial, no caso de empresa individual;

12.2.2. Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores;

12.2.2.1. O objeto social do licitante deverá ser compatível como serviço a ser licitado, caso o objeto social do licitante seja incompatível com o serviço a ser licitado, este será considerado inabilitado para a execução dos serviços;

12.2.3. Inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova de diretoria em exercício;

12.2.4. Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

12.2.5. Declaração, em cumprimento da Lei 9.854/99, de que não emprega mão-de-obra de menores. Ou, empregando-a, cumpre disposição expressada no inciso I do § 3º do artigo 227 combinada com a norma estatuída no inciso XXXIII do artigo 7º, tudo da Constituição Federal.

12.3. Da Regularidade Fiscal e Trabalhista:

12.3.1. Prova no Cadastro Nacional de Pessoa Jurídica (CNPJ);

12.3.2. Prova de regularidade para com a Fazenda Federal, mediante apresentação de Certidão Conjunta de Débitos Relativos a Tributos Federais e à Dívida Ativa da União, emitida pela Secretaria da Receita Federal do Brasil ou pela Procuradoria-Geral da Fazenda Nacional;

12.3.3. Prova de regularidade para com a Fazenda Estadual do domicílio ou sede do licitante, mediante apresentação de certidão emitida pela Secretaria competente do Estado;

12.3.4. Prova de regularidade para com a Fazenda Municipal do domicílio ou sede do licitante mediante apresentação de certidão emitida pela Secretaria competente do Município;

12.3.5. Prova de regularidade relativa ao Fundo de Garantia por Tempo de Serviço - FGTS, emitida pela Caixa Econômica Federal, demonstrando situação regular no cumprimento dos encargos sociais instituídos por Lei;

12.3.6. Certidão Negativa de Débitos Trabalhistas – CNDT, emitida em todos os portais da Justiça do Trabalho na rede mundial de computadores (Tribunal Superior do Trabalho, Conselho Superior da Justiça do Trabalho e Tribunais Regionais do Trabalho).

12.4. Qualificação Econômico-Financeira:

12.4.1. Certidão negativa de falência ou concordata expedida pelo cartório distribuidor da sede da pessoa jurídica, no máximo, 60 (sessenta) dias antes da data fixada para entrega das propostas:

12.4.1.1. As licitantes em recuperação judicial deverão apresentar comprovação de que o plano de recuperação foi acolhido na esfera judicial, na forma do art. 58 e do art. 162 da Lei n. 11.101/2005.

12.4.2. Os documentos que não tragam em seu bojo a data de validade serão considerados válidos pelo prazo de 180 (cento e oitenta) dias;

12.4.3. Serão admitidas fotocópias sem autenticação cartorial dos documentos exigidos neste edital, desde que os respectivos originais sejam apresentados na reunião de abertura dos envelopes "documentação";

12.4.4. Os documentos mencionados acima não poderão ser substituídos por qualquer tipo de protocolo.

12.5. Qualificação Técnica

12.5.1. Atestado(s) de capacidade técnica emitido(s) por pessoa jurídica de direito público ou privado, em papel timbrado, comprovando que a licitante prestou serviços similares ao objeto licitado de mínimo 30% do valor estimado da contratação, indicando o endereço do contratado, de forma a permitir possível diligência para esclarecimentos;

12.5.1.1. O(s) atestado(s) apresentado(s) deverá(ão) conter, obrigatoriamente, a especificação dos serviços executados/produto fornecido, o nome e cargo do declarante.

12.5.1.2. A FEMA se resguarda no direito de diligenciar junto à emitente do

Atestado/Declaração de Capacidade Técnica, visando obter informações sobre o serviço prestado e cópias dos respectivos contratos e/ou outros documentos comprobatórios do conteúdo declarado.

12.5.1.3. Não será aceito atestado/declaração emitido pela própria licitante, sob pena de infringência ao princípio da moralidade, posto que a licitante não possui a impessoalidade necessária para atestar sua própria capacitação técnica.

12.5.1.4. O(s) atestado(s) deve(m) estar em papel timbrado, com a devida identificação e assinatura do responsável, devendo possuir ainda os contatos do emissor.

12.5.1.5. Será admitida a somatória dos atestados para comprovação do valor mínimo exigido.

12.5.1.6. É vedada a participação de empresas em regime de consórcio, qualquer seja a forma de constituição.

13. CRITÉRIOS DE SUSTENTABILIDADE

13.1. Para atender às necessidades de contratação de serviços especializados nas dependências do CEPEIN, é essencial incorporar critérios de sustentabilidade que minimizem os impactos ambientais e promovam práticas responsáveis. A Lei nº 14.133/21, em seus diversos artigos, fornece a base legal para a inclusão desses critérios nas licitações e contratos públicos.

14. FORMA DE PAGAMENTO

14.1. O pagamento será efetuado no prazo de até 15 (quinze) dias úteis após o recebimento definitivo do produto e apresentação do respectivo documento fiscal.

14.2. As notas fiscais/faturas que apresentarem incorreções serão devolvidas à Contratada e seu vencimento ocorrerá em 05 (cinco) dias corridos após a data de sua apresentação válida;

14.3. O pagamento será feito por meio de sistema bancário.

14.4. Não será admitida proposta com condição de pagamento diferente da definida nesta cláusula.

14.5. Nenhum pagamento será efetuado ao licitante vencedor enquanto pendente de

liquidação ou qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência.

14.6. Os valores ofertados pela CONTRATADA em sua proposta comercial já consideraram todos os encargos incidentes sobre o objeto do Contrato, não sendo aceita reivindicação posterior para sua inclusão nesses valores, salvo se houver comprovação de que são novos e criados por ato de governo.

14.7. A CONTRATANTE se reserva o direito de suspender o pagamento se o serviço for prestado em desacordo com as especificações constantes deste Contrato, ou se houver qualquer erro ou irregularidade em relação a dados constantes da fatura/nota fiscal apresentada, o que não acarretará para a CONTRATANTE a responsabilidade por quaisquer ônus decorrentes desse não pagamento, como multas e correções. O pagamento somente será efetuado se a CONTRATANTE atestar a execução satisfatória do serviço.

14.8. O pagamento efetuado não implica reconhecimento pela CONTRATANTE de adimplemento por parte da CONTRATADA relativamente às obrigações previdenciárias, sociais, trabalhistas, tributárias e fiscais, nem novação em relação a qualquer regra constante destas especificações.

15. DAS OBRIGAÇÕES DA CONTRATADA

15.1 A empresa contratada será responsável por seguir as diretrizes estabelecidas no edital de licitação e no contrato, conforme Art. 144, Parágrafo 1 da Lei 14.133/21, garantindo o fiel cumprimento das obrigações assumidas perante a Administração, incluindo as multas, os prejuízos e as indenizações decorrentes de inadimplemento, conforme estipula o Art. 97, § 1º da mesma lei.

15.2. Constituem obrigações da CONTRATADA, além do fiel cumprimento de todas as disposições contidas deste contrato, edital e anexos:

15.2.1. Ser a única responsável pelos serviços desenvolvidos na FEMA.

15.2.2. Acatar prontamente as exigências e observações da fiscalização baseadas nas especificações, regras de boa técnica e normas em vigor.

15.2.3. Ser a única responsável pela segurança de trabalho de seus funcionários, técnicos e de terceiros na execução do objeto deste contrato.

15.2.4. A empresa deverá prestar suporte técnico durante a vigência do contrato.

15.3. Cabe ainda à contratada responder por:

15.3.1. Todos os encargos previdenciários e obrigações sociais previstos na legislação social e trabalhista em vigor, obrigando-se a saldá-los na época própria, vez que os seus empregados não manterão nenhum vínculo empregatício com o CONTRATANTE;

15.3.2. Todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie forem vítimas os seus empregados durante a execução deste contrato, ainda que acontecido em dependência do CONTRATANTE;

15.3.3. Todos os encargos de possível demanda trabalhista, civil ou penal, relacionada à execução deste contrato, originariamente ou vinculada por prevenção, conexão ou continência;

15.3.4. Encargos fiscais e comerciais resultantes desta contratação.

15.3.5. A inadimplência da CONTRATADA, com referência aos encargos estabelecidos no item anterior, não transfere a responsabilidade por seu pagamento à Administração do CONTRATANTE, nem pode onerar o objeto deste contrato, razão pela qual a CONTRATADA renuncia expressamente a qualquer vínculo de solidariedade, ativa ou passiva, com o CONTRATANTE.

16. DAS OBRIGAÇÕES DA CONTRATANTE

16.1. A Administração deverá adaptar o ambiente para receber os serviços de capacitar servidores para a gestão e fiscalização do contrato, conforme orientação do Art. 18, § 1º, inciso X da Lei 14.133/21.

16.2. Pagar à CONTRATADA o valor devido, nas datas avençadas;

16.3. Acompanhar e fiscalizar o cumprimento da execução dos serviços;

16.4. Solicitar o ajuste ou a correção de qualquer falha, defeito ou incorreção nos observada nos serviços;

16.5. Prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos da CONTRATADA.

17. DAS SANÇÕES APLICÁVEIS

17.1. São previstas sanções administrativas para o inadimplemento contratual,

incluindo multas e indenizações, conforme detalhado nos Arts. 97 a 99 da Lei 14.133/21.

18. DA RESCISÃO CONTRATUAL

18.1. As condições para rescisão contratual estarão em conformidade com o estabelecido na Lei 14.133/21, assegurando a proteção dos interesses da Administração Pública e a observância dos princípios legais.

19. DAS DISPOSIÇÕES FINAIS

19.1. Este termo de referência foi elaborado a partir do Documento de Formalização de Demanda encaminhado pelo CEPEIN, considerando a demanda apresentada pela coordenação, bem como, as informações contidas no Estudo Técnico Preliminar elaborado em conjunto.

19.2. A contratada será responsável pela confidencialidade das informações do órgão público a que tiver acesso durante a prestação dos serviços.

19.3. É vedada a subcontratação total ou parcial do objeto desta contratação.

Assis, 30 de outubro de 2024

Luiz Ricardo Begosso
Coordenador do CEPEIN

Nivaldo Aparecido de Melo
Coordenador Administrativo

Eduardo Aparecido de Souza
Chefe de Seção

Juliana Santos De Nigris Batista
Chefe de Seção

Isadora Pelizone de Lima Cintra
Assistente Administrativo

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: 0D1B-26C4-EC81-B45B

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:

- LUIZ RICARDO BEGOSSO (CPF 078.XXX.XXX-23) em 30/10/2024 16:28:55 (GMT-03:00)
  Papel: Parte
  Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

- EDUARDO APARECIDO DE SOUZA (CPF 138.XXX.XXX-37) em 30/10/2024 16:56:42 (GMT-03:00)
  Papel: Parte
  Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

- ISADORA PELIZONE DE LIMA CINTRA (CPF 442.XXX.XXX-78) em 31/10/2024 08:14:45 (GMT-03:00)
  Papel: Parte
  Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

- NIVALDO APARECIDO DE MELO (CPF 061.XXX.XXX-86) em 31/10/2024 14:56:36 (GMT-03:00)
  Papel: Parte
  Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

- JULIANA DE NIGRIS (CPF 384.XXX.XXX-04) em 31/10/2024 16:54:13 (GMT-03:00)
  Papel: Parte
  Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

Para verificar a validade das assinaturas, acesse a Central de Verificação por meio do link:

https://fema.1doc.com.br/verificacao/0D1B-26C4-EC81-B45B