



TERMO DE REFERÊNCIA

SIGILO: () SIM (X) NÃO

PREVISÃO NO PLANO DE CONTRATAÇÃO ANUAL: (X) SIM () NÃO

1. ÁREA DEMANDANTE

Secretaria Demandante: Secretaria de Administração e Modernização

Secretária: Elizabete Cilião Guilherme.

Email (institucional): sinopcompras@gmail.com

Telefone (Institucional): (66) 3520-7298

2. OBJETO

2.1. O presente Termo de Referência tem por objeto o **Registro de Preços para futura e eventual contratação de empresa especializada para prestação de serviços de segurança da informação**, compreendendo o fornecimento e a disponibilização de equipamentos, appliances, licenças, subscrições, softwares, plataformas, componentes, acessórios e demais recursos necessários, bem como a implantação, instalação, configuração, integração, parametrização, testes, ativação, suporte técnico, manutenção, atualização tecnológica, gerenciamento, monitoramento e demais serviços necessários ao pleno e adequado funcionamento da solução, destinada à proteção da infraestrutura de tecnologia da informação do Município de Sinop-MT, conforme condições, quantidades, especificações e exigências estabelecidas neste Termo de Referência, no respectivo Estudo Técnico Preliminar e demais documentos que integram a contratação.

2.1.1. A contratação compreende **11 (onze) itens**, integrantes de uma solução corporativa e integrada de segurança da informação, abrangendo, conforme as especificações técnicas estabelecidas neste Termo de Referência, mecanismos de proteção perimetral de rede, gerenciamento de recursos de segurança, monitoramento e análise de eventos, proteção de estações de trabalho e servidores, segurança de aplicações em ambiente web, conectividade sem fio corporativa, avaliação de vulnerabilidades, conscientização em segurança da informação e



suporte técnico especializado. A relação detalhada dos itens, respectivas unidades de medida, quantitativos e especificações consta da tabela de composição do objeto.

2.1.2. A solução será executada em **lote único**, cabendo a uma única contratada o fornecimento e a execução dos 11 (onze) itens registrados, observadas as demandas efetivamente formalizadas pela Administração durante a vigência da Ata de Registro de Preços. A contratada será responsável por assegurar, quando aplicável, a compatibilidade, interoperabilidade, integração e pleno funcionamento dos componentes efetivamente demandados, inclusive quando houver dependência técnica entre diferentes recursos da solução.

2.1.3. A contratação não se limita à entrega física de equipamentos, licenças ou componentes. Para cada demanda formalizada pela Administração, caberá à contratada adotar todas as providências necessárias para que a solução solicitada seja entregue, instalada, configurada, integrada, parametrizada, testada, ativada e disponibilizada em pleno e desimpedido funcionamento, observadas as especificações, funcionalidades, níveis de desempenho e demais requisitos estabelecidos neste Termo de Referência.

2.1.4. Caberá integralmente à contratada disponibilizar todos os equipamentos, licenças, subscrições, softwares, acessórios, componentes, módulos, cabos, fontes, suportes, cases, antenas e demais recursos materiais ou tecnológicos necessários à instalação, operacionalização e pleno funcionamento da solução, ainda que determinados componentes acessórios não estejam individualmente discriminados nos quantitativos, desde que sejam indispensáveis à execução do objeto e estejam abrangidos pelas especificações e obrigações estabelecidas neste Termo de Referência.

2.1.5. A disponibilização dos equipamentos e demais componentes necessários à prestação dos serviços não implica sua aquisição ou incorporação ao patrimônio do Município, permanecendo a propriedade desses recursos com a contratada quando assim previsto na solução e durante o período de sua utilização, cabendo à contratada sua manutenção, substituição, atualização e demais providências necessárias ao funcionamento dos serviços, ressalvadas as hipóteses expressamente estabelecidas neste Termo de Referência.

2.1.5.1. Nenhum dos 11 (onze) itens prevê aquisição definitiva ou incorporação patrimonial pela Prefeitura.

2.1.6. Os equipamentos, appliances, licenças, subscrições, softwares, plataformas, módulos, acessórios, componentes, cabos, fontes, suportes, racks, cases, antenas e



demaís recursos disponibilizados pela CONTRATADA para a execução dos serviços constituem meios necessários à prestação da solução contratada, permanecendo sob sua responsabilidade e propriedade durante toda a execução, não implicando transferência de propriedade ou incorporação ao patrimônio do Município de Sinop-MT, independentemente do período de disponibilização ou utilização.

2.1.6.1. Ao término da vigência da contratação ou da prestação do serviço correspondente, os equipamentos e demais recursos de propriedade da CONTRATADA deverão ser retirados ou recolhidos, quando aplicável, observadas as condições de encerramento, transição e continuidade dos serviços estabelecidas neste Termo de Referência.

2.1.6.2. A disponibilização dos equipamentos e demais recursos necessários à execução dos serviços não caracteriza aquisição, doação, incorporação patrimonial ou transferência de propriedade à Administração, constituindo obrigação acessória e indispensável à adequada prestação dos serviços contratados.

ITENS	NATUREZA	MEDIÇÃO	RECURSOS FÍSICOS/TECNOLÓGICOS	PROPRIEDADE
1 a 10	Serviço especializado	Mensal	Disponibilizados pela contratada quando necessários	Contratada
11	Serviço Técnico Especializado	Hora/UST	Conforme necessidade da execução	Contratada/Sem transferência patrimonial

2.1.7. A Secretaria Municipal de Administração e Modernização será responsável pela gestão centralizada da contratação e consolidação das demandas das Secretarias e demais unidades administrativas integrantes do Poder Executivo Municipal, contando com o acompanhamento técnico do Centro de Processamento de Dados - CPD. A centralização da gestão não caracteriza atendimento exclusivo à Secretaria de Administração, uma vez que a solução será destinada à proteção da infraestrutura tecnológica corporativa utilizada pelas diferentes unidades administrativas do Município.

2.1.8. A efetiva contratação dos itens registrados ocorrerá de forma parcelada e conforme a necessidade da Administração, mediante a formalização da respectiva demanda e a observância dos procedimentos administrativos aplicáveis, não constituindo o quantitativo registrado garantia de contratação integral pela Administração.



2.1.9. Centralização da Demanda: A presente contratação será conduzida de forma centralizada pela Secretaria Municipal de Administração e Modernização, unidade responsável pela gestão da infraestrutura tecnológica do Município de Sinop-MT.

Embora a contratação seja formalizada por uma única unidade administrativa, a solução atenderá de forma integrada às necessidades das diversas Secretarias Municipais, considerando que a infraestrutura tecnológica utilizada pelas diversas Secretarias Municipais é administrada de maneira centralizada, permitindo maior padronização, eficiência operacional, simplificação da gestão contratual e fortalecimento da segurança da informação em todo o ambiente computacional do Município.

2.1.10. Definição dos Quantitativos: Os quantitativos previstos para a presente contratação foram definidos pela Secretaria Municipal de Administração e Modernização mediante análise das necessidades da Administração Pública Municipal, considerando o histórico de consumo, as contratações anteriores, a evolução da infraestrutura tecnológica municipal, as previsões constantes do Plano de Contratações Anual (PCA), as demandas formalizadas pela unidade responsável e a expectativa de crescimento da infraestrutura tecnológica durante a vigência da futura contratação.

A metodologia adotada buscou assegurar compatibilidade entre a necessidade administrativa, a disponibilidade orçamentária e a utilização racional dos recursos públicos, evitando superdimensionamentos ou quantitativos insuficientes para atendimento das demandas institucionais.

Ressalta-se que os quantitativos dos Itens 2 e 7 possuem metodologia específica de dimensionamento, em razão da forma individualizada de utilização dos respectivos serviços. Nesses itens, o quantitativo estimado considera a possibilidade de atendimento de até 15 (quinze) pontos durante o período de 12 (doze) meses, resultando no quantitativo de 180 (cento e oitenta) unidade-mês por item. A metodologia de cálculo e a forma de utilização desses quantitativos serão detalhadas em tópico específico deste Estudo Técnico Preliminar.

2.1.11. Forma de Contratação: Considerando que a demanda poderá ocorrer de forma parcelada durante a vigência da contratação, optou-se pela utilização do Sistema de Registro de Preços, possibilitando que os serviços e eventuais fornecimentos acessórios sejam demandados conforme a necessidade da Administração.



Tal sistemática proporciona maior eficiência na gestão dos recursos públicos, evita aquisições antecipadas ou em quantitativos superiores aos efetivamente necessários, confere maior flexibilidade à Administração e assegura melhor aproveitamento dos recursos orçamentários, observadas as condições estabelecidas na futura Ata de Registro de Preços.

2.1.12. Relação dos itens: Os objetos que compõem a presente contratação estão relacionados na tabela a seguir (item 2.2.), contendo as respectivas descrições, unidades de medida e quantitativos estimados.

2.1.13. Público Beneficiado pela Contratação: A solução será utilizada pelas Secretarias Municipais e seus respectivos departamentos, beneficiando diretamente os servidores responsáveis pela utilização da infraestrutura tecnológica do Município. Indiretamente, a contratação contribuirá para a continuidade, segurança e confiabilidade dos serviços públicos prestados à população, mediante a proteção dos sistemas e das informações institucionais.

2.1.14. O Tribunal de Contas do Estado de Mato Grosso (TCE-MT) desenvolveu o Catálogo de Materiais e Serviços, ferramenta eletrônica que padroniza as especificações de itens licitáveis e é de uso obrigatório por todos os órgãos sob sua jurisdição. Desde 2017, o Município de Sinop utiliza o catálogo em seus processos licitatórios, seguindo as diretrizes do TCE-MT e fortalecendo as boas práticas de governança pública. A padronização das descrições promove transparência, ampla concorrência e segurança técnica, evitando direcionamentos e inconsistências nas especificações. Além disso, o catálogo funciona como um banco de dados de preços, permitindo melhor planejamento e controle das contratações.

2.2. Descrição e quantidades:

Nº	ITEM	COD. TCE.	DESCRIÇÃO E ESPECIFICAÇÃO	UND. FORN.	QUANT.	VALOR UNITÁRIO	TOTAL (R\$)
1	4079 59	4049 19-5	Serviços especializados de segurança da informação com solução de NGFW/SD-Wan em cluster (alta disponibilidade) fornecidos em appliance Tipo 1. FortiGate 200G + Licença UTP	MÊS	12	R\$ 36.177,00	R\$ 434.124,00
2	4077 10	4049 19-5	Serviços especializados de segurança da informação com solução de NGFW/SD-WAN fornecidos em appliance Tipo 2. FortiGate 30G + Licença UTP	MÊS	12	R\$ 17.270,45	R\$ 207.245,40
3	4079 60	4049 19-5	Serviços especializados de segurança da informação com	MÊS	12	R\$ 20.228,98	R\$ 242.747,76



			solução da base de dados analíticos e logs fornecidos em appliance. FortiAnalyzer FAZ-300G				
4	4079 61	4049 19-5	Serviços especializados de segurança da informação com solução de gerenciamento de NGFW fornecidos em appliance. FortiManager FMG-200G	MÊS	12	R\$ 18.460,92	R\$ 221.531,04
5	4079 62	4049 19-5	Serviços especializados de segurança da informação com solução de endpoint corporativo do tipo EDR. FortiEDR Discover, Protect ERespond Cloud	MÊS	12	R\$ 72.870,00	R\$ 874.440,00
6	4079 63	4272 17-0	Serviços especializados de segurança da informação com solução de WAF. FortiWeb 100F	MÊS	12	R\$ 27.404,75	R\$ 328.857,00
7	4077 11	4049 19-5	Serviços especializados de segurança da informação com solução de Access Point corporativo. FortiAP 231-K	MÊS	12	R\$ 9.843,85	R\$ 118.126,20
8	4079 64	4272 17-0	Serviços especializados de segurança da informação com solução de Captive Portal. Wifeed	MÊS	12	R\$ 5.457,78	R\$ 65.493,36
9	4079 66	4272 17-0	Serviços especializados de segurança da informação com plataforma de conscientização e campanhas de phishing. Beephish	MÊS	12	R\$ 32.516,49	R\$ 390.197,88
10	4079 67	4132 46-7	Serviços especializados de segurança da informação para mapeamento de vulnerabilidades. Nessus Tenable	MÊS	12	R\$ 814,5	R\$ 9.774,00
11	4079 68	4132 46-7	Unidade de serviço técnico -UST	HORA	300	R\$ 918,77	R\$ 275.631,00
VALOR TOTAL (R\$)				R\$ 3.168.167,64			

2.2.1. DA FORMA DE QUANTIFICAÇÃO E COBRANÇA DOS SERVIÇOS:

2.2.1.1. Para os itens 2 (dois) e 7 (sete): cuja precificação está estabelecida por mensalidade correspondente à disponibilização de solução para até **15 (quinze) unidades**, o quantitativo registrado deverá ser interpretado como referência de capacidade de atendimento ao longo da vigência da contratação, não representando a contratação ou faturamento individual de cada unidade disponibilizada.

2.2.1.2. A mensalidade estabelecida para esses itens será devida pelo período de prestação do serviço, independentemente da quantidade efetivamente utilizada em cada mês, desde que esta permaneça dentro do limite de até 15 (quinze) unidades simultaneamente, não havendo redução ou acréscimo do valor mensal em razão da utilização de quantidade inferior ou igual ao limite contratado.

Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



2.2.1.3. O quantitativo de 180 (cento e oitenta) unidade-mês, quando utilizado na composição do planejamento da contratação (Estudo Técnico Preliminar - ETP), corresponde exclusivamente à projeção de 15 (quinze) unidades × 12 (doze) meses, não significando vigência contratual de 180 (cento e oitenta) meses.

2.2.1.4. Para fins de apresentação dos preços e estimativa do valor da contratação, a mensalidade será considerada para o período de 12 (doze) meses, observando-se o valor mensal estabelecido para a capacidade de até 15 (quinze) unidades.

Item	Descrição Resumida	QTD.	Unidade	Valor Unitário	Valor total estimado
2	Serviço mensal para até 15 rádios/unidades Capacidade: até 15 unidades simultâneas. Regra de cobrança: o valor mensal corresponde à disponibilização da solução para até 15 unidades, não sendo alterado pela utilização de quantidade inferior ao limite contratado.	12	MÊS	R\$ 17.270,45	R\$ 207.245,40
7	Serviço mensal para até 15 rádios/unidades Capacidade: até 15 unidades simultâneas. Regra de cobrança: o valor mensal corresponde à disponibilização da solução para até 15 unidades, não sendo alterado pela utilização de quantidade inferior ao limite contratado.	12	MÊS	R\$ 9.843,85	R\$ 118.126,20

2.2.2. Justificativa e forma de quantificação dos Itens 2 e 7: Os quantitativos dos itens 2 e 7 foram estabelecidos considerando a necessidade de disponibilização de serviços para até 15 (quinze) unidades/pontos simultaneamente, durante o período estimado de 12 (doze) meses de execução, conforme a necessidade da Administração.

Para fins de planejamento e registro do quantitativo, considera-se a unidade de medida unidade-mês, resultando no quantitativo de 180 (cento e oitenta) unidade-



mês, obtido pela seguinte memória de cálculo: **15 (quinze) unidades/pontos × 12 (doze) meses = 180 unidade-mês.**

O quantitativo de 180 unidade-mês não representa a contratação de um único equipamento ou ponto pelo período de 180 meses, tampouco implica prazo de execução ou vigência contratual dessa duração. Trata-se exclusivamente da soma estimada das unidades/pontos que poderão ser disponibilizados ao longo de 12 (doze) meses.

Para os itens 2 e 7, o valor estabelecido corresponde à mensalidade da solução para atendimento de até 15 (quinze) unidades/pontos, de modo que a utilização de quantidade inferior ou igual a esse limite, em determinado mês, não implicará redução ou alteração do valor mensal contratado.

Assim, a Administração poderá demandar, conforme sua necessidade, quantidade variável de unidades/pontos ao longo da execução, respeitado o limite de até 15 (quinze) unidades/pontos simultaneamente, sem que isso implique obrigação de utilização integral do quantitativo estimado.

A título exemplificativo, caso sejam disponibilizadas 5 (cinco) unidades em determinado mês, a mensalidade permanecerá correspondente à solução contratada para até 15 (quinze) unidades. Da mesma forma, caso sejam disponibilizadas 15 (quinze) unidades, será aplicado o mesmo valor mensal. O limite de 15 unidades representa, portanto, a capacidade máxima contemplada pela mensalidade, e não uma quantidade individualmente faturada.

Dessa forma, o quantitativo de 180 unidade-mês deve ser compreendido como o limite quantitativo estimado para o período de 12 (doze) meses, correspondente à capacidade de atendimento de até 15 (quinze) unidades/pontos por mês, podendo sua utilização ocorrer de forma parcelada e variável, conforme a efetiva necessidade da Administração.

Item	Solução	Capacidade máxima	Período estimado	Cálculo do quantitativo	Quantitativo registrado	Unidade de cobrança	Valor mensal
2	NGFW/SD-WAN – Appliance Tipo 2	Até 15 pontos	12 meses	15 × 12	180	unidade-mês	R\$ 17.270,45
7	Access Point Corporativo	Até 15 pontos	12 meses	15 × 12	180	unidade-mês	R\$ 9.843,85

Nota: O valor mensal indicado corresponde à solução para atendimento de até 15 pontos/unidades, não sendo multiplicado individualmente pela quantidade de



unidades-mês registrada. Para fins de estimativa financeira, considera-se o valor mensal $\times 12$ meses.

2.2.3. Da indicação de marcas e da possibilidade de soluções equivalentes: as marcas, fabricantes, modelos, plataformas e soluções tecnológicas eventualmente indicados na descrição dos itens constituem **referências técnicas**, utilizadas para estabelecer as características, funcionalidades, desempenho e padrão tecnológico pretendidos pela Administração.

2.2.3.1. A indicação de referência tecnológica não caracteriza exclusividade de fabricante ou marca, sendo admitida a apresentação de solução de outro fabricante, modelo, plataforma ou composição tecnológica, desde que atendidos integralmente os requisitos estabelecidos no Edital e neste Termo de Referência.

2.2.3.2. A solução apresentada em condição diversa da referência deverá comprovar sua equivalência técnica, especialmente quanto a:

- compatibilidade;
- interoperabilidade;
- desempenho;
- funcionalidades;
- integração com a infraestrutura existente;
- requisitos de segurança; e
- demais características técnicas exigidas no instrumento convocatório.

2.2.3.3. Caberá à licitante apresentar, quando solicitado, os elementos necessários à comprovação da equivalência técnica, podendo ser exigidos:

- catálogos e fichas técnicas;
- documentação oficial do fabricante;
- declarações do fabricante;
- certificações;
- demonstrações da solução;
- esclarecimentos técnicos;
- documentação de compatibilidade;
- realização de testes; e
- outros elementos tecnicamente pertinentes.

2.2.3.4. A análise técnica das soluções ofertadas será realizada pela Administração, mediante encaminhamento pelo Pregoeiro à unidade responsável pela análise técnica, com apoio do Centro de Processamento de Dados - CPD, quando necessário.



2.2.3.5. A Administração poderá realizar ou solicitar testes, demonstrações ou avaliações técnicas da solução ofertada, quando necessários, para verificar o atendimento aos requisitos estabelecidos neste Termo de Referência.

2.2.3.6. Quando tecnicamente necessário, poderá ser realizada visita técnica à estrutura da Administração, com a finalidade de avaliar aspectos relacionados à compatibilidade, interoperabilidade e integração da solução ofertada com a infraestrutura tecnológica existente.

2.2.3.7. A aceitação de solução diversa da referência estará condicionada à comprovação objetiva de atendimento integral aos requisitos técnicos, não podendo a alteração de fabricante, modelo ou plataforma comprometer a funcionalidade, o desempenho, a segurança, a interoperabilidade ou a continuidade da infraestrutura tecnológica municipal.

2.2.4. DAS INFORMAÇÕES TÉCNICAS REFERENCIAIS PARA ELABORAÇÃO DA PROPOSTA

2.2.4.1. As informações constantes deste item têm caráter técnico-referencial e orientativo, destinando-se a fornecer às empresas interessadas elementos adicionais acerca do ambiente tecnológico, das características e das funcionalidades que foram consideradas na estruturação de contratação anterior e que poderão servir como referência para a elaboração das propostas.

2.2.4.2. As informações apresentadas foram utilizadas e discutidas no âmbito do planejamento de contratação anterior, inclusive com participação do setor técnico responsável pela infraestrutura de tecnologia da informação do Município, constituindo-se em referência histórica das necessidades e características técnicas então identificadas.

2.2.4.3. Considerando o lapso temporal entre a contratação anterior e o presente processo, bem como a possibilidade de alterações na infraestrutura tecnológica, nas soluções disponíveis no mercado, nas versões de software, nos equipamentos utilizados, nos modelos de licenciamento e nas necessidades operacionais da Administração, as informações deste item não deverão ser interpretadas como requisitos técnicos obrigatórios, taxativos ou imutáveis da presente contratação, salvo quando expressamente incorporadas às especificações técnicas dos respectivos itens deste Termo de Referência.

2.2.4.4. As empresas interessadas poderão utilizar as informações deste item como norte técnico para compreensão do ambiente e das necessidades da CONTRATANTE, devendo, contudo, elaborar suas propostas com base nas
Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



especificações, quantitativos, condições e requisitos expressamente estabelecidos neste Termo de Referência e em seus anexos.

2.2.4.5. Eventuais diferenças entre as informações técnicas referenciais aqui apresentadas e a realidade tecnológica existente no momento da execução contratual não implicarão, por si só, descumprimento contratual, desde que a solução ofertada atenda integralmente aos requisitos obrigatórios estabelecidos neste Termo de Referência e seja compatível com a infraestrutura efetivamente existente no momento de sua implantação.

2.2.4.6. As empresas poderão, durante a elaboração de suas propostas, considerar as informações referenciais para fins de dimensionamento, compreensão das funcionalidades pretendidas e avaliação de compatibilidade e interoperabilidade da solução, podendo, quando necessário, solicitar esclarecimentos à Administração pelos meios e prazos estabelecidos no instrumento convocatório.

2.2.4.7. A utilização das informações técnicas referenciais pelas empresas deverá considerar a evolução tecnológica ocorrida desde a contratação anterior, sendo admitidas soluções tecnicamente equivalentes ou superiores, desde que atendidos os requisitos obrigatórios estabelecidos neste Termo de Referência e observadas as condições previstas no instrumento convocatório.

2.2.4.8. As informações constantes deste item não constituem indicação exclusiva de fabricante, marca, modelo, tecnologia proprietária ou solução específica, servindo exclusivamente como referência para compreensão do contexto técnico e operacional da contratação.

2.2.4.9. A CONTRATADA deverá, por ocasião da execução dos serviços, observar as condições efetivamente existentes na infraestrutura da CONTRATANTE, realizando as adequações técnicas necessárias à integração, interoperabilidade, segurança e pleno funcionamento da solução contratada, nos limites das obrigações estabelecidas neste Termo de Referência.

2.2.4.10. Para fins de interpretação, prevalecerão, em caso de divergência, as especificações técnicas e os requisitos expressamente estabelecidos para cada item deste Termo de Referência, e não as informações meramente referenciais constantes deste capítulo.

2.2.4.11. Referências técnicas para elaboração da proposta:

2.2.4.12. A CONTRATADA deverá prestar serviços especializados de segurança da informação, dentro do padrão técnico e melhores práticas de mercado, considerando as seguintes aplicações e soluções:



2.2.4.13. Solução de NGFW/SD-Wan em cluster fornecidos em appliance Tipo 1;

A CONTRATADA deverá prestar serviços especializados de segurança da informação, compreendendo o fornecimento, disponibilização, configuração, integração, manutenção, suporte técnico e atualização de solução de NGFW/SD-WAN em cluster (alta disponibilidade), fornecida em appliance Tipo 1, destinada à proteção da infraestrutura de rede do Município, observados os requisitos técnicos, funcionais e de desempenho estabelecidos nos subitens 2.2.4.25 a 2.2.4.279 deste Termo.

2.2.4.14. Solução de NGFW/SD-Wan fornecidos em appliance Tipo 2;

A CONTRATADA deverá prestar serviços especializados de segurança da informação, compreendendo o fornecimento, disponibilização, configuração, integração, manutenção, suporte técnico e atualização de solução de NGFW/SD-WAN, fornecida em appliance Tipo 2, destinada à proteção e conectividade segura da infraestrutura de rede do Município, observados os requisitos técnicos, funcionais e de desempenho estabelecidos nos subitens 2.2.4.280 a 2.2.4.532 deste Termo de Referência.

2.2.4.15. Solução da base de dados analíticos e logs fornecidos em appliance;

A CONTRATADA deverá prestar serviços especializados de segurança da informação, compreendendo o fornecimento, disponibilização, configuração, integração, manutenção, suporte técnico e atualização de solução de base de dados analíticos e gerenciamento de logs, fornecida em appliance, destinada ao armazenamento, processamento, análise e consulta centralizada dos registros e eventos de segurança da informação, observados os requisitos técnicos, funcionais e de desempenho estabelecidos nos subitens 2.2.4.533 a 2.2.4.615 deste Termo de Referência.

2.2.4.16. Solução de gerenciamento de NGFW fornecidos em appliance;

A CONTRATADA deverá prestar serviços especializados de segurança da informação, compreendendo o fornecimento, disponibilização, configuração, integração, manutenção, suporte técnico e atualização de solução de gerenciamento centralizado de NGFW, fornecida em appliance, destinada à administração, configuração, monitoramento e gestão das políticas e recursos de segurança dos equipamentos NGFW do Município, observados os requisitos técnicos, funcionais e de desempenho estabelecidos nos subitens 2.2.4.616 a 2.2.4.683 deste Termo de Referência.

2.2.4.17. Solução de Endpoint corporativo do tipo EDR;

A CONTRATADA deverá prestar serviços especializados de segurança da informação, compreendendo o fornecimento, disponibilização, configuração, integração, manutenção, suporte técnico e atualização de solução de proteção de Endpoint corporativo do tipo EDR (Endpoint Detection and Response), destinada à prevenção, detecção, monitoramento,



investigação e resposta a ameaças de segurança nos dispositivos corporativos do Município, observados os requisitos técnicos, funcionais e de desempenho estabelecidos nos subitens **2.2.4.684 a 2.2.4.818** deste Termo de Referência.

2.2.4.18. Solução de WAF appliance; A CONTRATADA deverá prestar serviços especializados de segurança da informação, compreendendo o fornecimento, disponibilização, configuração, integração, manutenção, suporte técnico e atualização de solução de WAF (Web Application Firewall), fornecida em appliance, destinada à proteção, monitoramento e controle do tráfego das aplicações web do Município contra ameaças e ataques cibernéticos, observados os requisitos técnicos, funcionais e de desempenho estabelecidos nos subitens **2.2.4.819 a 2.2.4.1.017** deste Termo.

2.2.4.19. Solução de access point corporativo; A CONTRATADA deverá prestar serviços especializados de segurança da informação, compreendendo o fornecimento, disponibilização, configuração, integração, manutenção, suporte técnico e atualização de solução de Access Point corporativo, destinada à disponibilização de conectividade de rede sem fio corporativa, com recursos de gerenciamento, segurança e controle de acesso, observados os requisitos técnicos, funcionais e de desempenho estabelecidos nos subitens **2.2.4.1.018 a 2.2.4.1.076** deste Termo.

2.2.4.20. Solução de Captive portal; A CONTRATADA deverá prestar serviços especializados de segurança da informação, compreendendo o fornecimento, disponibilização, configuração, integração, manutenção, suporte técnico e atualização de solução de Captive Portal, destinada ao gerenciamento, autenticação, controle e registro do acesso dos usuários à rede sem fio corporativa do Município, observados os requisitos técnicos, funcionais e de desempenho estabelecidos nos subitens **2.2.4.1.077 a 2.2.4.1.206** deste Termo de Referência.

2.2.4.21. Plataforma de conscientização e campanhas de phishing; A CONTRATADA deverá prestar serviços especializados de segurança da informação, compreendendo o fornecimento, disponibilização, configuração, integração, manutenção, suporte técnico e atualização de plataforma de conscientização em segurança da informação e realização de campanhas de phishing, destinada à capacitação e conscientização dos usuários do Município quanto às boas práticas de segurança da informação e à identificação e prevenção de ameaças cibernéticas, observados os requisitos técnicos, funcionais e de desempenho estabelecidos nos subitens **2.2.4.1.207 a 2.2.4.1.226** deste Termo de Referência.

2.2.4.22. Mapeamento de Vulnerabilidades; A CONTRATADA deverá prestar serviços especializados de segurança da informação, compreendendo a
Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



disponibilização, configuração, execução, análise, manutenção e suporte técnico de solução de mapeamento de vulnerabilidades, destinada à identificação, avaliação e análise de vulnerabilidades de segurança nos ativos e ambientes tecnológicos do Município, com emissão de relatórios e informações necessárias à avaliação dos riscos e à adoção de medidas de correção, observados os requisitos técnicos, funcionais e de desempenho estabelecidos nos subitens **2.2.4.1.227 a 2.2.4.1.262** deste Termo de Referência.

2.2.4.23. Unidade de serviço técnico – UST; A CONTRATADA deverá prestar serviços técnicos especializados de segurança da informação, mensurados por meio de Unidade de Serviço Técnico, destinados à execução, conforme demanda da Administração, de atividades de planejamento, configuração, integração, implantação, migração, testes, ajustes, manutenção, otimização, suporte técnico e demais serviços relacionados às soluções de segurança da informação objeto desta contratação, observados os requisitos técnicos, funcionais, operacionais e de medição estabelecidos nos subitens **2.2.4.1.263 a 2.2.4.1.282** deste Termo de Referência.

2.2.4.24. A CONTRATADA deverá fornecer a solução de acordo com a descrição técnica a seguir:

2.2.4.25. *Características técnicas dos serviços especializados de segurança da informação com solução de NGFW/SD-Wan em cluster (alta disponibilidade) fornecidos em appliance Tipo 1:*

2.2.4.26. Deverá ser fornecido em hardware do tipo appliance dedicado do mesmo fabricante;

2.2.4.27. Deve possuir interface de console serial via RJ45 ou USB;

2.2.4.28. Possuir no mínimo 1 interface RJ45-UTP para o gerenciamento out of band;

2.2.4.29. Possuir no mínimo 2 interfaces GE RJ45 para o gerenciamento do cluster;

2.2.4.30. Deve possuir no mínimo 8 (oito) interfaces GE RJ45;

2.2.4.31. Deve possuir no mínimo 8 (oito) interfaces 5/2.5/GE RJ45;

2.2.4.32. Possuir no mínimo 8 interfaces 10 GE SFP+/SFP / funcionalidades de link;

2.2.4.33. Deve possuir no mínimo 4 (quatro) interfaces GE SFP;

2.2.4.34. Deve possuir fonte de alimentação redundante;

2.2.4.35. Throughput de Firewall de no mínimo 39 (trinta e nove) Gbps;

2.2.4.36. Throughput de Prevenção de Ameaças (funcionalidades ativas de: Firewall, Controle de Aplicação, IPS, Proteção contra Malware) de no mínimo 6 (seis) Gbps;

2.2.4.37. Throughput de VPN IPSec de no mínimo 36 (trinta e seis) Gbps;

2.2.4.38. Permitir o número de túneis VPN IPSEC Site-to-Site mínimo de 2.000 mil;



- 2.2.4.39.** Permitir o número de túneis VPN IPSEC Client-to-Site mínimo de 16.000 (dezesesseis) mil;
- 2.2.4.40.** Permitir o número de túneis/usuários VPN SSL mínimo de 500 (quinhentos); Throughput de inspeção SSL de no mínimo 7 (sete) Gbps;
- 2.2.4.41.** Permitir no mínimo 11 (onze) milhões de sessões TCP Concorrentes;
- 2.2.4.42.** Permitir no mínimo 400 (quatrocentos) mil novas conexões TCP por segundo;
- 2.2.4.43.** Permitir no mínimo 10 (dez) Firewalls virtuais;
- 2.2.4.44.** Deve suportar e implementar tags de VLAN;
- 2.2.4.45.** Deve permitir a criação de no mínimo 200 VLANs padrão 802.1q nos equipamentos NGFW;
- 2.2.4.46.** Deve possuir funcionalidades de: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
- 2.2.4.47.** 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;
- 2.2.4.48.** A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
- 2.2.4.49.** A gestão do equipamento deve ser compatível através da interface de gestão Web no mesmo dispositivo de proteção da rede;
- 2.2.4.50.** Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;
- 2.2.4.51.** Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
- 2.2.4.52.** Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay; Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
- 2.2.4.53.** Os dispositivos de proteção de rede devem suportar sFlow;
- 2.2.4.54.** Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;
- 2.2.4.55.** Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
- 2.2.4.56.** Deve suportar NAT dinâmico (Many-to-1);
- 2.2.4.57.** Deve suportar NAT dinâmico (Many-to-Many);
- 2.2.4.58.** Deve suportar NAT estático (1-to-1);
- 2.2.4.59.** Deve suportar NAT estático (Many-to-Many);



- 2.2.4.60.** Deve suportar NAT estático bidirecional 1-to-1;
- 2.2.4.61.** Deve suportar Tradução de porta (PAT);
- 2.2.4.62.** Deve suportar NAT de Origem;
- 2.2.4.63.** Deve suportar NAT de Destino;
- 2.2.4.64.** Deve suportar NAT de Origem e NAT de Destino simultaneamente;
- 2.2.4.65.** Deve poder combinar NAT de origem e NAT de destino na mesma política;
- 2.2.4.66.** Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
- 2.2.4.67.** Deve suportar NAT64 e NAT46;
- 2.2.4.68.** Deve implementar o protocolo ECMP;
- 2.2.4.69.** Deve suportar SD-WAN de forma nativa;
- 2.2.4.70.** Deve implementar balanceamento de link por hash do IP de origem;
- 2.2.4.71.** Deve implementar balanceamento de link por hash do IP de origem e destino;
- 2.2.4.72.** Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;
- 2.2.4.73.** Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
- 2.2.4.74.** Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
- 2.2.4.75.** Enviar log para sistemas de monitoração externos, simultaneamente;
- 2.2.4.76.** Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
- 2.2.4.77.** Proteção anti-spoofing;
- 2.2.4.78.** Implementar otimização do tráfego entre dois equipamentos;
- 2.2.4.79.** Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
- 2.2.4.80.** Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
- 2.2.4.81.** Suportar OSPF graceful restart;
- 2.2.4.82.** Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;



2.2.4.83. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;

2.2.4.84. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

2.2.4.85. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

2.2.4.86. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;

2.2.4.87. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;

2.2.4.88. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;

2.2.4.89. A configuração em alta disponibilidade deve sincronizar: Sessões;

2.2.4.90. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QoS e objetos de rede;

2.2.4.91. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;

2.2.4.92. A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;

2.2.4.93. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

2.2.4.94. Deve possuir suporte à criação de sistemas virtuais no mesmo appliance;

2.2.4.95. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;

2.2.4.96. O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado a exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;

2.2.4.97. Controle, inspeção e descryptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);

2.2.4.98. Deve ser fornecido funcionalidade de Inspeção SSL sem limitação de licenciamento caso a solução ofertada possua licenciamento, deve ser fornecido em sua capacidade máxima.



- 2.2.4.99.** Permitir a integração com repositório de logs de forma segura e otimizada;
- 2.2.4.100.** Permitir identificar potenciais vulnerabilidades ou ameaças e orquestrar ação de prevenção.
- 2.2.4.101.** Deve existir um Serviço de Suporte que ofereça apoio do fabricante e atualização de sistema operacional;
- 2.2.4.102.** A console de administração deve suportar no mínimo inglês, espanhol e português.
- 2.2.4.103.** A console deve suportar a administração de switches e pontos de acesso para melhorar o nível de segurança;
- 2.2.4.104.** A solução deve suportar integração nativa de equipamentos de proteção de correio eletrônico, firewall de aplicações, proxy, cache e ameaças avançadas
- 2.2.4.105.** Deverá suportar controles por zona de segurança; Controles de políticas por porta e protocolo;
- 2.2.4.106.** Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
- 2.2.4.107.** Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
- 2.2.4.108.** Deve ser capaz de aplicar a inspeção Application Control e Webfiltering no mínimo e diretamente às políticas de segurança versus via perfis;
- 2.2.4.109.** Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente as políticas de firewall;
- 2.2.4.110.** Deve suportar automação de situações como detecção de equipamentos comprometidos, estado do sistema, mudanças de configuração, eventos específicos, e aplicar uma ação que possa ser notificação, bloqueio do equipamento, execução de scripts ou funções em nuvem pública;
- 2.2.4.111.** Deve suportar o padrão de indústria 'syslog' protocol para armazenamento usando o formato Common Event Format (CEF);
- 2.2.4.112.** Deve suportar integração de nuvens públicas e integração SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage e Kubernetes;
- 2.2.4.113.** Deve suportar integração com Solução de SIEM multi fabricante;
- 2.2.4.114.** Deve suportar o protocolo padrão da indústria VXLAN;
- 2.2.4.115.** A solução deve suportar a integração nativa com soluções de sandboxing;



2.2.4.116. O appliance deve estar licenciado e permitir a utilização de no mínimo 9 (nove) instâncias virtuais;

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

2.2.4.118. Reconhecer no mínimo 3000 aplicações diferentes, em camada 7, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e e-mail;

2.2.4.119. Reconhecer no mínimo as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

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

2.2.4.121. 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;

2.2.4.122. Identificar o uso de táticas evasivas via comunicações criptografadas; Atualizar a base de assinaturas de aplicações automaticamente;

2.2.4.123. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;

2.2.4.124. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

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

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

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



- 2.2.4.128.** Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
- 2.2.4.129.** Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;
- 2.2.4.130.** Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
- 2.2.4.131.** Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
- 2.2.4.132.** Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;
- 2.2.4.133.** Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
- 2.2.4.134.** Deve ser possível configurar Application Override permitindo selecionar aplicações individualmente;
- 2.2.4.135.** Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
- 2.2.4.136.** Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- 2.2.4.137.** As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;
- 2.2.4.138.** Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
- 2.2.4.139.** Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
- 2.2.4.140.** Deve permitir o bloqueio de vulnerabilidades;
- 2.2.4.141.** Deve incluir proteção contra ataques de negação de serviços;
- 2.2.4.142.** Deverá possuir os seguintes mecanismos de inspeção de IPS: Análise de decodificação de protocolo, Análise para detecção de anomalias de protocolo, IP



Defragmentation, Remontagem de pacotes de TCP, de pacotes mal formados e Bloqueio;

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

2.2.4.144. Detectar e bloquear a origem de portscans;

2.2.4.145. Bloquear ataques efetuados por worms conhecidos;

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

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

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

2.2.4.149. Identificar e bloquear comunicação com botnets;

2.2.4.150. 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;

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

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

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

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

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

2.2.4.156. Fornecer proteção contra ataques de dia zero por meio de estreita integração com os componentes incluindo NGFW (Next Generation Firewall), Sandbox (on-premise ou nuvem);

2.2.4.157. Deve ser considerado para esta especificação proteção via Sandbox do fabricante do NGFW ou terceiros, na modalidade "in cloud" ou "on premises", permitindo também na oferta de soluções on premises, appliances físicos ou virtuais.

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



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

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

2.2.4.161. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;

2.2.4.162. Possuir no mínimo 60 categorias de URLs;

2.2.4.163. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;

2.2.4.164. Permitir a customização de página de bloqueio;

2.2.4.165. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);

2.2.4.166. Além do Explicit Web Proxy, suportar proxy Web transparente;

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

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

2.2.4.169. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à utilização de sistemas virtuais, segmentos de rede, etc;

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

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



2.2.4.172. 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);

2.2.4.173. 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;

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

2.2.4.175. Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso à internet e gerenciamento da solução;

2.2.4.176. Com a finalidade de controlar aplicações de camada 7 e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esses tipos de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;

2.2.4.177. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;

2.2.4.178. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;

2.2.4.179. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;

2.2.4.180. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

2.2.4.181. Suportar a criação de políticas de QoS e Traffic Shaping por porta;

2.2.4.182. O QoS deve possibilitar a definição de tráfego com banda garantida;

2.2.4.183. O QoS deve possibilitar a definição de tráfego com banda máxima;

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

2.2.4.185. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

2.2.4.186. Suportar modificação de valores DSCP para o Diffserv;

2.2.4.187. Suportar priorização de tráfego usando informação de Type of Service;

2.2.4.188. Deve suportar QoS (traffic-shapping), em interface agregadas ou redundantes;

2.2.4.189. Permitir a criação de filtros para arquivos e dados pré-definidos;



- 2.2.4.190.** Os arquivos devem ser identificados por extensão e tipo;
- 2.2.4.191.** Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);
- 2.2.4.192.** Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 2.2.4.193.** Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 2.2.4.194.** Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;
- 2.2.4.195.** Deve contemplar a oferta do licenciamento de DLP caso a solução ofertada possua;
- 2.2.4.196.** Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
- 2.2.4.197.** Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
- 2.2.4.198.** Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;
- 2.2.4.199.** Permitir a utilização das funcionalidades de VPN Site-to-Site e Cliente-To-Site;
- 2.2.4.200.** Permitir utilizar IPSec VPN sem limitação de licenciamento caso a solução ofertada possua;
- 2.2.4.201.** Permitir utilizar SSL VPN sem limitação de licenciamento caso a solução ofertada possua;
- 2.2.4.202.** A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;
- 2.2.4.203.** A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
- 2.2.4.204.** A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
- 2.2.4.205.** A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
- 2.2.4.206.** Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
- 2.2.4.207.** Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;



- 2.2.4.208.** Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;
- 2.2.4.209.** Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
- 2.2.4.210.** Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
- 2.2.4.211.** Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
- 2.2.4.212.** Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
- 2.2.4.213.** Deverá manter uma conexão segura com o portal durante a sessão;
- 2.2.4.214.** O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior).
- 2.2.4.215.** Deverá suportar implementação de SD-WAN e possuir Console de Gerência Centralizada para essa solução;
- 2.2.4.216.** A solução SD-WAN deve ser fornecida no mesmo appliance que o NGFW;
- 2.2.4.217.** O SD-WAN deverá suportar vários links de acesso, como MPLS, Internet dedicada e Internet Móvel;
- 2.2.4.218.** Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
- 2.2.4.219.** Deve possuir capacidade de agregar e balancear, no mínimo, 2 circuitos de dados utilizando uma interface dedicada para cada circuito;
- 2.2.4.220.** Deve permitir a configuração de ISP (rota default estática) com a utilização de probe ou de forma similar para verificar a disponibilidade do provedor. A probe ou similar deve permitir verificar o acesso HTTP a pelo menos 1 (um) site web e deve considerar o ISP indisponível em caso de falha (ou alta latência);
- 2.2.4.221.** Deve balancear o tráfego das aplicações entre múltiplos links simultaneamente;
- 2.2.4.222.** Deve realizar a redistribuição do balanceamento do tráfego entre os links de comunicação utilizados, em caso de falhas nesses links, ou de acordo com as políticas de qualidade pré-definidas;
- 2.2.4.223.** Deverá simplificar a implantação de túneis criptografados de site para site;
- 2.2.4.224.** Deverá implementar a PKI usando a autoridade de certificação (CA);



2.2.4.225. Deverá permitir a comunicação indireta entre localidades por meio de topologia “hub and spoke”;

2.2.4.226. Deverá balancear o tráfego das aplicações entre múltiplos links simultaneamente;

2.2.4.227. Deverá analisar o tráfego em tempo real e realizar o balanceamento dos pacotes de um mesmo fluxo entre múltiplos links simultaneamente em uma extremidade e realizar a reordenação dos pacotes desse mesmo fluxo no outro extremo;

2.2.4.228. Deverá monitorar a latência, o jitter e o descarte de pacotes em cada um dos links individualmente;

2.2.4.229. A Solução SD-WAN deve realizar a redistribuição do balanceamento do tráfego entre os links de comunicação utilizados pelos Gateways, em caso de falhas nesses links, ou de acordo com as políticas de qualidade pré-definidas;

2.2.4.230. Deverá suportar arquitetura VRF, onde o tráfego poderá ser segmentado com base em uma definição comum de VRFs em todos os sites;

2.2.4.231. Deverá possuir serviço de servidor DHCP;

2.2.4.232. Deverá possuir serviço de DHCP relay;

2.2.4.233. Deverá implementar rotas estáticas;

2.2.4.234. Deverá implementar OSPF;

2.2.4.235. Deverá implementar BGP;

2.2.4.236. Deve ser possível implementar SD-WAN em alta disponibilidade (pelo menos 2 appliances) na Prefeitura, Unidade Municipais e Site Redundante;

2.2.4.237. Deve ser possível implementar SD-WAN utilizando VRRP e realizar a recuperação de falhas através de um roteador compatível com esse protocolo;

2.2.4.238. Deverá suportar aplicativos hospedados em Data Center próprio e também aqueles consumidos como serviço na nuvem;

2.2.4.239. A solução deverá garantir performance de aplicações que utilizam VPN nos sites remotos e serviços de nuvem (SaaS);

2.2.4.240. A solução deverá medir e reagir independentemente à condição de rede UNIDIRECIONALMENTE para todas as condições (Latência, Jitter, Perda, Largura de banda - BW);

2.2.4.241. Deverá fornecer desempenho para os aplicativos em um cenário de link de transporte duplo quando um dos links está prejudicado;

2.2.4.242. Deverá fornecer desempenho para os aplicativos em um cenário de link de transporte duplo quando os dois links estão prejudicados;



2.2.4.243. A Solução deverá possuir algum mecanismo de QoS para proteger o tráfego de Internet quanto tiver congestionamento na unidade regional;

2.2.4.244. A Solução deverá permitir que sites de unidades regionais acessem sites VPN legados (não-SD-WAN) sem fazer backhauling do tráfego de aplicativos por meio de um hub SD-WAN;

2.2.4.245. Deve ser possível criar políticas para a modelagem do tráfego definindo pelo menos os parâmetros:

2.2.4.246. IP de Origem;

2.2.4.247. IP de Destino;

2.2.4.248. Porta TCP/UDP de Destino;

2.2.4.249. Domínio e URL de destino;

2.2.4.250. Aplicação de camada 7 utilizada (Office 365, Exchange, SAS, Dropbox, Box, Zoom e etc);

2.2.4.251. Agendamento e gerenciamento de filas;

2.2.4.252. Remarcação de DSCP;

2.2.4.253. Definição dos links utilizados em situação normal;

2.2.4.254. Definição dos links utilizados em caso de falha do(s) link(s) primários;

2.2.4.255. Traffic Shapping;

2.2.4.256. A solução deverá suportar convergência rápida de tráfego de um túnel ao outro sem perda de sessões TCP/UDP previamente estabelecidas;

2.2.4.257. Poderá ser configurado utilizando perfis e políticas de segurança atribuídos de forma dinâmica;

2.2.4.258. Deverá possuir serviço de Firewall Stateful;

2.2.4.259. Deverá fornecer criptografia AES de 128 bits ou AES de 256 bits em sua VPN;

2.2.4.260. A solução deve permitir a inserção automática de serviços de segurança de nuvem, ou seja, com interceptação de tráfego por aplicação e envio à diferentes fornecedores de serviços de segurança em nuvem.

2.2.4.261. A solução deve suportar VPNs do tipo Hub Spoke e Full Mesh;

2.2.4.262. A solução deverá oferecer uma API RESTful completa para integração de orquestração no NOC de forma segura e criptografada;

2.2.4.263. Todo o provisionamento de serviços deverá ser feito via GUI no sistema de gerenciamento;

2.2.4.264. Todas as alterações de configuração deverão ser registradas e arquivadas para fins de auditoria;



2.2.4.265. Deverá suportar SNMP versões 2c e 3;

2.2.4.266. A console de Gerência deverá informar o status UP/DOWN/SPEED das interfaces LAN e WAN;

2.2.4.267. Deverá permitir que todos os alarmes e eventos sejam registrados na console de Gerência;

2.2.4.268. A Gerência SD-WAN deverá enviar mensagens syslog referentes aos Gateways SD- WAN para um servidor syslog externo da CONTRATADA e da CONTRATANTE;

2.2.4.269. Deverá realizar medições de latência, Jitter e descarte de pacotes para cada destino em cada uma das interfaces dos Gateways SD-WAN a cada 5 (cinco) minutos no mínimo;

2.2.4.270. As medições de taxa de ocupação do link, latência, Jitter e descarte de pacotes e as estatísticas de interface deverão ser coletadas de cada Gateway SDWAN a cada 5 (cinco) minutos no mínimo;

2.2.4.271. As medições de taxa de ocupação do link, latência, Jitter e descarte de pacotes deverão ser visíveis na GUI da gerência SD-WAN;

2.2.4.272. Possuir os contadores de estatísticas de LAN e WAN dos Gateway SD WAN (bits RX/TX, entrada/saída de pacotes, descartes de pacotes e erros);

2.2.4.273. Deverá ter a capacidade para medir os fluxos de aplicativos como volume de dados trafegados, quantidade de transações entre outros;

2.2.4.274. Os resultados de desempenho de link e aplicativo deverão ser visualizados em forma de gráfico a partir da GUI de Gerência SD-WAN;

2.2.4.275. Deverá suportar exportação de registros Netflow / IPFIX/ Netstream baseada em padrões;

2.2.4.276. Deverá possuir provisionamento do Zero Touch que deverá funcionar de tal forma que um CPE SD-WAN seja enviado diretamente do fornecedor de SD-WAN para uma instalação do cliente sem a necessidade de configuração prévia do CPE SD-WAN;

2.2.4.277. Deverá ter a flexibilidade para ser gerenciada pelo cliente e/ou gerenciada pelo parceiro.

2.2.4.278. Deverá possibilitar Geolocalização do dispositivo;

2.2.4.279. Deverá manter Backups de toda a solução sob sua guarda a fim de rápida recuperação em caso de substituição do equipamento.

2.2.4.280. Características técnicas dos serviços especializados de segurança da informação com solução de NGFW/SD-Wan fornecidos em appliance Tipo 2:



- 2.2.4.281.** Deverá ser fornecido em hardware do tipo appliance dedicado do mesmo fabricante;
- 2.2.4.282.** Deve possuir interface de console serial via RJ45 ou USB;
- 2.2.4.283.** Deve possuir no mínimo 1 (uma) interface RJ45-UTP dedicada ao gerenciamento out of band;
- 2.2.4.284.** Deve possuir no mínimo 4 (quatro) interfaces GE RJ45;
- 2.2.4.285.** Das 4 (quatro) interfaces GE RJ45 existentes, no mínimo 1 (uma) deve possuir funcionalidade de link;
- 2.2.4.286.** Throughput de Firewall de no mínimo 4 (quatro) Gbps;
- 2.2.4.287.** Throughput de Prevenção de Ameaças (funcionalidades ativas de: Firewall, Controle de Aplicação, IPS, Proteção contra Malware) de no mínimo 500 (quinhentos) Mbps;
- 2.2.4.288.** Throughput de VPN IPsec de no mínimo 3.5 (três ponto cinco) Gbps;
- 2.2.4.289.** Permitir o número de túneis VPN IPSEC Site-to-Site mínimo de 200 (duzentos);
- 2.2.4.290.** Permitir o número de túneis VPN IPSEC Client-to-Site mínimo de 250 (duzentos e cinquenta);
- 2.2.4.291.** Permitir no mínimo 600 (seiscentos) mil sessões TCP Concorrentes;
- 2.2.4.292.** Permitir no mínimo 30 (trinta) mil novas conexões TCP por segundo;
- 2.2.4.293.** Permitir no mínimo 10 (dez) Firewalls virtuais;
- 2.2.4.294.** Deve suportar e implementar tags de VLAN;
- 2.2.4.295.** Deve permitir a criação de no mínimo 100 VLANs padrão 802.1q nos equipamentos NGFW;
- 2.2.4.296.** Deve possuir funcionalidades de: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
- 2.2.4.297.** 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;
- 2.2.4.298.** A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
- 2.2.4.299.** A gestão do equipamento deve ser compatível através da interface de gestão Web no mesmo dispositivo de proteção da rede;
- 2.2.4.300.** Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;



- 2.2.4.301.** Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
- 2.2.4.302.** Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
- 2.2.4.303.** Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
- 2.2.4.304.** Os dispositivos de proteção de rede devem suportar sFlow;
- 2.2.4.305.** Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;
- 2.2.4.306.** Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
- 2.2.4.307.** Deve suportar NAT dinâmico (Many-to-1);
- 2.2.4.308.** Deve suportar NAT dinâmico (Many-to-Many);
- 2.2.4.309.** Deve suportar NAT estático (1-to-1);
- 2.2.4.310.** Deve suportar NAT estático (Many-to-Many);
- 2.2.4.311.** Deve suportar NAT estático bidirecional 1-to-1;
- 2.2.4.312.** Deve suportar Tradução de porta (PAT);
- 2.2.4.313.** Deve suportar NAT de Origem;
- 2.2.4.314.** Deve suportar NAT de Destino;
- 2.2.4.315.** Deve suportar NAT de Origem e NAT de Destino simultaneamente;
- 2.2.4.316.** Deve poder combinar NAT de origem e NAT de destino na mesma política;
- 2.2.4.317.** Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
- 2.2.4.318.** Deve suportar NAT64 e NAT46;
- 2.2.4.319.** Deve implementar o protocolo ECMP;
- 2.2.4.320.** Deve suportar SD-WAN de forma nativa;
- 2.2.4.321.** Deve implementar balanceamento de link por hash do IP de origem;
- 2.2.4.322.** Deve implementar balanceamento de link por hash do IP de origem e destino;
- 2.2.4.323.** Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;
- 2.2.4.324.** Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
- 2.2.4.325.** Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos
- Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;**
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;

2.2.4.326. Enviar log para sistemas de monitoração externos, simultaneamente;

2.2.4.327. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;

2.2.4.328. Proteção anti-spoofing;

2.2.4.329. Implementar otimização do tráfego entre dois equipamentos;

2.2.4.330. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

2.2.4.331. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

2.2.4.332. Suportar OSPF graceful restart;

2.2.4.333. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

2.2.4.334. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;

2.2.4.335. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

2.2.4.336. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

2.2.4.337. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;

2.2.4.338. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3;

2.2.4.339. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em layer 3 e com no mínimo 3 equipamentos no cluster;

2.2.4.340. A configuração em alta disponibilidade deve sincronizar: Sessões;

2.2.4.341. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QoS e objetos de rede;

2.2.4.342. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;

2.2.4.343. A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;

2.2.4.344. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;

2.2.4.345. Deve possuir suporte à criação de sistemas virtuais no mesmo appliance;



2.2.4.346. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;

2.2.4.347. O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado a exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;

2.2.4.348. Controle, inspeção e descryptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);

2.2.4.349. Deve ser fornecido funcionalidade de Inspeção SSL sem limitação de licenciamento caso a solução ofertada possua licenciamento, deve ser fornecido em sua capacidade máxima.

2.2.4.350. Permitir a integração com repositório de logs de forma segura e otimizada;

2.2.4.351. Permitir identificar potenciais vulnerabilidades ou ameaças e orquestrar ação de prevenção.

2.2.4.352. Deve existir um Serviço de Suporte que ofereça apoio do fabricante e atualização de sistema operacional;

2.2.4.353. A console de administração deve suportar no mínimo inglês, espanhol e português.

2.2.4.354. A console deve suportar a administração de switches e pontos de acesso para melhorar o nível de segurança;

2.2.4.355. A solução deve suportar integração nativa de equipamentos de proteção de correio eletrônico, firewall de aplicações, proxy, cache e ameaças avançadas

2.2.4.356. Deverá suportar controles por zona de segurança;

2.2.4.357. Controles de políticas por porta e protocolo;

2.2.4.358. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

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

2.2.4.360. Deve ser capaz de aplicar a inspeção Application Control e Webfiltering no mínimo e diretamente às políticas de segurança versus via perfis;



2.2.4.361. Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente as políticas de firewall;

2.2.4.362. Deve suportar automação de situações como detecção de equipamentos comprometidos, estado do sistema, mudanças de configuração, eventos específicos, e aplicar uma ação que possa ser notificação, bloqueio do equipamento, execução de scripts ou funções em nuvem pública;

2.2.4.363. Deve suportar o padrão de indústria 'syslog' protocol para armazenamento usando o formato Common Event Format (CEF);

2.2.4.364. Deve suportar integração de nuvens públicas e integração SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage e Kubernetes;

2.2.4.365. Deve suportar integração com Solução de SIEM multi fabricante;

2.2.4.366. Deve suportar o protocolo padrão da indústria VXLAN;

2.2.4.367. A solução deve suportar a integração nativa com soluções de sandboxing;

2.2.4.368. O appliance deve estar licenciado e permitir a utilização de no mínimo 9 (nove) instâncias virtuais;

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

2.2.4.370. Reconhecer no mínimo 3000 aplicações diferentes, em camada 7, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e e-mail;

2.2.4.371. Reconhecer no mínimo as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

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

2.2.4.373. 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;

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



- 2.2.4.375.** Atualizar a base de assinaturas de aplicações automaticamente;
- 2.2.4.376.** Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;
- 2.2.4.377.** Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
- 2.2.4.378.** Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
- 2.2.4.379.** O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- 2.2.4.380.** Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
- 2.2.4.381.** Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
- 2.2.4.382.** Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;
- 2.2.4.383.** Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
- 2.2.4.384.** Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
- 2.2.4.385.** Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;
- 2.2.4.386.** Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
- 2.2.4.387.** Deve ser possível configurar Application Override permitindo selecionar aplicações individualmente;
- 2.2.4.388.** Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
- 2.2.4.389.** Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- 2.2.4.390.** As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que
- Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;**
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

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

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

2.2.4.393. Deve permitir o bloqueio de vulnerabilidades;

2.2.4.394. Deve incluir proteção contra ataques de negação de serviços;

2.2.4.395. Deverá possuir os seguintes mecanismos de inspeção de IPS: Análise de decodificação de protocolo, Análise para detecção de anomalias de protocolo, IP Defragmentation, Remontagem de pacotes de TCP, de pacotes mal formados e Bloqueio;

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

2.2.4.397. Detectar e bloquear a origem de portscans;

2.2.4.398. Bloquear ataques efetuados por worms conhecidos;

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

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

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

2.2.4.402. Identificar e bloquear comunicação com botnets;

2.2.4.403. 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;

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

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

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

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

2.2.4.408. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos



de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por usuários, grupos de usuários, origem, destino e zonas de segurança;

2.2.4.409. Fornecer proteção contra ataques de dia zero por meio de estreita integração com os componentes incluindo NGFW (Next Generation Firewall), Sandbox (on-premise ou nuvem);

2.2.4.410. Deve ser considerado para esta especificação proteção via Sandbox do fabricante do NGFW ou terceiros, na modalidade "in cloud" ou "on premises", permitindo também na oferta de soluções on premises, appliances físicos ou virtuais.

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

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

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

2.2.4.414. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;

2.2.4.415. Possuir no mínimo 60 categorias de URLs;

2.2.4.416. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;

2.2.4.417. Permitir a customização de página de bloqueio;

2.2.4.418. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);

2.2.4.419. Além do Explicit Web Proxy, suportar proxy Web transparente;

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

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



2.2.4.422. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à utilização de sistemas virtuais, segmentos de rede, etc;

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

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

2.2.4.425. 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);

2.2.4.426. 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;

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

2.2.4.428. Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso à internet e gerenciamento da solução;

2.2.4.429. Com a finalidade de controlar aplicações de camada 7 e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esses tipos de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;

2.2.4.430. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;

2.2.4.431. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;

2.2.4.432. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;



- 2.2.4.433.** Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
- 2.2.4.434.** Suportar a criação de políticas de QoS e Traffic Shaping por porta;
- 2.2.4.435.** O QoS deve possibilitar a definição de tráfego com banda garantida;
- 2.2.4.436.** O QoS deve possibilitar a definição de tráfego com banda máxima;
- 2.2.4.437.** O QoS deve possibilitar a definição de fila de prioridade;
- 2.2.4.438.** Suportar marcação de pacotes Diffserv, inclusive por aplicação;
- 2.2.4.439.** Suportar modificação de valores DSCP para o Diffserv;
- 2.2.4.440.** Suportar priorização de tráfego usando informação de Type of Service;
- 2.2.4.441.** Deve suportar QoS (traffic-shapping), em interface agregadas ou redundantes;
- 2.2.4.442.** Permitir a criação de filtros para arquivos e dados pré-definidos;
- 2.2.4.443.** Os arquivos devem ser identificados por extensão e tipo;
- 2.2.4.444.** Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);
- 2.2.4.445.** Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 2.2.4.446.** Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 2.2.4.447.** Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;
- 2.2.4.448.** Deve contemplar a oferta do licenciamento de DLP caso a solução ofertada possua;
- 2.2.4.449.** Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
- 2.2.4.450.** Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
- 2.2.4.451.** Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;
- 2.2.4.452.** Permitir a utilização das funcionalidades de VPN Site-to-Site e Cliente-To-Site;
- 2.2.4.453.** Permitir utilizar IPSec VPN sem limitação de licenciamento caso a solução ofertada possua;



- 2.2.4.454.** Permitir utilizar SSL VPN sem limitação de licenciamento caso a solução ofertada possua;
- 2.2.4.455.** A VPN IPSEC deve suportar Autenticação MD5 e SHA-1;
- 2.2.4.456.** A VPN IPSEC deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
- 2.2.4.457.** A VPN IPSEC deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
- 2.2.4.458.** A VPN IPSEC deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
- 2.2.4.459.** Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
- 2.2.4.460.** Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSEC IPv6;
- 2.2.4.461.** Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;
- 2.2.4.462.** Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
- 2.2.4.463.** Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
- 2.2.4.464.** Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
- 2.2.4.465.** Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
- 2.2.4.466.** Deverá manter uma conexão segura com o portal durante a sessão;
- 2.2.4.467.** O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior).
- 2.2.4.468.** Deverá suportar implementação de SD-WAN e possuir Console de Gerência Centralizada para essa solução;
- 2.2.4.469.** A solução SD-WAN deve ser fornecida no mesmo appliance que o NGFW;
- 2.2.4.470.** O SD-WAN deverá suportar vários links de acesso, como MPLS, Internet dedicada e Internet Móvel;
- 2.2.4.471.** Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;



- 2.2.4.472.** Deve possuir capacidade de agregar e balancear, no mínimo, 2 circuitos de dados utilizando uma interface dedicada para cada circuito;
- 2.2.4.473.** Deve permitir a configuração de ISP (rota default estática) com a utilização de probe ou de forma similar para verificar a disponibilidade do provedor. A probe ou similar deve permitir verificar o acesso HTTP a pelo menos 1 (um) site web e deve considerar o ISP indisponível em caso de falha (ou alta latência);
- 2.2.4.474.** Deve balancear o tráfego das aplicações entre múltiplos links simultaneamente;
- 2.2.4.475.** Deve realizar a redistribuição do balanceamento do tráfego entre os links de comunicação utilizados, em caso de falhas nesses links, ou de acordo com as políticas de qualidade pré-definidas;
- 2.2.4.476.** Deverá simplificar a implantação de túneis criptografados de site para site;
- 2.2.4.477.** Deverá implementar a PKI usando a autoridade de certificação (CA);
- 2.2.4.478.** Deverá permitir a comunicação indireta entre localidades por meio de topologia “hub and spoke”;
- 2.2.4.479.** Deverá balancear o tráfego das aplicações entre múltiplos links simultaneamente;
- 2.2.4.480.** Deverá analisar o tráfego em tempo real e realizar o balanceamento dos pacotes de um mesmo fluxo entre múltiplos links simultaneamente em uma extremidade e realizar a reordenação dos pacotes desse mesmo fluxo no outro extremo;
- 2.2.4.481.** Deverá monitorar a latência, o jitter e o descarte de pacotes em cada um dos links individualmente;
- 2.2.4.482.** A Solução SD-WAN deve realizar a redistribuição do balanceamento do tráfego entre os links de comunicação utilizados pelos Gateways, em caso de falhas nesses links, ou de acordo com as políticas de qualidade pré-definidas;
- 2.2.4.483.** Deverá suportar arquitetura VRF, onde o tráfego poderá ser segmentado com base em uma definição comum de VRFs em todos os sites;
- 2.2.4.484.** Deverá possuir serviço de servidor DHCP;
- 2.2.4.485.** Deverá possuir serviço de DHCP relay;
- 2.2.4.486.** Deverá implementar rotas estáticas;
- 2.2.4.487.** Deverá implementar OSPF;
- 2.2.4.488.** Deverá implementar BGP;
- 2.2.4.489.** Deve ser possível implementar SD-WAN em alta disponibilidade (pelo menos 2 appliances) na Prefeitura, Unidade Municipais e Site Redundante;



2.2.4.490. Deve ser possível implementar SD-WAN utilizando VRRP e realizar a recuperação de falhas através de um roteador compatível com esse protocolo;

2.2.4.491. Deverá suportar aplicativos hospedados em Data Center próprio e também aqueles consumidos como serviço na nuvem;

2.2.4.492. A solução deverá garantir performance de aplicações que utilizam VPN nos sites remotos e serviços de nuvem (SaaS);

2.2.4.493. A solução deverá medir e reagir independentemente à condição de rede UNIDIRECIONALMENTE para todas as condições (Latência, Jitter, Perda, Largura de banda - BW);

2.2.4.494. Deverá fornecer desempenho para os aplicativos em um cenário de link de transporte duplo quando um dos links está prejudicado;

2.2.4.495. Deverá fornecer desempenho para os aplicativos em um cenário de link de transporte duplo quando os dois links estão prejudicados;

2.2.4.496. A Solução deverá possuir algum mecanismo de QoS para proteger o tráfego de Internet quanto tiver congestionamento na unidade regional;

2.2.4.497. A Solução deverá permitir que sites de unidades regionais acessem sites VPN legados (não-SD-WAN) sem fazer backhauling do tráfego de aplicativos por meio de um hub SD-WAN;

2.2.4.498. Deve ser possível criar políticas para a modelagem do tráfego definindo pelo menos os parâmetros:

2.2.4.499. IP de Origem;

2.2.4.500. IP de Destino;

2.2.4.501. Porta TCP/UDP de Destino;

2.2.4.502. Domínio e URL de destino;

2.2.4.503. Aplicação de camada 7 utilizada (Office 365, Exchange, SAS, Dropbox, Box, Zoom e etc);

2.2.4.504. Agendamento e gerenciamento de filas;

2.2.4.505. Remarcação de DSCP;

2.2.4.506. Definição dos links utilizados em situação normal;

2.2.4.507. Definição dos links utilizados em caso de falha do(s) link(s) primários;

2.2.4.508. Traffic Shapping;

2.2.4.509. A solução deverá suportar convergência rápida de tráfego de um túnel ao outro sem perda de sessões TCP/UDP previamente estabelecidas;

2.2.4.510. Poderá ser configurado utilizando perfis e políticas de segurança atribuídos de forma dinâmica;



- 2.2.4.511.** Deverá possuir serviço de Firewall Stateful;
- 2.2.4.512.** Deverá fornecer criptografia AES de 128 bits ou AES de 256 bits em sua VPN;
- 2.2.4.513.** A solução deve permitir a inserção automática de serviços de segurança de nuvem, ou seja, com interceptação de tráfego por aplicação e envio à diferentes fornecedores de serviços de segurança em nuvem.
- 2.2.4.514.** A solução deve suportar VPNs do tipo Hub Spoke e Full Mesh;
- 2.2.4.515.** A solução deverá oferecer uma API RESTful completa para integração de orquestração no NOC de forma segura e criptografada;
- 2.2.4.516.** Todo o provisionamento de serviços deverá ser feito via GUI no sistema de gerenciamento;
- 2.2.4.517.** Todas as alterações de configuração deverão ser registradas e arquivadas para fins de auditoria;
- 2.2.4.518.** Deverá suportar SNMP versões 2c e 3;
- 2.2.4.519.** A console de Gerência deverá informar o status UP/DOWN/SPEED das interfaces LAN e WAN;
- 2.2.4.520.** Deverá permitir que todos os alarmes e eventos sejam registrados na console de Gerência;
- 2.2.4.521.** A Gerência SD-WAN deverá enviar mensagens syslog referentes aos Gateways SD- WAN para um servidor syslog externo da CONTRATADA e da CONTRATANTE;
- 2.2.4.522.** Deverá realizar medições de latência, Jitter e descarte de pacotes para cada destino em cada uma das interfaces dos Gateways SD-WAN a cada 5 (cinco) minutos no mínimo;
- 2.2.4.523.** As medições de taxa de ocupação do link, latência, Jitter e descarte de pacotes e as estatísticas de interface deverão ser coletadas de cada Gateway SDWAN a cada 5 (cinco) minutos no mínimo;
- 2.2.4.524.** As medições de taxa de ocupação do link, latência, Jitter e descarte de pacotes deverão ser visíveis na GUI da gerência SD-WAN;
- 2.2.4.525.** Possuir os contadores de estatísticas de LAN e WAN dos Gateway SD WAN (bits RX/TX, entrada/saída de pacotes, descartes de pacotes e erros);
- 2.2.4.526.** Deverá ter a capacidade para medir os fluxos de aplicativos como volume de dados trafegados, quantidade de transações entre outros;
- 2.2.4.527.** Os resultados de desempenho de link e aplicativo deverão ser visualizados em forma de gráfico a partir da GUI de Gerência SD-WAN;



2.2.4.528. Deverá suportar exportação de registros Netflow / IPFIX / Netstream baseada em padrões;

2.2.4.529. Deverá possuir provisionamento do Zero Touch que deverá funcionar de tal forma que um CPE SD-WAN seja enviado diretamente do fornecedor de SD-WAN para uma instalação do cliente sem a necessidade de configuração prévia do CPE SD-WAN;

2.2.4.530. Deverá ter a flexibilidade para ser gerenciada pelo cliente e/ou gerenciada pelo parceiro.

2.2.4.531. Deverá possibilitar Geolocalização do dispositivo;

2.2.4.532. Deverá manter Backups de toda a solução sob sua guarda a fim de rápida recuperação em caso de substituição do equipamento.

2.2.4.533. Características Técnicas da Solução da Base de Dados Analíticos e Logs fornecidos em Appliance:

2.2.4.534. A solução de base de dados Analíticos e Log deverá ser fornecida em appliance dedicado e ser do mesmo fabricante da solução NGFW do Tipo 1 e Tipo 2;

2.2.4.535. Deve suportar o acesso via SSH, WEB (HTTPS) para gerenciamento da solução;

2.2.4.536. Possuir comunicação e autenticação criptografada com usuário e senha para obter relatórios, na interface gráfica (GUI) e via linha de comando no console de gerenciamento;

2.2.4.537. Deve possuir a capacidade de armazenar de forma centralizada no mínimo 100 Gigas de Log/Dia, por período mínimo de 90 dias;

2.2.4.538. Deve possuir capacidade de gerenciar Logs de no mínimo 180 dispositivos do tipo NGFW do Tipo 1 e Tipo 2;

2.2.4.539. Deve possuir no mínimo 2 (dois) discos com capacidade total de 8TB internos;

2.2.4.540. Deve suportar no mínimo RAID "0" e "1";

2.2.4.541. A solução deve ter o recurso de Multi-tenancy, possibilitando separar os logs de NGFW por grupos de acessos;

2.2.4.542. Permitir acesso simultâneo à administração, bem como criar no mínimo 2 (dois) perfis para administração e monitoramento;

2.2.4.543. Possuir suporte para SNMP versão 2 e 3;

2.2.4.544. Permitir a virtualização do gerenciamento e administração dos dispositivos, onde cada administrador tem acesso apenas aos equipamentos autorizados;



2.2.4.545. Deve permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução;

2.2.4.546. Deve estar licenciado, permitindo o uso integrado e operacional de todas as instâncias virtuais NGFW requisitadas;

2.2.4.547. Deve permitir ativar e desativar para cada interface da plataforma, as permissões de acesso HTTP, HTTPS e SSH;

2.2.4.548. Permitir a autenticação de usuários de acesso à plataforma via LDAP;

2.2.4.549. Permitir a autenticação de usuários de acesso à plataforma via Radius;

2.2.4.550. Permitir a autenticação de usuários de acesso à plataforma via TACACS +;

2.2.4.551. Permitir a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;

2.2.4.552. Permitir a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;

2.2.4.553. Permitir a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;

2.2.4.554. Permitir a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;

2.2.4.555. Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;

2.2.4.556. Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;

2.2.4.557. Deve possuir mecanismos de remoção automática para logs antigos;

2.2.4.558. Permitir importação e exportação de relatórios;

2.2.4.559. Deve ter a capacidade de criar relatórios no formato HTML;

2.2.4.560. Deve ter a capacidade de criar relatórios em formato PDF;

2.2.4.561. Deve ter a capacidade de criar relatórios no formato XML;

2.2.4.562. Deve ter a capacidade de criar relatórios no formato CSV;

2.2.4.563. Deve permitir exportar os logs no formato CSV;

2.2.4.564. Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;

2.2.4.565. Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;

2.2.4.566. A solução deve ter relatórios predefinidos;



2.2.4.567. Deve permitir o envio automático dos logs para um servidor FTP externo a solução;

2.2.4.568. A duplicação de relatórios existentes deve ser possível para edição posterior;

2.2.4.569. Deve ter a capacidade de personalizar a capa dos relatórios obtidos;

2.2.4.570. Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;

2.2.4.571. Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;

2.2.4.572. Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;

2.2.4.573. Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;

2.2.4.574. Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;

2.2.4.575. Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;

2.2.4.576. Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;

2.2.4.577. Permitir o envio de relatórios por e-mail automaticamente;

2.2.4.578. Deve permitir que o relatório seja enviado por e-mail para o destinatário específico;

2.2.4.579. Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;

2.2.4.580. Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;

2.2.4.581. Deve permitir o uso de filtros nos relatórios;

2.2.4.582. Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;

2.2.4.583. Permitir especificar o idioma dos relatórios criados;

2.2.4.584. Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;

2.2.4.585. Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;



- 2.2.4.586.** Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;
- 2.2.4.587.** Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;
- 2.2.4.588.** Deve ter uma ferramenta que permita analisar o desempenho na geração de relatórios, com o objetivo de detectar e corrigir problemas na geração deles;
- 2.2.4.589.** A solução deve permitir importar arquivos com logs de dispositivos compatíveis conhecidos e não conhecidos pela plataforma, para geração posterior de relatórios;
- 2.2.4.590.** Deve ser possível definir o espaço que cada instância de virtualização pode usar para armazenamento de log;
- 2.2.4.591.** Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;
- 2.2.4.592.** Deve ser compatível com a autenticação de fator duplo (token) para usuários do administrador da plataforma;
- 2.2.4.593.** Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;
- 2.2.4.594.** Deve permitir visualizar em tempo real os logs recebidos;
- 2.2.4.595.** Deve permitir o encaminhamento de log no formato syslog;
- 2.2.4.596.** Deve permitir o encaminhamento de log no formato CEF (Common Event Format);
- 2.2.4.597.** Deve permitir gerar alertas de eventos a partir de logs recebidos;
- 2.2.4.598.** Deve permitir a criação de incidentes a partir de alertas de eventos para o terminal;
- 2.2.4.599.** Deve permitir a integração ao sistema de tickets do ServiceNow;
- 2.2.4.600.** Deverá possuir licença do serviço de Indicadores de Comprometimento (IoC) do mesmo fabricante, que mostra as suspeitas de envolvimento do usuário final na Web e deve relatar no mínimo: endereço IP do usuário, nome do host, sistema operacional, veredito (classificação geral da ameaça) e o número de ameaças detectadas;
- 2.2.4.601.** Deverá possuir licença do serviço de detecção de surtos (Outbreak) com detecção automatizado de novos malwares, incluindo relatório resumo de como o malware detectado age;
- 2.2.4.602.** Deve suportar o padrão SAML para autenticação do usuário administrador;
- Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;**
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



- 2.2.4.603.** Deve ter um relatório de uso do aplicativo SaaS;
- 2.2.4.604.** Deve ter um relatório de prevenção de perda de dados (DLP);
- 2.2.4.605.** Deve ter um relatório de VPN;
- 2.2.4.606.** Deve ter um relatório IPS (Intruder Prevention System);
- 2.2.4.607.** Deve ter um relatório de reputação do cliente;
- 2.2.4.608.** Deve ter um relatório de análise de segurança do usuário;
- 2.2.4.609.** Deve ter um relatório de análise de ameaças cibernéticas;
- 2.2.4.610.** Deve ter um relatório diário resumido de eventos e incidentes de segurança;
- 2.2.4.611.** Deve ter um relatório de tráfego DNS;
- 2.2.4.612.** Deve ter um relatório de tráfego de e-mail;
- 2.2.4.613.** Deve ter um relatório dos 10 principais aplicativos usados na rede;
- 2.2.4.614.** Deve ter um relatório dos 10 principais sites usados na rede;
- 2.2.4.615.** Deve ter um relatório de uso de mídia social.
- 2.2.4.616. Características Técnicas da Solução de Gerencia de NGFW fornecidos em Appliance:**
- 2.2.4.617.** A solução de gerenciamento centralizado deverá ser do mesmo fabricante da solução de NGFW do Tipo 1 e Tipo 2;
- 2.2.4.618.** A solução de Gerência Centralizada deverá ser fornecida em appliance dedicado;
- 2.2.4.619.** Deve ter a capacidade de provisionamento e monitoramento da configuração de todos os dispositivos gerenciados a partir de um único console;
- 2.2.4.620.** Deve possuir a capacidade de gerenciar de forma centralizada, no mínimo 30 dispositivos do tipo NGFW;
- 2.2.4.621.** Deve possuir a capacidade de armazenar de forma centralizada no mínimo 2 Gigas de Log/Dia, por período mínimo de 90 dias;
- 2.2.4.622.** Deve possuir no mínimo 2 (dois) discos com capacidade total de 8TB internos;
- 2.2.4.623.** Deve suportar no mínimo RAID "0" e "1";
- 2.2.4.624.** Como parte da visibilidade dos dispositivos gerenciados centralmente, a solução deve possibilitar via dashboard status do link, desempenho do aplicativo, utilização da largura de banda e conformidade com o SLA objetivo;
- 2.2.4.625.** Deve ter a capacidade de automatizar fluxos de trabalho e configurações para dispositivos gerenciados em um único console;



2.2.4.626. A solução deve ter o recurso de Multi-tenancy para separar os dados de gerenciamento da infraestrutura lógica ou geograficamente e permitir a implantação do zerotouch para o rápido provisionamento em massa;

2.2.4.627. Deve ter a capacidade de permitir o provisionamento de comunidades VPN e monitorar as conexões VPN de todos os dispositivos gerenciados a partir de um único console e exibir sua localização geográfica em um mapa;

2.2.4.628. A solução deve permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança;

2.2.4.629. Permite a integração de trocas e compartilhamento de dados com terceiros por meio do pxGrid, OCI e Esxi;

2.2.4.630. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

2.2.4.631. Permitir acesso concorrente de administradores;

2.2.4.632. Possuir interface baseada em linha de comando para administração da solução de gerência;

2.2.4.633. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

2.2.4.634. Bloqueio de alterações, no caso de acesso simultâneo de dois ou mais administradores;

2.2.4.635. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

2.2.4.636. Gerar alertas automáticos via Email;

2.2.4.637. Gerar alertas automáticos via SNMP;

2.2.4.638. Gerar alertas automáticos via Syslog;

2.2.4.639. Deve suportar backup/restore de todas as configurações da solução de gerência, permitindo ao administrador agendar backups da configuração em um determinado dia e hora;

2.2.4.640. Deve ser permitido ao administrador transferir os backups para um servidor FTP;

2.2.4.641. Deve ser permitido ao administrador transferir os backups para um servidor SCP;

2.2.4.642. Deve ser permitido ao administrador transferir os backups para um servidor SFTP;

2.2.4.643. As alterações realizadas em um servidor de gerência deverão ser automaticamente replicadas para o servidor redundante;



2.2.4.644. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de contas de usuários LOCAIS;

2.2.4.645. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de base externa TACACS;

2.2.4.646. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de usuários de base externa LDAP;

2.2.4.647. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de base externa RADIUS;

2.2.4.648. Deve ser permitido aos administradores se autenticarem nos servidores de gerência através de Certificado Digital X.509 (PKI);

2.2.4.649. Deve suportar sincronização do relógio interno via protocolo NTP;

2.2.4.650. Deve registrar as ações efetuadas por quaisquer usuários;

2.2.4.651. Devem ser fornecidos manuais de instalação, configuração e operação de toda a solução, na língua portuguesa ou inglesa, com apresentação de boa qualidade;

2.2.4.652. Suportar SNMP versão 2 e versão 3 nos equipamentos de gerência;

2.2.4.653. Deve permitir habilitar e desabilitar, para cada interface de rede da solução de gerência, permissões de acesso HTTP, HTTPS, SSH, SNMP e Telnet;

2.2.4.654. Deve permitir virtualizar a solução de gerência, de forma que cada administrador possa gerenciar, visualizar e editar apenas os dispositivos autorizados e cadastrados no seu ambiente virtualizado;

2.2.4.655. O gerenciamento deve possibilitar a criação e administração de políticas de firewall e controle de aplicação;

2.2.4.656. O gerenciamento deve possibilitar a criação e administração de políticas de IPS, Antivírus e Anti-Spyware;

2.2.4.657. O gerenciamento deve possibilitar a criação e administração de políticas de Filtro de URL;

2.2.4.658. Permitir localizar quais regras um objeto está sendo utilizado;

2.2.4.659. Permitir criação de regras que fiquem ativas em horário definido;

2.2.4.660. A solução deve permitir o repositório de assinaturas de antivírus, IPS, filtragem da Web e filtragem de e-mail para otimizar a velocidade e o download centralizado de dispositivos gerenciados;

2.2.4.661. Deve ter a capacidade de exibir os resultados da auditoria de segurança dos dispositivos gerenciados;

2.2.4.662. Permitir backup das configurações e rollback de configuração para a última configuração salva;



- 2.2.4.663.** Deve possuir mecanismo de Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
- 2.2.4.664.** Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;
- 2.2.4.665.** Deve permitir que todos os gateways sejam controlados de forma centralizada utilizando apenas um servidor de gerência;
- 2.2.4.666.** A solução deve incluir uma ferramenta para gerenciar centralmente as licenças de todos os appliances controlados pela estação de gerenciamento, permitindo ao administrador atualizar licenças nos appliances através dessa ferramenta;
- 2.2.4.667.** A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances;
- 2.2.4.668.** Deve ser capaz de gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas;
- 2.2.4.669.** Deve permitir criar fluxos de aprovação na solução de gerência, onde um administrador possa criar todas as regras, mas com opção de serem aplicadas após aprovação de outro administrador;
- 2.2.4.670.** Possuir "wizard" na solução de gerência para adicionar os dispositivos via interface gráfica utilizando IP, login e senha dos mesmos;
- 2.2.4.671.** Permitir que eventuais políticas e objetos já presentes nos dispositivos sejam importados quando o mesmo for adicionado à solução de gerência;
- 2.2.4.672.** Permitir visualizar, a partir da estação de gerência centralizada, informações detalhadas dos dispositivos gerenciados, tais como hostname, serial, IP de gerência, licenças, horário do sistema e firmware;
- 2.2.4.673.** Possuir "wizard" na solução de gerência para instalação de políticas e configurações dos dispositivos;
- 2.2.4.674.** Permitir criar na solução de gerência templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração;
- 2.2.4.675.** Permitir criar scripts personalizados, que sejam executados de forma centralizada em um ou mais dispositivos gerenciados com comandos de CLI dos mesmos;
- 2.2.4.676.** Possuir histórico dos scripts executados nos dispositivos gerenciados pela solução de gerência;



2.2.4.677. Permitir configurar e visualizar balanceamento de links nos dispositivos gerenciados de forma centralizada;

2.2.4.678. Permitir criar vários pacotes de políticas que serão aplicados/associados à dispositivos ou grupos de dispositivos;

2.2.4.679. Deve permitir criar regras de NAT64 e NAT46 de forma centralizada;

2.2.4.680. Permitir criar regras anti DoS de forma centralizada;

2.2.4.681. Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;

2.2.4.682. Permitir criar, a partir da solução de gerência, VPNs entre os dispositivos gerenciados de forma centralizada, incluindo topologia (hub, spoke, dial-up), autenticações, chaves e métodos de criptografia;

2.2.4.683. Deve permitir o uso de DDNS em VPNs de forma centralizada.

2.2.4.684. Características Técnicas da Solução de Endpoint corporativo do tipo EDR:

2.2.4.685. A solução de EDR deve suportar a gestão de no mínimo 2.500 máquinas, simultaneamente e possuir gerenciamento WEB;

2.2.4.686. A solução ofertada não deve fazer uso de nenhum elemento na infraestrutura local, com exceção dos coletores nas estações e servidores gerenciados;

2.2.4.687. A solução proposta deve ser compatível com os seguintes sistemas operacionais Windows: XP SP2, 7, 8, 8.1, 10 e 11 (versões 32 e 64 bits);

2.2.4.688. A solução proposta deve ser compatível com os seguintes sistemas operacionais Windows Server: 2003 SP2, 2003 R2 SP2, 2008 SP1, 2008 R2 SP2, 2012, 2012 R2, 2016, 2019 e 2022;

2.2.4.689. A solução proposta deve ser compatível com os seguintes sistemas operacionais macOS: Big Sur (11), and Monterey (12) e Ventura (13);

2.2.4.690. A solução proposta deve ser compatível com os seguintes sistemas operacionais Linux: RedHat Enterprise Linux e CentOS 6.8+, 7.2+, 8+ e 9+; Ubuntu LTS 16.04.5+, 18.04, 20.04 e 22.04 server; Oracle Linux 6.10, 7.7+ e 8.2+; Amazon Linux AMI 2 2018; Open SUSE Leap 15.2; SUSE Linux Enterprise Server SLES v12 SP5 e v15; RedHat 9;

2.2.4.691. A solução proposta deve ser compatível com os seguintes ambientes de VDI (Virtual Desktop Infrastructure): VMware Horizons 6 e 7 e Citrix XenDesktop 7;

2.2.4.692. A solução proposta deve ter um consumo máximo de 350 MB de memória RAM;



2.2.4.693. A solução proposta deve ter um consumo médio de menos de 2% do uso da CPU;

2.2.4.694. A solução proposta deve ter um consumo máximo de 1 GB de espaço em disco;

2.2.4.695. A solução proposta deve oferecer suporte à implantação em massa por meio de ferramentas como MS System Center, JAMF e Satellite;

2.2.4.696. A solução proposta deve ter a capacidade de atualizar o terminal sem interação do usuário e sem exigir uma reinicialização;

2.2.4.697. A solução proposta deve ter proteção "Anti-violação" no Agente;

2.2.4.698. A solução proposta deve funcionar sem depender de assinaturas hash locais conhecidas para a detecção de arquivos maliciosos;

2.2.4.699. A solução proposta deve ser capaz de registrar em tempo real informações do processo e informações adicionais, como o conhecimento do usuário associado aos eventos;

2.2.4.700. A solução proposta deve ter a opção de definir a senha para desinstalar o agente no terminal;

2.2.4.701. A solução proposta deve ser capaz de gerar um instalador Windows pré-configurado. Esta configuração deve permitir a instalação sem a necessidade de interação ou configuração do usuário;

2.2.4.702. O coletor que será instalado nos terminais da solução proposta deve ser capaz de trabalhar por trás de um proxy;

2.2.4.703. A solução proposta deve ser capaz de funcionar no modo "offline" sem que o Agente esteja conectado à rede corporativa;

2.2.4.704. A solução proposta deve ser capaz de detectar processos em execução, inícios de processos, paradas de processos e interações entre processos;

2.2.4.705. A solução proposta deve ser capaz de detectar, eliminar e retornar ao seu valor inicial as alterações feitas por processos maliciosos no registro do PC;

2.2.4.706. A solução proposta deve ser capaz de detectar as solicitações de DNS enviadas do dispositivo;

2.2.4.707. A solução proposta deve ser capaz de detectar conexões de rede a partir do dispositivo;

2.2.4.708. A solução proposta deve ser capaz de detectar atividades suspeitas associadas a arquivos DLL;

2.2.4.709. A solução proposta deve ser capaz de incorporar inteligência de ameaças ao esquema de detecção;



2.2.4.710. A solução proposta deve ser capaz de incorporar as técnicas MITER ATT&CK no esquema de detecção e mostrar quais dessas técnicas foram utilizadas;

2.2.4.711. A solução proposta deve ter a capacidade de pesquisar ameaças nas estações do Windows usando indicadores de comprometimento (IOC), como: nome do arquivo e hash do arquivo, etc.;

2.2.4.712. A solução proposta deve ter a capacidade de pesquisar ameaças em estações Windows usando indicadores de comprometimento (IOC), como ações relacionadas a arquivos (Criação, Exclusão, Renomear);

2.2.4.713. A solução proposta deve ter a capacidade de pesquisar ameaças em estações Windows usando indicadores de comprometimento (IOC), como ações relacionadas a processos (Terminação de Processo, Criação de Processo, Carregamento de Executáveis);

2.2.4.714. A solução proposta deve ter a capacidade de pesquisar ameaças em estações Windows usando indicadores de comprometimento (IOC), como ações relacionadas ao uso da rede (Socket Connect, Socket Close, Socket Bind);

2.2.4.715. A solução proposta deve ter a capacidade de pesquisar ameaças em estações Windows usando indicadores de comprometimento (IOC), como ações relacionadas aos logs do Windows (Log de eventos);

2.2.4.716. A solução proposta deve ter a capacidade de pesquisar ameaças nas estações do Windows usando indicadores de comprometimento (IOC), como ações relacionadas ao registro do Windows (criação de chave, exclusão de chave, conjunto de valores);

2.2.4.717. A solução proposta deve ter a capacidade de realizar consultas de texto livre para filtrar as informações disponíveis para a caça de ameaças;

2.2.4.718. A solução proposta deve ter a capacidade de armazenar pesquisas realizadas para serem reutilizadas no futuro;

2.2.4.719. A solução proposta deve ter a capacidade de agendar pesquisas armazenadas;

2.2.4.720. A solução proposta deve identificar atividades maliciosas conhecidas;

2.2.4.721. A solução proposta deve ter a capacidade de receber atualizações diárias de inteligência;

2.2.4.722. A solução proposta deve ter a capacidade de categorizar os eventos detectados em diferentes categorias (Ex: Malicioso, Suspeito, Inconclusivo, Provavelmente Seguro);



2.2.4.723. A solução proposta deve ter a capacidade de coexistir com outras soluções de segurança de endpoint do tipo de antivírus tradicional ou de nova geração;

2.2.4.724. A solução proposta deve ter a capacidade de prevenir a execução de arquivos maliciosos;

2.2.4.725. A solução proposta deve incorporar um mecanismo de antivírus de última geração (Next-Generation Antivírus) baseado no kernel do sistema operacional, com capacidade de "Aprendizado de Máquina" (Machine Learning);

2.2.4.726. A solução proposta deve ter a capacidade de controlar dispositivos USB;

2.2.4.727. A solução proposta deve ter a capacidade de criar exceções para dispositivos USB com base no nome do dispositivo;

2.2.4.728. A solução proposta deve ter a capacidade de criar exceções para dispositivos USB com base no fornecedor do dispositivo;

2.2.4.729. A solução proposta deve ter a capacidade de criar exceções para dispositivos USB com base no número de série do dispositivo;

2.2.4.730. A solução proposta deve ter a capacidade de criar exceções para dispositivos USB com base em uma combinação de: nome do dispositivo, fornecedor, número de série;

2.2.4.731. A solução proposta deve ser capaz de bloquear o tráfego malicioso de exfiltração de dados;

2.2.4.732. A solução proposta deve ser capaz de bloquear o tráfego de comunicação malicioso para C&C (Comando e Controle);

2.2.4.733. A solução proposta deve ser capaz de impedir violações de segurança e tentativas de ransomware em tempo real;

2.2.4.734. A solução proposta deve ser capaz de evitar a criptografia causada por ransomware e modificação de arquivos ou registro de dispositivos, caso isso ocorra, a solução deverá restaurar os arquivos afetados/modificados para o seu estado original em tempo real;

2.2.4.735. A solução proposta deve permitir que as políticas nela contidas sejam modificadas permitindo vários estados tais como: ativo, desativado ou apenas criar "logs" para as regras de segurança contidas nestes;

2.2.4.736. A solução proposta deve ser capaz de ser configurada em modo de simulação onde nenhum bloqueio é feito, mas todas as atividades maliciosas são registradas;



2.2.4.737. A solução proposta deve ser capaz de permitir a modificação das regras de detecção de eventos maliciosos de forma que essas regras apenas armazenem um registro ou fiquem em modo de bloqueio;

2.2.4.738. A solução proposta deve ser capaz de permitir verificações periódicas dos arquivos contidos nos dispositivos com o Agente instalado;

2.2.4.739. A solução proposta deve permitir o isolamento automático do tráfego de rede de um dispositivo onde foi encontrada uma atividade causada por malware;

2.2.4.740. A solução proposta deve permitir alterar as políticas atribuídas de um dispositivo onde uma atividade causada por malware foi encontrada;

2.2.4.741. A solução proposta deve permitir o bloqueio de atividades realizadas por arquivos maliciosos;

2.2.4.742. A solução proposta deve ter a capacidade de criar exceções para processos com base na localização do arquivo (Caminho do Arquivo);

2.2.4.743. A solução proposta deve ter a capacidade de criar exceções para processos com base no destino do tráfego gerado pelo processo;

2.2.4.744. A solução proposta deve ter a capacidade de criar exceções para os processos baseados no usuário que o processo executou;

2.2.4.745. A solução proposta deve ter a capacidade de criar exceções manualmente para falsos positivos para marcar a atividade como um falso positivo e evitar a ocorrência de falhas futuras;

2.2.4.746. A solução proposta deve ter a capacidade de reclassificar automaticamente a atividade como um falso positivo e evitar a ocorrência de detecções semelhantes;

2.2.4.747. A solução proposta deve permitir a criação de exceções de eventos com base em endereços IP, aplicações e protocolos;

2.2.4.748. A solução proposta deve permitir um histórico dos eventos por no mínimo 6 meses;

2.2.4.749. A solução proposta deve armazenar metadados gerados pelos dispositivos para que possam ser usados em investigações forenses;

2.2.4.750. A solução proposta deve permitir a integração com plataformas SIEMs (Security Information and Event Management) através de um syslog;

2.2.4.751. A solução proposta deve ter a capacidade de obter instantâneos de memória ou "dumps" de memória que permitam a realização de processos forenses;

2.2.4.752. A solução proposta deve ter a capacidade de abrir tickets em plataformas de gerenciamento como ServiceNow e JIRA;



2.2.4.753. A solução proposta deve permitir a integração através de API onde tem a capacidade de entregar informações geradas em um evento como: endereço IP, nome do host, usuário, data / hora ocorrida, atividade suspeita, etc.) para permitir a integração via API;

2.2.4.754. A solução proposta deve ter a capacidade de encerrar um processo com base em sua classificação;

2.2.4.755. A solução proposta deve ter a capacidade de excluir um arquivo com base em sua classificação;

2.2.4.756. A solução proposta deve ser a capacidade de restaurar as configurações de registro básicas com base na classificação de atividade predefinida;

2.2.4.757. A solução proposta deve ter a capacidade de isolar os dispositivos infectados da rede.

2.2.4.758. A solução proposta deve ter a capacidade de restringir automaticamente o acesso do dispositivo à rede de acordo com a classificação (malicioso, suspeito, etc.) do processo detectado;

2.2.4.759. A solução proposta deve obter visibilidade total da cadeia de ataques e alterações maliciosas;

2.2.4.760. A solução proposta deve permitir a limpeza automática do dispositivo e reverter alterações maliciosas, mantendo o tempo de atividade do dispositivo;

2.2.4.761. A solução proposta deve permitir a assinatura de serviços opcionais de detecção e resposta a incidentes (Ex: serviços gerenciados de detecção e resposta);

2.2.4.762. A solução proposta deve permitir o envio de executáveis para análise em um sandbox, a fim de determinar se são maliciosos ou inofensivos;

2.2.4.763. A solução proposta deve possuir integração com Active Directory a fim de possibilitar a utilização de playbooks para contenção e resposta à incidentes de segurança;

2.2.4.764. A solução proposta deve fornecer vários mecanismos de proteção, incluindo o encerramento de um processo, a exclusão de um arquivo malicioso, o bloqueio de uma conexão de rede;

2.2.4.765. A solução proposta deve ter a capacidade de descobrir aplicativos que estão se comunicando através da rede e que representam risco para o terminal;

2.2.4.766. A solução proposta deve ter capacidade para realizar um patch virtual, através da restrição de acessos de comunicação nas aplicações vulneráveis;



2.2.4.767. A solução proposta deve permitir a redução das superfícies de ataque utilizando políticas de comunicação proativas baseadas no risco de acordo com o CVE e a qualificação ou reputação que uma aplicação possa ter;

2.2.4.768. A solução proposta deve ter a capacidade de impedir que aplicativos não autorizados se comuniquem pela rede;

2.2.4.769. A solução proposta deve ter a capacidade de criar políticas que tenham a capacidade de impedir a comunicação de aplicativos de acordo com a versão do aplicativo instalado;

2.2.4.770. A solução proposta deve ser capaz de detectar e identificar todas as aplicações nos dispositivos que se comunicam na rede;

2.2.4.771. A solução proposta deve ser capaz de fornecer informações sobre o uso de aplicativos de rede mostrando, por exemplo, quais dispositivos geram tráfego para um aplicativo;

2.2.4.772. A solução proposta deve ser capaz de visualizar e entregar informações sobre o uso dos aplicativos de rede mostrando informações como os destinos IP do tráfego gerado pelo aplicativo;

2.2.4.773. A solução proposta deve identificar e prevenir tentativas de perseguição de privilégios;

2.2.4.774. A solução proposta deve bloquear ataques de ransomware conhecidos;

2.2.4.775. A solução proposta deve detectar malware desconhecido como RAT (Trojan de acesso remoto) por meio das atividades do malware e não de uma assinatura;

2.2.4.776. A solução proposta deve proteger contra scripts Powershell maliciosos;

2.2.4.777. A solução proposta deve proteger contra scripts CScript maliciosos;

2.2.4.778. A solução proposta deve proteger contra macros maliciosas do Office;

2.2.4.779. A solução proposta deve ter controle sobre dispositivos USB;

2.2.4.780. A solução proposta deve ter a capacidade de descobrir dispositivos IOT não gerenciados na rede;

2.2.4.781. A solução proposta deve ter a capacidade de detectar dispositivos não gerenciados e protegidos pela solução com sistemas operacionais macOS / Linux / Windows;

2.2.4.782. A Solução deve conter políticas de segurança e playbooks básicos pré-definidos, sem que haja a necessidade de criação manual logo após a instalação da solução;



2.2.4.783. A solução proposta, caso oferecida em nuvem, deve estar em conformidade com o padrão da AICPA SOC;

2.2.4.784. A solução proposta deve estar em conformidade com o padrão GDPR;

2.2.4.785. O console de gerenciamento da solução proposta deve permitir a integração com o "Active Directory" para garantir o cumprimento dos requisitos da política de senhas da empresa;

2.2.4.786. O console de administração da solução proposta deve permitir o uso de autenticação de dois fatores (2FA) para acessá-la;

2.2.4.787. O console de administração da solução proposta deve permitir a integração com SAML para autenticação do usuário no console de gerenciamento;

2.2.4.788. O console de administração da solução proposta deve permitir o uso de funções granulares para administradores;

2.2.4.789. O console de administração da solução proposta deve permitir o gerenciamento de ambientes multilocatários;

2.2.4.790. O console de administração da solução proposta deve permitir o gerenciamento por meio da API Full Restful;

2.2.4.791. A solução proposta deve ser capaz de ser totalmente gerenciada na nuvem sem a necessidade de serviços locais;

2.2.4.792. A solução proposta deve ser capaz de ser gerenciada em uma arquitetura híbrida usando serviços locais complementados com outros na nuvem;

2.2.4.793. A solução proposta deve possuir integração nativa com soluções de controle de acesso;

2.2.4.794. A solução proposta deve possuir integração nativa com soluções de SIEM;
A solução proposta deve possuir integração nativa com soluções de firewall;

2.2.4.795. A solução proposta deve possuir integração nativa com com soluções Sandbox;

2.2.4.796. A solução proposta deve possuir integração nativa com com soluções de ATP;

2.2.4.797. O console de administração da solução proposta deve permitir a visualização dos eventos registrados nos dispositivos que requerem atenção;

2.2.4.798. O console de administração da solução proposta deve permitir a visualização da saúde dos Agentes instalados;

2.2.4.799. O console de administração da solução proposta deve permitir a desinstalação remota do Agente instalado nos dispositivos;



- 2.2.4.800.** O console de administração da solução proposta deve permitir a desativação / ativação remota do Agente instalado nos dispositivos;
- 2.2.4.801.** O console de administração da solução proposta deve permitir a atualização remota do Agente instalado nos dispositivos;
- 2.2.4.802.** O console de administração da solução proposta deve permitir a criação de relatórios executivos contendo um resumo que descreva os eventos de segurança e o status do sistema;
- 2.2.4.803.** O console de administração da solução proposta deve permitir a criação de grupos organizacionais de dispositivos nos quais cada grupo possa ter regras de proteção independentes dos demais;
- 2.2.4.804.** O console de administração da solução proposta deve permitir a exportação dos logs locais gerados pelos Agentes a partir do mesmo console;
- 2.2.4.805.** O console de administração da solução proposta deve permitir a criação de relatórios de inventário dos Agentes implantados contendo informações como: Endereço IP, Nome do Host, Sistema Operacional, Endereço MAC, Versão do Agente instalado, Status do Agente, último dia visto pelo console;
- 2.2.4.806.** O console de gerenciamento da solução proposta deve ter a visibilidade dos eventos gerados pelos dispositivos ou eventos de acordo com o processo executado;
- 2.2.4.807.** O console de administração da solução proposta deve permitir a integração de um SMTP externo para envio de alertas por e-mail;
- 2.2.4.808.** O console de administração da solução proposta deve permitir auditorias de alterações feitas por administradores / operadores. Essas auditorias também devem ser baixadas em formato CSV;
- 2.2.4.809.** A solução proposta deve exigir que uma senha seja desabilitada por um aplicativo de terceiros;
- 2.2.4.810.** A solução proposta deve permitir o isolamento de um dispositivo através da integração de um NAC de acordo com a categoria do evento detectado;
- 2.2.4.811.** A solução proposta deve permitir adicionar endereços IP maliciosos detectados em um ou mais firewalls remotos integrados;
- 2.2.4.812.** A solução proposta deve permitir a configuração de perfis nas informações coletadas para a função de caça a ameaças;
- 2.2.4.813.** A solução proposta deve permitir exclusões de informações que não serão coletadas na função de caça a ameaças;



2.2.4.814. A solução proposta deve ser certificada pela Microsoft como uma solução antivírus e ser capaz de se integrar com o Windows Security Center;

2.2.4.815. A solução proposta deve entregar informações geradas pelos serviços de inteligência para a tomada de decisão na nuvem sobre o evento detectado;

2.2.4.816. A solução proposta deve permitir que os serviços em nuvem recategorizem uma classificação de evento;

2.2.4.817. A solução proposta deve permitir que os administradores desabilitem as notificações para um evento de descoberta;

2.2.4.818. A solução proposta deve permitir que as funções de filtragem da web sejam realizadas bloqueando o acesso a páginas da web categorizadas como maliciosas.

2.2.4.819. Características Técnicas da Solução de WAF:

2.2.4.820. Deve ser do tipo appliance físico com software e recurso dedicado à função de Firewall de Aplicação (WAF);

2.2.4.821. Deve oferecer a funcionalidade de cluster de alta disponibilidade entre dois dispositivos no modo Ativo-Passivo e Ativo-Ativo, para que quando o principal falhar o tráfego possa continuar sendo processado;

2.2.4.822. Deve possuir throughput mínimo para tráfego HTTPS, com chave de 2048 bytes, de no mínimo 100 (cem) Mbps;

2.2.4.823. Devem introduzir latência inferior a 5 milissegundos, a fim de não impactar o desempenho das aplicações Web;

2.2.4.824. Deve suportar quantidade ilimitada de aplicações protegidas;

2.2.4.825. Deve possuir, no mínimo 4 (quatro) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;

2.2.4.826. Deve possuir fonte de alimentação bivolt (100/240V);

2.2.4.827. Deve possuir interface de console serial via RJ45 ou USB;

2.2.4.828. Deve possuir armazenamento mínimo SSD de 64 (sessenta e quatro) GB;

2.2.4.829. Deve suportar no mínimo 32 políticas de servidores;

2.2.4.830. Deve suportar no mínimo 256 grupos ou pools de servidores, e cada pool deve suportar no mínimo 1.000 membros;

2.2.4.831. Deve suportar no mínimo 1.000 IPs virtuais configurados e ativos simultaneamente;

2.2.4.832. Deve Possuir LEDs para a indicação do status e atividade das interfaces;

2.2.4.833. A solução deve possuir softwares específicos, e hardware dedicado para os itens de appliance físico, destinados à finalidade de Firewall de Aplicação Web



(WAF), bem como as licenças necessárias, para o seu funcionamento e proteção de servidores e aplicações Web;

2.2.4.834. Deve possuir garantia, suporte técnico, suporte a atualizações e estar licenciado com as funcionalidades descritas neste termo;

2.2.4.835. A solução deve ser capaz de ser implementada no modo Proxy (Transparente e Reverso), Passivo e Inline Transparente (Bridge);

2.2.4.836. A solução deve ser capaz de ser implementada com protocolo WCCP;

2.2.4.837. Suportar VLANs no padrão IEEE 802.1q;

2.2.4.838. Deve implementar o protocolo de negociação Link Aggregation Control Protocol (LACP) - IEEE 802.3ad;

2.2.4.839. Suportar endereçamento IPv4 e IPv6 nas interfaces físicas e virtuais (VLANs);

2.2.4.840. A solução ofertada deve possibilitar cluster de alta disponibilidade entre dois dispositivos no modo Ativo- Passivo e Ativo-Ativo, para que quando o principal falhar o tráfego possa continuar sendo processado;

2.2.4.841. A solução deve suportar a sincronização de configuração entre dois appliances iguais, com o objetivo de operar no modo ativo-ativo, com a distribuição de tráfego sendo realizada por balanceador de carga externo ou pela própria solução;

2.2.4.842. A solução deve suportar roteamento por política (policy route);

2.2.4.843. O sistema operacional / firmware deve suportar interface gráfica web para a configuração das funções do sistema operacional, utilizando navegadores disponíveis gratuitamente e protocolo HTTPS, e através de CLI (interface de linha de comando), acessando localmente, via porta de console, ou remotamente via SSH;

2.2.4.844. Deve possuir administração baseada em interface web HTTPS;

2.2.4.845. Possuir auto-complementação de comandos na CLI;

2.2.4.846. Possuir ajuda contextual na CLI;

2.2.4.847. A solução deve possuir Interface Gráfica com informações sobre o sistema Ex: (Informações do Cluster, hostname, número de série, modo de operação, tempo em serviço, versão do firmware);

2.2.4.848. Deverá ser possível visualizar através da interface gráfica de gerência informações de licenças e assinaturas;

2.2.4.849. Deve prover, na interface de gerência, as informações do sistema para cada gateway o consumo de CPU e estatísticas das conexões;

2.2.4.850. Deve ser possível visualizar na interface de gerência as informações de consumo de memória;



2.2.4.851. Deve ser possível visualizar na interface de gerência ou CLI as informações de utilização de disco de log;

2.2.4.852. O Deverá possuir ferramenta, na interface gráfica de gerência (dashboard) que permita visualizar os últimos logs de ataque detectados/bloqueados;

2.2.4.853. Deve prover as seguintes informações, na interface de gráfica de gerência: estatísticas de throughput HTTP em tempo real, estatísticas dos eventos de ataque detectados/bloqueados, estatísticas de requisições HTTP em tempo real e últimos logs de eventos do sistema;

2.2.4.854. Possuir na interface gráfica estatísticas de conexões concorrentes e por segundo, de políticas de segurança do sistema;

2.2.4.855. Possuir um painel de visualização com informações das interfaces de rede do sistema;

2.2.4.856. A configuração de administração da solução deve possibilitar a utilização de perfis;

2.2.4.857. Deve ser possível executar e restaurar backup via interface Web (GUI);

2.2.4.858. Deve ter a opção para criptografar o backup;

2.2.4.859. Deve ser possível executar e restaurar backup utilizando-se um ou mais dos seguintes protocolos: FTP, SFTP ou TFTP;

2.2.4.860. Deve ser possível instalar um firmware alternativo em disco e inicializá-lo em caso de falha do firmware principal;

2.2.4.861. Deve ter suporte ao protocolo de monitoração SNMP v1, SNMP v2c e SNMP v3;

2.2.4.862. Deve ser capaz de realizar notificações de eventos de segurança através de e-mail, traps SNMP e Syslog;

2.2.4.863. A solução deverá ter a capacidade de armazenar logs localmente em disco e em servidor externo via protocolo SYSLOG;

2.2.4.864. Ter a capacidade de armazenar logs em appliance remoto;

2.2.4.865. A solução deve ter a capacidade de enviar alertas por e-mail de eventos baseados em severidades e/ou categorias;

2.2.4.866. A solução deve possuir dados analíticos contendo localização geográfica dos clientes web;

2.2.4.867. A solução deve possuir dados analíticos, sendo possível visualizar a contagem total de ataques e percentual de cada país de origem, o volume total de tráfego em bytes e percentual de cada país de origem e o total de acessos (hits) e percentual de cada país de origem;



2.2.4.868. Deverá ter a capacidade de gerar relatórios detalhados baseados em tráfego/acessos/atividades do usuário;

2.2.4.869. Deve ter suporte a RESTful API para gerenciamento de configurações;

2.2.4.870. Os usuários devem ser capazes de autenticar através do cabeçalho de autorização HTTP / HTTPS;

2.2.4.871. Os usuários devem ser capazes de autenticar através de formulários HTML embutidos;

2.2.4.872. A solução deverá ser capaz de autenticar usuários através de certificados digitais pessoais;

2.2.4.873. Deve possuir base local para armazenamento e autenticação de contas de usuários;

2.2.4.874. A solução deve ter a capacidade de autenticar usuários em bases externas/remotas LDAP e RADIUS;

2.2.4.875. Os usuários devem ser capazes de autenticar através de contas de usuários em base remota NTLM;

2.2.4.876. A solução deve ser capaz de criar grupos de usuários para acessos semelhantes na autenticação;

2.2.4.877. Deverá ser capaz de identificar e bloquear ataques através de um banco de dados de assinaturas de vírus e IP reputation, atualizado de forma automática;

2.2.4.878. Deverá implementar recurso de machine learning, onde será permitido implementar proteção para um servidor ou grupo de servidores de aplicação web, de forma automatizada através da análise da utilização da aplicação, fazendo a descoberta da estrutura e padrões e padrões de uso, buscando separar o comportamento anormal do abusivo, detectando anomalias e tentativas de ataque;

2.2.4.879. Ter a capacidade de criação de assinaturas de ataque customizáveis;

2.2.4.880. Ter a capacidade de proteção para ataques do tipo Adobe Flash binary (AMF) protocol;

2.2.4.881. Ter a capacidade de proteção para ataques do tipo Botnet;

2.2.4.882. Ter a capacidade de proteção para ataques do tipo Browser Exploit Against SSL/TLS (BEAST);

2.2.4.883. A solução deverá possuir funcionalidade de proteção positiva contra ataques como acesso por força bruta;

2.2.4.884. Deve suportar detecção a ataques de Clickjacking;

2.2.4.885. Deve suportar detecção a ataques de alteração de cookie;

2.2.4.886. Identificar e prevenir ataques do tipo Credit Card Theft;



- 2.2.4.887.** Identificar e prevenir ataque Cross Site Request Forgery (CSRF);
- 2.2.4.888.** A solução deverá possuir funcionalidade de proteção positiva contra ataques como cross site scripting (XSS);
- 2.2.4.889.** Deve possuir proteção contra ataques de Denial of Service (DoS);
- 2.2.4.890.** Ter a capacidade de proteção para ataques do tipo HTTP header overflow;
- 2.2.4.891.** Ter a capacidade de proteção para ataques do tipo Local File inclusion (FLI);
- 2.2.4.892.** Ter a capacidade de proteção para ataques do tipo Man-in-the-middle (MITM);
- 2.2.4.893.** Ter a capacidade de proteção para ataques do tipo Remote File Inclusion (RFI);
- 2.2.4.894.** Ter a capacidade de proteção para ataques do tipo Server Information Leakage;
- 2.2.4.895.** Proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection);
- 2.2.4.896.** Ter a capacidade de proteção para ataques do tipo Malformed XML;
- 2.2.4.897.** Identificar e prevenir ataques do tipo Low-rate DoS;
- 2.2.4.898.** Prevenção contra Slow POST attack;
- 2.2.4.899.** Proteger contra ataques Slowloris;
- 2.2.4.900.** Ter a capacidade de proteção para ataques do tipo SYN flood;
- 2.2.4.901.** Ter a capacidade de proteção para ataques do tipo Forms Tampering;
- 2.2.4.902.** A solução deverá possuir funcionalidade de proteção positiva contra ataques de manipulação de campo escondido;
- 2.2.4.903.** Ter a capacidade de proteção para ataques do tipo Directory Traversal;
- 2.2.4.904.** Ter a capacidade de proteção do tipo Access Rate Control;
- 2.2.4.905.** Ter a habilidade de configurar proteção do tipo TCP SYN flood-style para prevenção de DoS para qualquer política, através de Syn Cookie e Half Open Threshold;
- 2.2.4.906.** Permitir configurar regras de bloqueio a métodos HTTP indesejados;
- 2.2.4.907.** Permitir que sejam configuradas regras de limite de upload por tamanho de arquivo;
- 2.2.4.908.** Deve permitir que o administrador bloqueie o tráfego de entrada e/ou tráfego de saída com base nos países, sem a necessidade de gerir manualmente os ranges de endereços IP correspondentes a cada país;



- 2.2.4.909.** Deve suportar a criação de políticas por geolocalização, permitindo que o tráfego de determinado país seja bloqueado;
- 2.2.4.910.** Permitir configurar listas negras de bloqueio e listas brancas de confiança, baseadas em endereço IP de origem;
- 2.2.4.911.** Permitir a liberação temporária ou definitiva (whitelist) de endereços IP bloqueados por terem originados ataques detectados pela solução;
- 2.2.4.912.** Deve permitir adicionar, automaticamente ou manualmente, em uma lista de bloqueio, os endereços IP de origem, de acordo com a base de IP Reputation;
- 2.2.4.913.** Ter a capacidade de Prevenção ao Vazamento de Informações (DLP), bloqueando o vazamento de informações de cabeçalho HTTP;
- 2.2.4.914.** Ter a funcionalidade de proteger o website contra ações de desfiguração (defacement), com restauração automática e rápida do site caso ocorra à falha;
- 2.2.4.915.** Ter a funcionalidade de antivírus para inspeção de tráfego e arquivos;
- 2.2.4.916.** Ter a capacidade de investigar e analisar todo o tráfego HTTP para atestar se está em conformidade com a respectiva RFC, bloqueando ataques e tráfego em não- conformidade;
- 2.2.4.917.** Deverá ser capaz de fazer aceleração de SSL, onde os certificados digitais são instalados na solução e as requisições HTTP são enviadas aos servidores sem criptografia;
- 2.2.4.918.** A solução deve ser capaz de funcionar como Terminador de sessões SSL para a aceleração de tráfego;
- 2.2.4.919.** Para SSL/TLS offload suportar no mínimo TLS 1.0, 1.1, 1.2 e 1.3;
- 2.2.4.920.** A solução deve ter a capacidade de armazenar certificados digitais de CA's;
- 2.2.4.921.** A solução deve ser capaz de gerar CSR para ser assinado por uma CA;
- 2.2.4.922.** A solução deve ser capaz de validar os certificados que são válidos e não foram revogados por uma lista de certificados revogados (CRL);
- 2.2.4.923.**
- 2.2.4.924.** A solução deve conter as assinaturas de robôs conhecidos como link checkers, indexadores de web, search engines, spiders e web crawlers que podem ser colocados nos perfis de controle de acesso, bem como resetar tais conexões;
- 2.2.4.925.** A solução deve ter um sistema de reputação de endereços IP públicos conhecidos como fontes de ataques DDoS, botnets, spammers, etc. Tal sistema deve ser atualizado automaticamente;



2.2.4.926. A solução deverá ser capaz de limitar o total de conexões permitidas para cada servidor real de um pool de servidores;

2.2.4.927. A solução deve permitir a customização ou redirecionar solicitações e respostas HTTP no HTTP Host, Request URL HTTP, HTTP Referer, HTTP Body e HTTP Location;

2.2.4.928. A solução deve permitir criar regras definindo a ordem em que as páginas devem ser acessados para prevenir ataques como cross-site request forgery (CSRF);

2.2.4.929. A solução deve ter a capacidade de definir restrições a métodos HTTP;

2.2.4.930. A solução deve ter a capacidade de proteger contra a detecção de campos ocultos;

2.2.4.931. Permitir que sejam criadas assinaturas customizadas de ataques e DLP, através de expressões regulares;

2.2.4.932. A solução deve incluir capacidade de atuar como um scanner de vulnerabilidades ou permitir a integração com scanners de vulnerabilidade de terceiros para diagnóstico e identificação de ameaças nos servidores web, software desatualizado e potenciais buffers overflows;

2.2.4.933. Deve gerar perfil de proteção automaticamente a partir de relatório em formato XML gerado por scanner de vulnerabilidade de terceiros;

2.2.4.934. A solução deve gerar um relatório da análise de vulnerabilidades no formato HTML;

2.2.4.935. A solução deve permitir a exclusão de URLs na análise de vulnerabilidades;

2.2.4.936. Deverá ser capaz de fazer compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;

2.2.4.937. Suportar redireção e reescrita de requisições e respostas HTTP;

2.2.4.938. Permitir redirecionar requisições HTTP para HTTPS;

2.2.4.939. Permitir reescrever a linha URL no cabeçalho de uma requisição HTTP;

2.2.4.940. Permitir reescrever o campo "Host:" no cabeçalho de uma requisição HTTP;

2.2.4.941. Permitir reescrever o campo "Referer:" no cabeçalho de uma requisição HTTP;

2.2.4.942. Permitir redirecionar requisições para outro web site;

2.2.4.943. Permitir enviar resposta HTTP 403 Forbidden para requisições HTTP;

2.2.4.944. Permitir reescrever o parâmetro "Location:" no cabeçalho HTTP de uma resposta de redireção HTTP de um servidor web;



- 2.2.4.945.** Permitir reescrever o corpo ("body") de uma resposta HTTP de um servidor web;
- 2.2.4.946.** Permitir adicionar o campo X-Forwarded-For para identificação do endereço real do cliente quando no modo de proxy reverso;
- 2.2.4.947.** A solução deve suportar regras para definir se as solicitações HTTP serão aceitas com base na URL e a origem do pedido e, se necessário, aplicar uma taxa específica de transferência (rate limit);
- 2.2.4.948.** A solução deve suportar o mecanismo de combinação de controle de acesso e autenticação utilizando mecanismos como HTML Form, Basic e Suporte a SSO, métodos como LDAP e RADIUS para consultas e integração dos usuários da aplicação;
- 2.2.4.949.** Possuir capacidade de caching para aceleração web;
- 2.2.4.950.** Deve permitir ao Administrador a criação de novas assinaturas e/ou alteração de assinaturas já existentes;
- 2.2.4.951.** A solução deve incluir funcionalidade de balanceamento de carga entre servidores web;
- 2.2.4.952.** Deve ter a habilidade de configurar portas não-padrão para aplicação web HTTP e HTTPS;
- 2.2.4.953.** Ter a capacidade de balancear/distribuir tráfego e rotear o conteúdo através de vários servidores web;
- 2.2.4.954.** A solução deve permitir criar grupos de servidores (Server Farm / Pool) para distribuir as conexões dos usuários;
- 2.2.4.955.** Suportar algoritmo Round Robin para balanceamento de carga de servidores;
- 2.2.4.956.** Suportar algoritmo Weighted Round Robin para balanceamento de carga de servidores;
- 2.2.4.957.** Suportar algoritmo Least Connections para balanceamento de carga de servidores;
- 2.2.4.958.** A solução deve ser capaz de criar servidores virtuais que definem a interface de rede/bridge e endereço IP por onde o tráfego destinado ao Server Pool é recebido;
- 2.2.4.959.** Os servidores virtuais devem entregar o tráfego à um único servidor web e também possuir a opção de distribuir as sessões/conexões entre os servidores web do Server Pool;



- 2.2.4.960.** Deve ser possível especificar o número máximo de conexões TCP simultâneas para um determinado servidor membro do Server Pool;
- 2.2.4.961.** Permitir teste de disponibilidade de servidor web através do método TCP;
- 2.2.4.962.** Permitir teste de disponibilidade de servidor web através do método ICMP ECHO_REQUEST (ping);
- 2.2.4.963.** Permitir teste de disponibilidade de servidor web através do método TCP Half Open;
- 2.2.4.964.** Permitir teste de disponibilidade de servidor web através do método TCP SSL;
- 2.2.4.965.** Permitir teste de disponibilidade de servidor web através do método HTTP;
- 2.2.4.966.** Permitir teste de disponibilidade de servidor web através do método HTTPS;
- 2.2.4.967.** Nos testes de disponibilidade HTTP e HTTPS, permitir indicar a URL exata a ser testada;
- 2.2.4.968.** Nos testes de disponibilidade HTTP e HTTPS, permitir escolher entre os métodos HEAD, GET e POST;
- 2.2.4.969.** Nos testes de disponibilidade HTTP e HTTPS, permitir indicar o nome do campo HTTP "host" a ser testado;
- 2.2.4.970.** Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Host";
- 2.2.4.971.** Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "URL";
- 2.2.4.972.** Suportar roteamento das requisições dos clientes web baseado "Parâmetro HTTP";
- 2.2.4.973.** Suportar roteamento das requisições dos clientes web baseado "Referer";
- 2.2.4.974.** Suportar roteamento das requisições dos clientes web baseado "Endereço IP de Origem";
- 2.2.4.975.** Suportar roteamento das requisições dos clientes web baseado "Cabeçalho";
- 2.2.4.976.** Suportar roteamento das requisições dos clientes web baseado "Cookie";
- 2.2.4.977.** Suportar roteamento das requisições dos clientes web baseado em conteúdo HTTP, através de "Valor de campo do Certificado X509";
- 2.2.4.978.** Implementar Cache de Conteúdo para HTTP, permitindo que objetos sejam armazenados e requisições HTTP sejam respondidas diretamente pela solução;



2.2.4.979. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por endereço IP de origem;

2.2.4.980. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência analisando qualquer parâmetro do header HTTP;

2.2.4.981. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência analisando a URL acessada;

2.2.4.982. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por cookie - método cookie insert e cookie rewrite;

2.2.4.983. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por embedded cookie (cookie original mais porção randômica);

2.2.4.984. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em Reescrita de Cookie;

2.2.4.985. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em Cookie Persistente;

2.2.4.986. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em ASP Session ID;

2.2.4.987. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em PHP Session ID;

2.2.4.988. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência baseada em JSP Session ID;

2.2.4.989. A solução deverá ser capaz de balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência por sessão SSL;

2.2.4.990. Fornecer proteção para a comunicação API, sejam elas implementadas usando XML, JSON API ou RESTful API;



- 2.2.4.991.** Permitir a utilização de arquivos de esquema JSON para verificar o conteúdo JSON em solicitações HTTP, a fim de determinar o conteúdo aceitável e validar se o conteúdo está bem formado;
- 2.2.4.992.** Permitir definir a limitação de parametros JSON tais como total de dados, tamanho da chave, total de chaves, entre outros;
- 2.2.4.993.** Permitir ações do tipo alertar, bloquear, bloquear temporariamente, redirecionar ou responder com erro 403;
- 2.2.4.994.** Permitir definir o nível de severidade dos logs das ações;
- 2.2.4.995.** Permitir a utilização de arquivos de esquema XML para verificar o conteúdo XML em solicitações HTTP, a fim de determinar o conteúdo aceitável e validar se o conteúdo está bem formado;
- 2.2.4.996.** Permitir definir a limitação de parametros XML tais como total de atributo, tamanho do nome do atributo, tamanho CDATA, entre outros;
- 2.2.4.997.** Permitir definir elementos proibidos XML tais como entidade externa, XInclude, local do esquema, entre outros;
- 2.2.4.998.** Permitir definir o seguinte formato do esquema: SOAP ou XML;
- 2.2.4.999.** Permitir ações do tipo alertar, bloquear, bloquear temporariamente, redirecionar ou responder com erro 403;
- 2.2.4.1000.** Permitir definir o nível de severidade dos logs das ações;
- 2.2.4.1001.** Fornecer suporte a proteção OpenAPI;
- 2.2.4.1002.** Permitir o upload de arquivo de descrição OpenAPI, e bloquear as solicitações que não correspondam às definições do arquivo;
- 2.2.4.1003.** Suportar a proteção de API Movei;
- 2.2.4.1004.** Permitir a verificação de flags de API móvel e com a regra de proteção de API configuradas, executar as ações definidas na regra de proteção;
- 2.2.4.1005.** Permitir ações do tipo alertar, bloquear, bloquear temporariamente, entre outras;
- 2.2.4.1006.** Permitir definir o nível de severidade dos logs das ações;
- 2.2.4.1007.** Suportar as funções de API gateway;
- 2.2.4.1008.** Suportar gerenciamento de usuários API;
- 2.2.4.1009.** Suportar verificação de chave API;
- 2.2.4.1010.** Suportar controle de acesso API;
- 2.2.4.1011.** Suportar controle de limite de taxa;
- 2.2.4.1012.** Suportar reescrita de chamada de API;



2.2.4.1013. Permitir definir usuários de API para restringir o acesso a APIs com base em chaves de API;

2.2.4.1014. Permitir a restrição baseada em endereçamento IP;

2.2.4.1015. Permitir a restrição baseada em referenciadores HTTP;

2.2.4.1016. Permitir a criação de grupos de usuários;

2.2.4.1017. Permitir restringir o acesso à API através de regras envolvendo verificação de chave API, transferência de chave API, agrupamento de usuários API, configuração de subURL e ações específicas de qualquer violação de chamada API;

2.2.4.1018. Características Técnicas da Solução de Access Point corporativo:

2.2.4.1019. Ponto de acesso (AP) que permita acesso dos dispositivos à rede através da wireless e que possua todas as suas configurações centralizadas em controlador wireless;

2.2.4.1020. Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;

2.2.4.1021. Deve identificar automaticamente o controlador wireless ao qual se conectará;

2.2.4.1022. Deve permitir ser gerenciado remotamente através de links WAN;

2.2.4.1023. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;

2.2.4.1024. Deve possuir capacidade tri-band com rádios 2.4GHz, 5GHz e 6GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;

2.2.4.1025. O ponto de acesso deva funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (WIDS/WIPS) em tempo real e com operação 24x7;

2.2.4.1026. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;

2.2.4.1027. Deve permitir a conexão de no mínimo 512 (quinhentos e doze) clientes por rádio simultaneamente;

2.2.4.1028. Deve possuir 2 (duas) interfaces Ethernet padrão sendo uma 100M/1000M/2.5G/5.0G Base-T RJ45 e outra serial RS-232 RJ45;

2.2.4.1029. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;



2.2.4.1030. Deve ser compatível com o padrão UL 2043, regulando os componentes dos materiais com o intuito de proteger contra danos causados por fogo, bem como pela fumaça;

2.2.4.1031. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;

2.2.4.1032. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at. Adicionalmente deve possuir entrada de alimentação 12VDC;

2.2.4.1033. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless;

2.2.4.1034. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;

2.2.4.1035. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve

2.2.4.1036. suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;

2.2.4.1037. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;

2.2.4.1038. Deve permitir operação em modo Mesh;

2.2.4.1039. Deve possuir potência de irradiação mínima de 22dBm em ambas as frequências;

2.2.4.1040. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 2400 Mbps em um único rádio;

2.2.4.1041. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);

2.2.4.1042. Deve suportar OFDMA;



2.2.4.1043. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2,4, 5 e 6GHz servindo clientes wireless 802.11ax;

2.2.4.1044. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;

2.2.4.1045. Deve suportar BSS Coloring;

2.2.4.1046. Deve suportar operação em 2.4GHz com canais de 20 e 40MHz;

2.2.4.1047. Deve suportar operação em 5GHz com canais de 20, 40, 80 e 160MHz;

2.2.4.1048. Deve suportar operação em 6GHz com canais de 20, 40, 80, 160 e 320MHz;

2.2.4.1049. Deve possuir sensibilidade mínima de -93dBm quando operando em 5 e 6GHz com MCS0 (HT20);

2.2.4.1050. Deve possuir antenas internas ao equipamento com ganho mínimo de 4.2 dBi em 2.4GHz e 5GHz e 5.1 dBi para 6GHz;

2.2.4.1051. Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;

2.2.4.1052. Em conjunto com o controlador wireless, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4, 5 e 6 GHz;

2.2.4.1053. Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz;

2.2.4.1054. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;

2.2.4.1055. Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS);

2.2.4.1056. Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 24 (vinte e quatro) SSIDs com operação simultânea;

2.2.4.1057. Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);

2.2.4.1058. Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3;

2.2.4.1059. Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;



2.2.4.1060. Deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP- TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP- AKA, EAP-FAST;

2.2.4.1061. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

2.2.4.1062. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;

2.2.4.1063. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

2.2.4.1064. Deve implementar o padrão IEEE 802.11e;

2.2.4.1065. Deve implementar o padrão IEEE 802.11h;

2.2.4.1066. Deve implementar o padrão IEEE 802.3az;

2.2.4.1067. Deve suportar ser gerenciado via SNMP;

2.2.4.1068. Deve suportar consultas via REST API;

2.2.4.1069. Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar todos os acessórios para fixação;

2.2.4.1070. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 50° C;

2.2.4.1071. Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar;

2.2.4.1072. Deve possuir indicadores luminosos (LED) para indicação de status;

2.2.4.1073. O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;

2.2.4.1074. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste deverão ser fornecidos;

2.2.4.1075. Deve possuir certificado emitido pela Wi-Fi Alliance;

2.2.4.1076. Deve estar homologado pela ANATEL na data de execução do pregão;

2.2.4.1077. Características Técnicas da Solução de Captive Portal:

2.2.4.1078. Fornecimento de solução de software para autenticação de acesso, captação de dados de perfil e informações comportamentais dos usuários, inteligência



de dados, além da veiculação de campanhas de marketing, relacionamento e fidelização através do Wi-Fi;

2.2.4.1079. O software deve funcionar através da disponibilização de licenças para uso, que são ativadas para uso nos APs (access points). A aplicação deve operar por meio de servidores em nuvem e atuar no momento da autenticação do usuário à rede, via captive portal. Além do captive portal, deverá ser disponibilizado também, acesso à plataforma web, que disponibilizará todos os dados e informações coletadas, em tempo real. O sistema deve conter as seguintes funcionalidades:

2.2.4.1080. Veiculação de mídias, no formato mobile e desktop, através do Wi-Fi: Banners com botões interativos (01 ou 02 botões, pesquisas de múltipla escolha), campo aberto, vídeos, pesquisas quantitativas, qualitativas e pesquisas NPS;

2.2.4.1081. Segmentação das campanhas com base na localização por grupo, local, ou aparelho, data de veiculação, dia da semana, horário do dia, sexo e idade dos usuários e outros;

2.2.4.1082. Captação de informações e dados cadastrais através do Wi-Fi: Nome completo, e-mail, data de nascimento, sexo, telefone, entre outros que desejarem, assim como o “opt-in” do usuário nos Termos de Uso;

2.2.4.1083. Captação de dados e informações de comportamento do usuário através do Wi-Fi: Período médio de conexão, quantidade de acessos, quantidade de novos usuários cadastrados, frequência de acessos, IP, MAC Address, tempo em tela, cliques, viewability, impressões, engajamento, rejeição e outros;

2.2.4.1084. Canal de comunicação: Ambiente privado para envio de sugestões e comentários dos usuários;

2.2.4.1085. Redirecionamento para website de escolha após a liberação do acesso;

2.2.4.1086. Sistema web: com área de visualização, em tempo real, de relatórios e gráficos com os dados e as informações supracitadas;

2.2.4.1087. Integração com sistemas específicos, API Pública e Webhook: para envio automatizado dos leads impactados pelas campanhas veiculadas, com objetivo de disparo de e-mail marketing e/ou outras ações de CRM;

2.2.4.1088. Exportação dos dados captados através de planilhas de eletrônicas para alimentar outros sistemas e/ou base de dados;

2.2.4.1089. Módulo de Gerenciamento de Usuários: Gestão de múltiplas contas de usuários que terão acesso à plataforma web com controle de permissões de ações e locais;



2.2.4.1090. Módulo de Gerenciamento de Locais: Gestão dos Locais, grupos de locais e access points;

2.2.4.1091. Gestão de Rede Interna: Autenticação via voucher, SSO (Single-sign-on), LDAP, SAML, integração com Active Directory e outros métodos;

2.2.4.1092. Deverá homologar no mínimo os seguintes equipamentos: Aruba, Aerohive, Extreme, Cambium Networks, Meraki, Cisco, Fortinet, Huawei, Intelbras, Mikrotik, Ruckus, TP Link, Ubiquiti, GrandStream, Tanaza, Enterasys, Motorola, pfSense, Xirrus, Zyxel, Teltonika, Draytek, Ruijie, Edgecore, com a possibilidade de homologação de outros equipamentos desde que possuam certificado SSL;

2.2.4.1093. Deverá possibilitar integração com os rastreadores Meta Pixel e Google Tag, onde através de sua configuração ser possível realizar um remarketing automatizado através de anúncios nas plataformas compatíveis (Instagram, Facebook, YouTube e etc), dos usuários que acessaram o Wi-Fi.

2.2.4.1094. O escopo deverá abranger uma solução de software de captive portal proprietária, hospedada em nuvem, compatível com o formato mobile e desktop, que irá funcionar localmente, dentro de uma infraestrutura de redes composta por roteadores e/ou access points Wi-Fi, podendo possuir também equipamentos como switches, controladoras, firewalls, entre outros;

2.2.4.1095. O escopo também deverá abranger uma plataforma Web, que possui conexão em tempo real com o servidor, para gestão centralizada de usuários, pontos de acesso, locais, campanhas de publicidade, voucher, entre outros;

2.2.4.1096. A plataforma deverá ser compatível nativamente com roteadores, sendo eles: Aruba, Aerohive, Extreme, Cambium Networks, Meraki, Cisco, Fortinet, Huawei, Intelbras, Mikrotik, Ruckus, TP Link, Ubiquiti, GrandStream, Tanaza, Enterasys, Motorola, pfSense, Xirrus, Zyxel, Teltonika, Draytek, Ruijie, Edgecore e equipamentos que possuem certificado SSL;

2.2.4.1097. Deverá possuir processo de liberação da autenticação via protocolo Radius ou através de API sobre SSL;

2.2.4.1098. Deverá registrar as seguintes informações de Mac do Equipamento do usuário conectado, horário do momento que o usuário se conectou, informações relacionadas ao tipo de aparelho do usuário e método de envio dos dados do usuário;

2.2.4.1099. Deve possibilitar uso de ACL's que farão o controle do tráfego, liberando apenas os endereços necessários para o funcionamento da plataforma, antes do usuário ter efetuado a autenticação na plataforma;



2.2.4.1100. Deve ser possível a liberação da autenticação para usuários específicos ou internos ao local;

2.2.4.1101. Ter a possibilidade de implementar Vlan para gerência de rede;

2.2.4.1102. Possibilitar trabalhar com protocolos de roteamento e redes privadas (com NAT ativo);

2.2.4.1103. A plataforma deverá utilizar o conceito de conta para definir uma empresa ou organização que irá utilizar a ferramenta, sendo que as contas serão gerenciadas única e exclusivamente pelos administradores da plataforma;

2.2.4.1104. O conceito de usuário deverá ser aplicado para definir um indivíduo que pertence a uma organização e poderá ter acesso a plataforma através de login e senha;

2.2.4.1105. O acesso à plataforma deverá ser realizado através de login e senha, sendo o login um email válido e único em toda a plataforma;

2.2.4.1106. Toda conta deverá possuir um usuário principal definido como usuário máster;

2.2.4.1107. Para a criação de uma conta, as informações de Razão Social, CNPJ, endereço, contato principal e email do usuário master deverão ser obrigatórias;

2.2.4.1108. Ao criar uma conta o sistema deverá enviar um e-mail de boas-vindas ao usuário master com um link que possibilitará a definição da senha de acesso;

2.2.4.1109. A função de recuperação de senha deverá enviar um link para definir uma nova senha para o e-mail do usuário cadastrado na plataforma;

2.2.4.1110. Todos os serviços deverão ser em containers, onde serão utilizados o Kubernetes para orquestração deles. Nele deverá ter configurações de zero time update e garantia mínima de containers daquele serviço funcionando independente da máquina que tiverem recursos na infraestrutura no momento;

2.2.4.1111. Todo o processo deverá ser criado para prover segurança e evitar potenciais falhas, além de possibilitar um rollback sem perder os dados, caso seja necessário;

2.2.4.1112. Todos os dados do sistema deverão ser criptografados e possuírem camadas de segurança de acordo com a sensibilidade de cada dado e/ou processo/operação;

2.2.4.1113. A plataforma deverá permitir que uma conta possua mais de um usuário. Isso possibilitará criar uma hierarquia de usuários, onde determinado usuário de nível superior poderá gerenciar todos os usuários que estão abaixo de sua posição na árvore;



2.2.4.1114. Deverá ser possível segmentar os usuários por nível de cargo e os administradores serão personalizáveis;

2.2.4.1115. Para cadastrar um novo usuário será obrigatório informar um nome e um e-mail, sendo que o e-mail deverá ser o login de acesso;

2.2.4.1116. Deverá ser possível realizar o upload de um avatar para o usuário. Este avatar irá ser apresentado na listagem de campanhas para melhor identificar o criador da mesma;

2.2.4.1117. A edição do usuário deverá permitir alterar as informações de nome e e-mail. Também deverá ser possível reenviar o e-mail de boas-vindas para os usuários que ainda não acessaram o sistema e obter o link para a redefinição de senha, que pode ser útil caso ocorra algum problema no envio do e-mail de boas-vindas;

2.2.4.1118. Deverá ser possível realizar a exclusão de um usuário. Esta operação deverá transferir todos os itens de sistema criados pelo usuário, como por exemplo campanhas, para seu superior ou para o usuário máster, caso não exista um superior;

2.2.4.1119. A plataforma deverá permitir liberar ou restringir determinadas operações através das permissões de sistema, conforme a seguir:

2.2.4.1120. Visualizar Estatísticas;

2.2.4.1121. Gerenciar API;

2.2.4.1122. Visualizar Cadastros;

2.2.4.1123. Gerenciar Locais;

2.2.4.1124. Gerenciar Integrações;

2.2.4.1125. Visualizar Conexões;

2.2.4.1126. Visualizar Campanhas;

2.2.4.1127. Visualizar Auditoria;

2.2.4.1128. Criar Campanhas;

2.2.4.1129. Gerenciar Usuários;

2.2.4.1130. Gerenciar Comentários.

2.2.4.1131. A plataforma deverá permitir liberar ou restringir a gerência de determinados locais, para que cada usuário possa visualizar apenas os dados e informações dos locais de sua gerência, definidos pelo usuário máster;

2.2.4.1132. Um local deverá ser representado por um espaço físico onde a ferramenta de captive portal irá atuar. Para cadastrar um local deverá ser necessário informar um nome que identifique o local, o endereço (CEP, rua, número, complemento, bairro, cidade e estado) e o tempo que o usuário irá usufruir da conexão com a Internet após ser liberado;



2.2.4.1133. Deverá ser possível configurar no local os tipos de logins que serão aceitos quando um usuário realizar um acesso no captive portal (Formulário ou redes sociais);

2.2.4.1134. Os locais poderão ser agrupados com o uso de grupos de locais. Estes poderão ser compostos por locais e outros grupos de locais. Para criar um grupo de local deverá ser necessário informar um nome para identificação do mesmo;

2.2.4.1135. Um aparelho deverá representar um ponto de acesso dentro de um local, que irá propagar o sinal de Wi-Fi e irá permitir a conexão de um ou mais usuários. Para cadastrar um aparelho deverá ser necessário informar um nome que identifique o aparelho dentro do local, qual seu tipo (fabricante/firmware) e qual sua chave de ativação, que no caso será o MAC Address do equipamento;

2.2.4.1136. Os aparelhos poderão ser agrupados com o uso de um grupo de aparelhos dentro de determinado local. Estes poderão ser compostos por aparelhos e outros grupos de aparelhos. Para criar um grupo de aparelho deverá ser necessário informar um nome para identificação do mesmo;

2.2.4.1137. A plataforma deverá permitir a criação de no mínimo 11 níveis de hierarquia de locais ou grupos, onde os aparelhos podem estar inseridos. Deverá ser possível criar grupos vinculados ou grupos isolados;

2.2.4.1138. Em cada aparelho deverá ser possível visualizar o status de conexão, sendo eles: Ativo, Inativo e Desconectado;

2.2.4.1139. Uma campanha é uma publicidade que será apresentada no momento em que o usuário se conectar ao ponto de acesso. Ela deverá ser composta por telas com imagens, vídeos e botões que chamamos de interações;

2.2.4.1140. Toda campanha deverá possuir um nome para identificação, um período de veiculação e uma página de pós autenticação que será apresentada após o usuário realizar o processo de liberação no captive portal, lembrando que a página de pós autenticação só será apresentada caso o equipamento do usuário (smartphone, tablet ou computador) possuir a funcionalidade de redirecionamento após liberação;

2.2.4.1141. A plataforma deverá permitir o agendamento das campanhas de acordo com um determinado período de tempo. Podendo ser programada para início em data futura ou início imediato. As datas e dias da semana podem ou não ser aleatórios;

2.2.4.1142. O modelo de agendamento deverá permitir múltiplos agendamentos, sem qualquer tipo de limite. Todos os agendamentos podem ser segmentados de acordo com os grupos ou locais criados na plataforma;



2.2.4.1143. Todas as campanhas deverão possibilitar serem pré-visualizadas no sistema antes da ativação;

2.2.4.1144. A plataforma deverá permitir que o usuário segmente a campanha. O gerenciamento deverá ser feito de forma centralizada ou dividida por determinados usuários. Esta segmentação poderá ser feita por:

2.2.4.1145. Dias da semana;

2.2.4.1146. Horários do dia;

2.2.4.1147. Sexo do usuário;

2.2.4.1148. Faixa etária;

2.2.4.1149. Locais, pontos e aparelhos (equipamentos);

2.2.4.1150. Regiões;

2.2.4.1151. Cidades;

2.2.4.1152. Clusters ou grupos definidos no sistema;

2.2.4.1153. Dentre outras segmentações de público.

2.2.4.1154. As campanhas seguem os grupos de pastas criados na segmentação de locais e permitem até 11 níveis de hierarquia. As ativações podem ser realizadas em todos os equipamentos da rede selecionando apenas o grupo geral, com uma única operação ou em grupos selecionados;

2.2.4.1155. As interações que compõem uma campanha podem ser de 4 tipos:

2.2.4.1156. Banner: interação com um ou dois botões clicáveis;

2.2.4.1157. Pesquisa Objetiva Quantitativa: apresenta uma pergunta e a possibilidade de até no máximo 6 opções de resposta;

2.2.4.1158. Pesquisa Escrita: apresenta uma pergunta e a resposta é feita através de um campo em texto, podendo ser aberto ou com número de caracteres restrito;

2.2.4.1159. Pesquisa NPS: apresenta uma pergunta e a possibilidade de o usuário escolher um valor entre 0 (zero) e dez (10);

2.2.4.1160. Todos os tipos de interações devem permitir o upload de uma imagem de fundo nos formatos JPG e PNG, assim como a possibilidade de personalização de cores dos botões;

2.2.4.1161. No formato de interação vídeo, a interação deve permitir o upload de um vídeo com áudio no formato MP4, WMV ou AVI, além de possibilidade de inserção de link de plataformas de vídeos. As interações podem ser antes ou após o cadastro;

2.2.4.1162. O tamanho limite dos arquivos deve ser de no máximo 20Mb e a plataforma deve permitir o envio de múltiplos arquivos;



2.2.4.1163. Todas as campanhas devem ser altamente customizáveis, sendo possível editar cores, mudar plano de fundo, logo, editar textos, fontes e ainda o tamanho das letras. O módulo de campanhas deve ser feito para que o cliente final possa personalizá-lo de acordo com a sua identidade visual e as suas diretrizes de design;

2.2.4.1164. Deve ser possível criar um fluxo de navegação entre as interações da campanha com base na ação do usuário que está executando a campanha, porém esta navegação restringe a visualização de até no máximo 3 interações por campanha no momento da execução da campanha;

2.2.4.1165. Uma campanha deverá possibilitar ser apresentada uma única vez ou várias vezes por usuário. Esta função deve ser definida pelo atributo “repetir”, que poderá ser ativado ou não;

2.2.4.1166. A plataforma deve permitir que uma campanha possa ser ativada ou não através de uma flag de ativação, facilitando o controle de veiculação da mesma;

2.2.4.1167. Para garantir a confiabilidade das estatísticas de visualização de uma campanha, após a mesma ser veiculada, não deverá ser mais possível editar suas interações, porém será possível editar o nome, a data de veiculação e os filtros de segmentação da mesma, incluindo os locais que a mesma será veiculada;

2.2.4.1168. Uma campanha poderá ser excluída, porém seus dados de acesso deverão permanecer nas estatísticas;

2.2.4.1169. No gerenciamento de campanhas deverá ser possível definir a ordem que as mesmas serão apresentadas para um usuário;

2.2.4.1170. Os conteúdos deverão ser agendados mesmo sem a disponibilidade de internet, sendo atualizados assim que a conexão for reestabelecida;

2.2.4.1171. O sistema deverá possuir um módulo específico para estabelecimentos que desejam monetizar a sua rede ou comercializar o espaço de mídia através de anúncios de terceiros. Neste caso, deverá ser criado um login específico, vinculando aquele anunciante ao determinado local ou locais definidos pelo cliente final, onde suas campanhas serão veiculadas normalmente;

2.2.4.1172. O processo de liberação deverá ser realizado por captive portal, iniciando no momento em que usuário se conecta a um dos pontos de acesso configurado e registrado na plataforma;

2.2.4.1173. A veiculação das mídias ou do conteúdo poderá ocorrer no pré-cadastro ou pós- cadastro;



2.2.4.1174. O redirecionamento inicial para o captive portal dependerá do modelo do dispositivo do usuário e da versão do mesmo, podendo existir alguns casos onde ocorra falha ao iniciar o processo. Neste caso, deverá ser possível criar um botão especial, com um CTA (call-to-action) para uma URL específica, que poderá ser mudada com base em campanhas específicas ou até mesmo grupos. A posição do botão pode ser definida no momento da criação da campanha;

2.2.4.1175. Para acesso ao hotspot, deverá ser possível habilitar dois formatos de login: Acesso via base externa de cadastro e acesso como convidado;

2.2.4.1176. Acesso via base externa: Deverá ser possível importar uma base de cadastros ou integrá-los à uma base já existente, para que colaboradores ou grupo previamente cadastrado acessem automaticamente a partir do seu CPF ou login e senha;

2.2.4.1177. Para os demais usuários, deverá ser necessário realizar o cadastro na plataforma no momento do acesso, informando seus dados pessoais. Alguns dados que podem ser requeridos são: nome, e-mail, data de nascimento, sexo, telefone e CPF, por exemplo. Este formulário deverá ser personalizável de acordo com a necessidade da empresa contratante;

2.2.4.1178. Após o cadastro, o usuário deverá ser obrigado a aceitar os termos de uso da plataforma. Na etapa de aceite, ele deverá visualizar os termos de uso e clicar sobre o opt-in para permitir o uso das informações para fins de marketing;

2.2.4.1179. Caso o usuário já possua um cadastro na plataforma, o mesmo deverá ser direcionado para a execução da campanha após conectar-se no ponto de acesso através do login automático. O login deverá ser feito também utilizando apenas o e-mail ou CPF do usuário, não havendo necessidade de preencher novamente as demais informações;

2.2.4.1180. A operação de login deverá ser feita através do formulário ou através de login social via Facebook, Instagram, X, Google, LinkedIn ou demais redes, sendo que o login social deverá se comportar apenas como um facilitador para o preenchimento do formulário, pois algumas informações obrigatórias para o cadastro na plataforma não são obtidas com o uso do login social;

2.2.4.1181. Ao executar uma campanha o usuário deverá visualizar até 3 interações no máximo, antes de ser liberado para acesso à Internet;

2.2.4.1182. Nas interações, o usuário poderá rejeitar a interação, clicando em um botão de rejeição apresentado na tela;



2.2.4.1183. Nas interações do tipo Banner e Pesquisa Objetiva, o usuário deverá enviar um comentário para o estabelecimento;

2.2.4.1184. A plataforma deverá liberar o acesso à Internet, sem restrições, durante o prazo estabelecido pelo usuário responsável pelo local;

2.2.4.1185. A plataforma poderá bloquear novamente o acesso à Internet ao término do período de liberação estabelecido;

2.2.4.1186. Após a liberação do acesso, o usuário deverá ser redirecionado para o link configurado na criação da campanha;

2.2.4.1187. No momento da liberação da conexão com a Internet a plataforma deverá armazenar as seguintes informações, considerando a lei do Marco Civil da Internet: data e hora do início e fim da conexão, MAC Address do equipamento do usuário, endereço IP obtido pelo usuário;

2.2.4.1188. No momento do acesso ao captive portal, o usuário poderá indicar qual o idioma será apresentado nas telas de cadastro e termos de uso. Podendo escolher entre Português, Inglês e Espanhol;

2.2.4.1189. A plataforma deverá oferecer modelos de templates de campanhas, pré-configurados;

2.2.4.1190. Todos os relatórios, estatísticas e outras informações deverão ser segmentadas de acordo com filtros universais, já estabelecidos, como: Data, local ou grupo de local, nº de acessos e também por meio de uma função de busca no próprio sistema;

2.2.4.1191. Deverá ser possível exportar dados em arquivo no formato .xlsx com as informações de cada acesso realizado em um determinado período contendo dados básicos de acesso como id, data e horário, e informações referentes às interações realizadas por cada usuário (Nome, Sobrenome, E-Mail, Plataforma de autenticação, Sexo, Data de Nascimento, Telefone, informações de data e tempo do acesso, entre outros dados);

2.2.4.1192. Deverá possibilitar exportar dados em arquivo no formato .csv com as informações cadastrais dos usuários e quantidade de acessos;

2.2.4.1193. Deverá ser possível exportar dados em arquivo no formato .csv com as informações de download de conteúdo entre o servidor e os access points;

2.2.4.1194. Deverá ser possível exportar dados com as informações de inserções, edições, atualizações, exclusões e quaisquer atividades realizadas na plataforma por determinado usuário;

2.2.4.1195. Deverá informar o número de usuários conectados em tempo real;



2.2.4.1196. Ao realizar o cadastro, o usuário poderá optar por fazê-lo respondendo o seu e-mail, nome completo, data de nascimento, telefone e sexo; ou utilizando o preenchimento automático através das principais redes sociais;

2.2.4.1197. Deverá possibilitar informar a média do tempo que os usuários passaram conectados à internet do local;

2.2.4.1198. Deverá possibilitar métodos de autenticação para redes internas para controle de acesso de colaboradores e fornecedores, em SSID separado e VLAN específica;

2.2.4.1199. Deverá possibilitar trabalhos com os principais formatos de autenticação, como: SSO (Single-Sign-On), Voucher, LDAP, SAML, diferenciação de acesso, integração via Active Directory e também através de ERPs específicos;

2.2.4.1200. Deverá permitir visualização de todos os usuários cadastrados na plataforma;

2.2.4.1201. Deverá permitir visualização dos visitantes que mais acessaram a plataforma;

2.2.4.1202. Deverá permitir visualização dos visitantes mais recentes;

2.2.4.1203. Deverá permitir visualização de locais e aparelhos cadastrados;

2.2.4.1204. Deverá permitir visualizar campanhas criadas, usuário cadastrados, comentários feitos pelos usuários e usuários conectados no momento;

2.2.4.1205. Deverá possibilitar cadastrar termos de uso customizáveis e editáveis pelas contas e usuários selecionados e ser possível editar o campo de opt-in de forma isolada;

2.2.4.1206. Deverá ser garantido o armazenamento dos dados e logs dos usuários recorrentes durante a vigência do contrato, garantindo que as informações cadastrais e de acessos estejam acessíveis e protegidas durante todo o período de utilização dos serviços. Para usuários não recorrentes, os dados deverão ser mantidos no sistema por um período de um ano após a última conexão, assegurando conformidade com as políticas de privacidade e Marco Civil da Internet;

2.2.4.1207. Características Técnicas da Plataforma de conscientização e campanhas de phishing:

2.2.4.1208. A CONTRATADA deverá fornecer os seguintes serviços para atendimento desta solução:

Item	Descrição do item	Quantidade Total
1	Subscrição de licença de plataforma integrada	2500 licenças



	de campanhas de phishing e treinamentos on-line, na modalidade de Ensino à Distância (EaD), voltados à capacitação e conscientização em Segurança da Informação, Segurança Cibernética e Proteção de Dados Pessoais. Licença para 12 meses	
2	Suporte técnico especializado para a plataforma integrada de campanhas de phishing e treinamentos online. Suporte para 12 meses	20 horas
3	Treinamento para administração da plataforma (on-line). Suporte para 3 horas	3 horas

2.2.4.1209. Os serviços devem compreender o seguinte:

2.2.4.1210. Identificar usuários que necessitam de treinamento em Segurança da Informação, Segurança Cibernética e Proteção de Dados Pessoais, através de campanhas de phishing;

2.2.4.1211. Gerar estatísticas de uso para identificar elementos que possam confundir o usuário a clicar em links maliciosos ou responder a e-mails de phishing;

2.2.4.1212. Consolidar os dados coletados para permitir a análise crítica e a avaliação de ações pela Administração, mitigando riscos relacionados à utilização do e-mail corporativo;

2.2.4.1213. Proporcionar ferramentas e recursos educacionais para capacitar os usuários conforme suas necessidades individuais.

2.2.4.1214. O objetivo da contratação da plataforma integrada de campanhas de phishing e treinamentos on-line é para gerar os seguintes benefícios:

2.2.4.1215. Aumento da conscientização sobre as melhores práticas de segurança da informação;

2.2.4.1216. Melhoria na compreensão dos riscos e ameaças cibernéticas;

2.2.4.1217. Fortalecimento das habilidades em identificar e reportar incidentes de segurança;

2.2.4.1218. Redução do número de incidentes de segurança causados por erros humanos;

2.2.4.1219. Aumento da adesão às políticas e diretrizes de segurança da informação;



2.2.4.1220. Melhoria na proteção de dados pessoais e informações sensíveis da prefeitura municipal de Sinop-MT.

2.2.4.1221. Criação de uma cultura de segurança da informação, tornando-se agentes na proteção de ativos e recursos digitais desta instituição.

2.2.4.1222. A CONTRATADA deve realizar um treinamento para a equipe da CONTRATANTE que atuará com a administração da plataforma integrada de campanhas de phishing e treinamentos on-line;

2.2.4.1223. A capacitação da equipe técnica designada pela CONTRATANTE poderá ser realizada presencialmente, em suas instalações, ou por meio de Ensino à Distância (EaD) síncrono (on-line e ao vivo), com a opção de gravação ser disponibilizada posteriormente à CONTRATANTE;

2.2.4.1224. A capacitação deve abranger a gestão e operação da plataforma, ocorrendo preferencialmente nos primeiros dias úteis após a assinatura do contrato;

2.2.4.1225. A comprovação de capacidade técnica para este item observará as diretrizes estabelecidas no item 5.12 deste Termo de Referência, devendo demonstrar experiência anterior na prestação de serviços de natureza compatível com soluções de conscientização em segurança da informação, treinamentos ou campanhas de phishing, sem a exigência de quantitativo mínimo percentual fixo.

2.2.4.1226. Como condição de eficácia para a execução contratual, caso não seja a própria fabricante da solução ofertada, deverá comprovar, previamente à assinatura do contrato (ou ao início da prestação dos serviços), a condição de parceira, revenda ou prestadora autorizada pelo fabricante, assegurando o cumprimento da legislação de propriedade intelectual, direitos autorais e o fornecimento regular das atualizações de software e suporte técnico. A comprovação destina-se exclusivamente a garantir a legitimidade da execução contratual.

2.2.4.1227. Dos Serviços de Mapeamento de Vulnerabilidades:

2.2.4.1228. Varredura simples para descobrir hosts ativos e portas abertas;

2.2.4.1229. Varredura completa do sistema indicada para qualquer ativo na rede;

2.2.4.1230. Verificação sem restrições ou recomendações;

2.2.4.1231. Verificação dinâmica de plug-in sem restrições ou recomendações;

2.2.4.1232. Verificação de malware em sistema Windows e Unix;

2.2.4.1233. Verificação de vulnerabilidades da Web publicadas e desconhecidas;

2.2.4.1234. Verificação de autenticação para hospedagem e enumeração de atualizações ausentes;

2.2.4.1235. Verificações remotas e locais para CVE-2017-5689;



- 2.2.4.1236.** Verificação remota e local para CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754;
- 2.2.4.1237.** Verificação remota e local para MS17-010;
- 2.2.4.1238.** Varredura remota para hosts de impressão digital potencialmente executando a pilha Treck na rede;
- 2.2.4.1239.** Verificação remota para detectar a elevação de privilégio do Microsoft Netlogon (zerologon);
- 2.2.4.1240.** Verificação local e remota para detectar vulnerabilidades do SolarWinds Solorigate;
- 2.2.4.1241.** Verificação local e remota para detectar vulnerabilidades do Exchange direcionadas pelo HAFNIUM;
- 2.2.4.1242.** Verificação local para detectar a vulnerabilidade do PrintNightmare no spooler de impressão do Windows;
- 2.2.4.1243.** Busque por configurações incorretas no Active Directory;
- 2.2.4.1244.** Detecção do Apache Log4j CVE-2021-44228;
- 2.2.4.1245.** Detecção do Apache Log4j CVE-2021-44228 por meio de verificações diretas;
- 2.2.4.1246.** Detecção de vulnerabilidades do Log4Shell;
- 2.2.4.1247.** Detecção de vulnerabilidades de alertas recentes no CISA;
- 2.2.4.1248.** Detecção de vulnerabilidades de alertas recentes no CISA;
- 2.2.4.1249.** Auditoria de configurações de serviços de nuvem de terceiros;
- 2.2.4.1250.** Possibilitar verificação de vulnerabilidade interna do PCI DSS (11.21);
- 2.2.4.1251.** Possibilitar auditoria de configuração dos dispositivos de rede;
- 2.2.4.1252.** Possibilitar auditoria das configurações dos sistemas relacionadas a uma linha de base conhecida;
- 2.2.4.1253.** Possibilitar auditoria de sistemas utilizando definições SCAP e OVAL;
- 2.2.4.1254.** Deve possibilitar automatizar avaliações para encontrar, prever, avaliar, diagnosticar e apontar ações que devem ser realizadas para corrigir as vulnerabilidades encontradas;
- 2.2.4.1255.** Deve contemplar o recurso de Descobertas como a primeira etapa da avaliação de vulnerabilidades, gerando inventário completo de todos os ativos de rede, num ambiente distribuído. O processo de descoberta deve utilizar de recursos de avaliação de vulnerabilidades com softwares dotados de inteligência artificial devidamente licenciado;



2.2.4.1256. Deve contemplar o recurso de Avaliar para identificar de forma rápida e eficiente as vulnerabilidades, as configurações incorretas, os pontos fracos na rede de computadores, ativos e vetores de ameaças em potencial;

2.2.4.1257. Deverá contemplar o recurso de Conformidade, neste processo é realizado uma auditoria nas conformidades das configurações, embasadas na análise de benchmarks do Center for Internet Security (CIS) e conjunto de melhores práticas compiladas nas áreas de defesa, energia, finanças, transportes, engenharia etc;

2.2.4.1258. Deverá contemplar o recurso de Analisar, esse recurso fornece visão geral da organização, analisará filtragens e agrupamentos sofisticados permitindo uma busca detalhada com análise de resultados, para obter os detalhes de vulnerabilidades e o que podem ser potencialmente afetados acelerando o tempo de detecção, análise e correção;

2.2.4.1259. Deverá contemplar o recurso de Relatar no formato PDF todos os snapshots e informações colhidas no processo de mapeamento de vulnerabilidades, informando as características da análise;

2.2.4.1260. O mapeamento de vulnerabilidades deverá ser realizado, após a implementação das soluções de NGFW e Endpoints Corporativos, como condição de entrega e validação destes serviços;

2.2.4.1261. O processo de mapeamento de vulnerabilidades deverá ser realizado por técnicos da CONTRATADA devidamente capacitado;

2.2.4.1262. Deverá ser enviado no prazo máximo de 10 dias úteis após a realização de cada mapeamento de vulnerabilidades, relatório detalhado com resultados da análise, para um e-mail indicado pela CONTRATANTE.

2.2.4.1263. Unidade de serviço técnico - UST

2.2.4.1264. Cada Unidade de Serviço Técnicos (UST) corresponderá à 4h (quatro horas) de profissional especializado. O serviço deverá ser prestado pelo próprio fabricante (Professional Services) ou pela empresa contratada através de profissional certificado;

2.2.4.1265. Atividades: assessment, desenvolvimento de plano de implementação, planejamento, análise, configuração, integração, migração, testes de verificação, ajustes, tuning, hardening; otimização; troubleshooting; updates; upgrades; provas de conceito; ensaios de contingência; customização de consultas de relatórios; participação em comitês de segurança para esclarecimentos; documentação "as built"; documentação para rollout;



2.2.4.1266. Os perfis dos profissionais/atividades definidas seguirão o padrão de perfis indicados por metodologias de projetos, como PMBOK:

2.2.4.1267. Arquitetura: definição da arquitetura lógica e física do projeto, garantindo a qualidade durante a implantação e o atendimento de todos os requisitos funcionais e não funcionais; propor melhorias; definir controles e monitoramento do ambiente, sugerindo métricas, thresholds e indicadores de acompanhamento; apoio no planejamento, execução e avaliação de mudanças;

2.2.4.1268. Implementação: Levantamento de dados, execução das implantações incluindo configuração customizada, integração, migrações e testes, adaptações código, criação de infraestrutura, orientação, documentação, entre outros;

2.2.4.1269. Gerenciamento de projetos: gerenciamento do projeto propriamente dito, considerando controle de prazos, esforço, elaboração de relatórios de posicionamento executivo, indicadores do projeto e qualquer outra métrica prevista no PMBOOK. O objetivo de todas estas atividades é a garantia de qualidade do projeto no que tange prazos e esforço;

2.2.4.1270. Suporte: Atendimento a incidentes de suporte realizando análises, troubleshooting, diagnósticos; realizando ajustes e otimização configurações; analisando e aplicando patches e updates; realizando testes e ensaios; monitorando o ambiente;

2.2.4.1271. As atividades deverão ser prestadas na modalidade on-site, exceto quando expressamente autorizado pelo Departamento de T.I da Prefeitura de Sinop;

2.2.4.1272. Dinâmica de contratação: O departamento de T.I da Prefeitura contratará a quantidade de Unidades de Serviços Técnicos estimadas para consumo;

2.2.4.1273. A Contratada deverá prestar os serviços conforme à quantidade de Unidades de Serviços contratadas, que poderão ser consumidos pelo município ao longo do período do contrato, de acordo com a necessidade das secretarias municipais;

2.2.4.1274. O departamento de T.I consultará a CONTRATADA para calcular a quantidade de Unidades de Serviços Técnicos necessárias para realizar a atividade pretendida e emitirá Ordem de Serviço para a Contratada prestar os serviços. E, ao final dos serviços, contabilizará o consumo das Unidades de Serviços Técnico utilizadas;

2.2.4.1275. O prazo máximo para início das atividades pela empresa contratada será de 5 (cinco) dias;



2.2.4.1276. As contabilizações de UST serão feitas individualmente para cada profissional alocado;

2.2.4.1277. As UST executadas fora do expediente comercial por solicitação deste órgão, serão contabilizadas em dobro;

2.2.4.1278. A empresa Contratada deverá nomear funcionário capacitado que será responsável por fornecer aconselhamento técnico e operacional sobre os serviços, assistência sobre as condições do contrato, gerenciamento de escalação junto ao fabricante, gerenciamento de recursos e cronograma de entrega dos serviços;

2.2.4.1279. Neste modelo de execução dos serviços não se caracteriza a subordinação direta e nem a pessoalidade, visto que não haverá qualquer relação de subordinação jurídica entre os profissionais da equipe da empresa contratada a este Órgão. As empresas proponentes deverão considerar em seus custos todos os recursos necessários ao completo atendimento aos objetos, tais como despesas com pessoal (salários, férias, encargos, benefícios, seleção, outras) de modo a garantir os serviços definidos;

2.2.4.1280. Para o controle da execução dos serviços será utilizado a Unidade de medida UST (Unidade de Serviço Técnico);

2.2.4.1281. A UST consiste na “moeda” usada para dimensionar todas as atividades que serão demandadas pela CONTRATANTE, no escopo de cada Ordem de Serviço;

2.2.4.1282. A contratação será em volume de UST por atividade e a licitação resultará na oferta do valor de uma UST que irá representar o esforço combinado de profissionais envolvidos, variando a complexidade e prioridade da atividade.

2.2.4.1283. ESPECIFICAÇÕES TÉCNICAS GERAIS:

2.2.4.1284. A CONTRATADA deverá garantir a prestação dos serviços, conforme as exigências e determinações constantes neste instrumento, independentemente de marca e modelos dos produtos, software ou hardwares que serão utilizados;

2.2.4.1285. Cada hardware deverá ser fornecido com todos os acessórios e programas necessários à sua instalação, operação e monitoração, cabendo inclusive, a CONTRATADA, a instalação do hardware e configurações de todas as funcionalidades da solução;

2.2.4.1286. Cada software deverá ser fornecido devidamente licenciado, instalado e configurado conforme a necessidade da Prefeitura de Sinop/MT.

2.2.4.1287. Deve possuir, para os casos de appliances físicos, serviço de RMA com entrega de equipamentos e peças em até 4 horas após diagnóstico, durante toda a vigência do contrato;



2.2.4.1288. Em caso de defeitos em peças/dispositivos que possuam armazenamento de dados, o serviço de RMA deve permitir a retenção, pelo cliente, dessas peças/dispositivos defeituosos, a fim de garantir o sigilo dos dados pessoais e dos dados críticos para a Prefeitura ali armazenados;

2.2.4.1289. Toda a solução deve ser nova, disponível para primeiro uso e em pleno período de vida, sem previsão de término dos tempos de vida, vendas e suporte;

2.2.4.1290. Não serão aceitos equipamentos em modo End of Support, End of Life ou equivalentes anunciados pelo fabricante até a data da abertura das propostas que englobem o período total do contrato. Dessa forma, na data de abertura das propostas, o equipamento deve estar em sua fase do ciclo de vida de plena comercialização e suporte, não sendo aceitos equipamentos com qualquer limitação a essa condição (End of Life, End of Support ou equivalente) considerando a data de abertura das propostas, essa condição será verificada por meio do acesso ao site do fabricante; **Todas as citações a seguir, do item 5.1 ao 5.12, estão no apêndice;**

2.2.4.1291. Todos os serviços especializados de segurança da informação (hardwares, softwares e licenças) dos itens 5.1, 5.2, 5.3, 5.4, 5.6 e 5.7, deverão ser fornecidos em hardwares dedicados do tipo appliance e serem do mesmo fabricante;

2.2.4.1292. Os serviços especializados de segurança da informação com solução de endpoint corporativo do tipo EDR deverá ser fornecido em nuvem e serem do mesmo fabricante dos itens 5.1, 5.2, 5.3, 5.4, 5.5, 5.6 e 5.7;

2.2.4.1293. Todos os serviços especializados de segurança da informação (hardwares, softwares e licenças) dos itens 5.1, 5.2, 5.3, 5.4, 5.5, 5.6 e 5.7 deverão ser compatíveis e se integrar nativamente, através de protocolo proprietário todas as funcionalidades de segurança e defesa cibernética com a infraestrutura de gerenciamento e monitoramento do CORE da rede do Data Center da Prefeitura (switches core, topo de rack e de distribuição).

2.2.4.1294. Toda a solução deve ser fornecida contemplando licenciamento e garantia do fabricante, durante toda a vigência do contrato;

2.2.4.1295. Todos os equipamentos que compõem os itens 5.1, 5.2, 5.6 e 5.7 deverão possuir homologação da Agência Nacional de Telecomunicações (ANATEL), conforme determina a Resolução nº 715, de 23 de outubro de 2019, com validade na data da apresentação das propostas. Os documentos comprobatórios deverão ser apresentados juntamente com a proposta comercial;

2.2.4.1296. Com o objetivo de reforçar a segurança da camada de acesso a infraestrutura da rede de computadores municipal, o gerenciamento dos ativos de
Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



rede e cibersegurança deverão obrigatoriamente serem gerenciados pelo protocolo Fortilink, desta forma esses ativos de rede tornarão uma extensão do NGFW, integrando-os diretamente no Security Fabric.

2.2.4.1297. Deverá ser realizado no mínimo 3 (três) horas de treinamento em segurança da informação para os gestores e/ou grupos de servidores, através de profissional devidamente especializado em governança e segurança da informação, conforme critérios a serem estabelecidos por este órgão;

2.2.4.1298. Deverá ser elaborado um High-Level Design (HLD), contemplando todas as unidades públicas municipais com o detalhamento de como a solução ofertada atende às necessidades apontadas na licitação;

2.2.4.1299. A aprovação do HLD deverá ser feita pela equipe técnica indicada pelo departamento de T.I do órgão;

2.2.4.1300. Para os NGFW deverá ser apresentado um teste de laboratório (Nacional ou Internacional) que compare o produto ofertado com no mínimo 3 (três) fabricantes, garantindo que o equipamento seja capaz de:

2.2.4.1301. Prevenir no mínimo 70% (setenta por cento) dos malwares testados;

2.2.4.1302. Prevenir no mínimo 70% (setenta por cento) de variantes de malwares conhecidos;

2.2.4.1303. Possuir uma taxa de falso positivo na detecção de malware menor que 1% (um por cento);

2.2.4.1304. Possuir taxa de prevenção de phishing e URL maliciosas maior que 90% (noventa por cento);

2.2.4.1305. O teste deve ter duração mínima de 90 (noventa) dias com no mínimo 300 (trezentos) conjuntos de dados maliciosos (vírus e malwares).

2.2.4.1306. Para o teste especificado acima, poderá ser utilizado como referência os testes realizados pela empresa Miercom (www.miercom.com). Um exemplo de teste que aborda todos os indicadores acima é o de número SR220915Q - NGFW Firewall Security Benchmark 2023 - Firewall Security Efficacy Competitive Assessment Summary Lab Report;

2.2.4.1307. O fabricante da solução de segurança ofertada deverá ser parceiro do site www.cve.org, onde deverão estar indicados todos os CVE (Common Vulnerabilities and Exposures);

2.2.4.1308. O fabricante da solução de segurança ofertada deverá manter em seu site todos os CVE identificados, seu detalhamento e correções disponibilizadas.

2.2.4.1309. SUPORTE TÉCNICO:

Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



2.2.4.1310. Toda a solução deve ser fornecida contemplando suporte técnico 24x7 do Fabricante e da CONTRATADA;

2.2.4.1311. A contratada deverá manter contrato de manutenção e de suporte de todos os ativos e seus respectivos softwares junto ao fabricante durante toda a vigência do contrato;

2.2.4.1312. Deve ser contemplado e declarado em proposta o serviço de Suporte técnico que atenda os seguintes SLAs:

2.2.4.1313. Prazo máximo de reposta ao atendimento inicial em casos emergenciais com indisponibilidade de serviços em até 10 (dez) minutos, exceção ao prazo estabelecido no item **6.18.6.2.1.** casos emergenciais que impliquem indisponibilidade dos serviços, que será de até 15 (quinze) minutos;

2.2.4.1314. Prazo máximo de resposta ao atendimento inicial em casos com criticidade alta (situações de perda de funcionalidades ou instabilidades) em até 10 (dez) minutos;

2.2.4.1315. Prazo máximo para atendimento dos chamados em casos emergenciais com indisponibilidade de serviços de 1 (uma) hora;

2.2.4.1316. Prazo máximo para atendimento dos chamados com criticidade alta de 1 (uma) horas;

2.2.4.1317. Prazo máximo para atendimento dos chamados para solução de contorno em casos emergenciais com indisponibilidade dos serviços de até 3 (três) horas;

2.2.4.1318. A CONTRATADA deverá disponibilizar técnicos especializados com disponibilidade 24x7 durante toda a vigência do contrato;

2.2.4.1319. Para abertura de chamados, deverá obrigatoriamente ser realizada somente através de telefone 0800, celular ou aplicativo de mensagens corporativo. O registro do atendimento e acompanhamento é de total responsabilidade da CONTRATADA;

2.2.5. DO DEMONSTRATIVO DE COMPROVAÇÃO DAS ESPECIFICAÇÕES TÉCNICAS

2.2.5.1. A licitante convocada para apresentação da proposta de preços deverá, juntamente com a proposta, preencher o **Demonstrativo de Comprovação das Especificações Técnicas, conforme modelo e orientações constantes do Apêndice 1** deste Termo de Referência, indicando, para cada requisito técnico que demande comprovação, os respectivos documentos comprobatórios, trechos e páginas que evidenciem o atendimento às especificações estabelecidas.

2.2.5.2. A documentação apresentada deverá permitir a análise objetiva do atendimento aos requisitos técnicos previstos neste Termo de Referência, podendo



ser utilizados, conforme o caso, datasheets, manuais, declarações do fabricante, certificados, documentos técnicos públicos e demais documentos pertinentes à comprovação da solução ofertada.

2.2.5.3. Os documentos utilizados para comprovação deverão ser anexados à proposta, observadas as orientações constantes do Apêndice 1, inclusive quanto à identificação dos arquivos e, quando se tratar de documentação pública, à indicação do respectivo endereço eletrônico para consulta.

2.2.5.4. A ausência de comprovação, a insuficiência da documentação apresentada ou a constatação de que a solução ofertada não atende aos requisitos técnicos estabelecidos poderá ensejar a desclassificação da proposta, observado o procedimento previsto na legislação aplicável.

2.3. Estimativa de consumo individualizada de cada um dos órgãos participantes: A estimativa das quantidades a serem contratadas foi elaborada em observância ao disposto no inciso IV do § 1º do art. 18 da Lei Federal nº 14.133/2021, considerando as necessidades identificadas pela Administração e a interdependência dos componentes que integram a solução de segurança da informação, de modo a possibilitar o adequado dimensionamento da contratação e a racionalização dos recursos públicos.

Estimativa das quantidades a serem contratadas, acompanhada das memórias de cálculo e dos documentos que lhe dão suporte, considerando a interdependência com outras contratações, de modo a possibilitar economia de escala (inciso IV do § 1º do art. 18 da Lei 14.133/21).

Considerando a natureza corporativa e integrada da solução, a demanda não foi dimensionada de forma individualizada por Secretaria quanto aos equipamentos, licenças e demais componentes da solução. A Secretaria Municipal de Administração e Modernização atua como unidade responsável pela centralização da demanda e pela gestão da contratação, sendo os recursos contratados destinados ao atendimento da infraestrutura tecnológica corporativa utilizada pelas diversas Secretarias e unidades administrativas do Município de Sinop-MT.

Dessa forma, os quantitativos foram definidos com base na estrutura tecnológica municipal, na capacidade necessária para atendimento das unidades administrativas e na provável utilização dos serviços durante o período de execução, considerando ainda a necessidade de disponibilização integrada dos recursos de segurança da informação.



A utilização dos serviços ocorrerá conforme a efetiva necessidade da Administração, observados os quantitativos e limites estabelecidos neste Termo de Referência, não havendo garantia de contratação integral dos quantitativos registrados.

Para complementar a forma de se chegar à quantidade estimada da contratação, segundo o Decreto Municipal nº 359/2023, pode-se chegar às quantidades estimadas com base no consumo anterior ou na provável utilização. No caso em questão, que consiste em **Registro de Preços para futura e eventual contratação de empresa especializada para prestação de serviços de segurança da informação**, *compreendendo o fornecimento e a disponibilização de equipamentos, appliances, licenças, subscrições, softwares, plataformas, componentes, acessórios e demais recursos necessários, bem como a implantação, instalação, configuração, integração, parametrização, testes, ativação, suporte técnico, manutenção, atualização tecnológica, gerenciamento, monitoramento e demais serviços necessários ao pleno e adequado funcionamento da solução, destinada à proteção da infraestrutura de tecnologia da informação do Município de Sinop-MT*, a estimativa das quantidades foi estabelecida considerando a provável utilização da solução e as necessidades da infraestrutura tecnológica corporativa municipal.

Considerando a natureza sistêmica e integrada da contratação, a Secretaria Municipal de Administração e Modernização atua como unidade gestora e centralizadora da demanda, consolidando as necessidades das demais Secretarias e unidades administrativas do Município de Sinop-MT, de modo que os quantitativos estimados não correspondem a uma demanda exclusiva da unidade solicitante, mas à necessidade consolidada da estrutura administrativa municipal.

A definição dos quantitativos considerou a estrutura tecnológica existente, a capacidade necessária para atendimento das unidades administrativas e a projeção de utilização dos serviços durante o período estimado de execução, observadas as características e a interdependência dos componentes que integram a solução de segurança da informação.

Dessa forma, os documentos e informações apresentados pela Secretaria Municipal de Administração e Modernização constituíram a base para a consolidação da demanda de toda a estrutura municipal, tendo em vista sua responsabilidade pela centralização do planejamento e gestão da contratação. A formalização da demanda ocorreu mediante os documentos encaminhados pela referida Secretaria, por meio



eletrônico e físico, juntamente com seus respectivos anexos, os quais foram utilizados para subsidiar o dimensionamento da contratação.

2.1.1. SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO E MODERNIZAÇÃO				
COD. TCE.	DESCRIÇÃO E ESPECIFICAÇÃO	UND. FORN.	QUANT. MIN. PARA 1 ANO	QUANT. MAX. PARA 1 ANO
404919-5	Serviços especializados de segurança da informação com solução de NGFW/SD-Wan em cluster (alta disponibilidade) fornecidos em appliance Tipo 1. FortiGate 200G + Licença UTP	MÊS	1	12
404919-5	Serviços especializados de segurança da informação com solução de NGFW/SD-Wan fornecidos em appliance Tipo 2. FortiGate 30G + Licença UTP	MÊS	1	12
404919-5	Serviços especializados de segurança da informação com solução da base de dados analíticos e logs fornecidos em appliance. FortiAnalyzer FAZ-300G	MÊS	1	12
404919-5	Serviços especializados de segurança da informação com solução de gerenciamento de NGFW fornecidos em appliance. FortiManager FMG-200G	MÊS	1	12
404919-5	Serviços especializados de segurança da informação com solução de endpoint corporativo do tipo EDR. FortiEDR Discover, Protect ERespond Cloud	MÊS	1	12
427217-0	Serviços especializados de segurança da informação com solução de WAF. FortiWeb 100F	MÊS	1	12
404919-5	Serviços especializados de segurança da informação com solução de Access Point corporativo. FortiAP 231-K	MÊS	1	12
427217-0	Serviços especializados de segurança da informação com solução de Captive Portal. Wifeed	MÊS	1	12
427217-0	Serviços especializados de segurança da informação com plataforma de conscientização e campanhas de phishing. BeePhish	MÊS	1	12
413246-7	Serviços especializados de segurança da informação para mapeamento de vulnerabilidades. Nessus Tenable	MÊS	1	12
413246-7	Unidade de serviço técnico -UST	HORA	1	300

3. JUSTIFICATIVA/NECESSIDADE DA CONTRATAÇÃO

3.1. Justificativa: Considerando que a Lei nº 14.133/2021 estabelece, como regra, a realização das licitações por meio eletrônico, ressalvadas as hipóteses legalmente justificadas, apresenta-se a motivação para a presente contratação.

A contratação de solução integrada de segurança da informação tem por finalidade fortalecer a proteção da infraestrutura tecnológica da Administração Pública



Municipal, assegurando a disponibilidade, a integridade e a confidencialidade das informações institucionais, bem como a continuidade dos serviços públicos suportados por recursos de tecnologia da informação.

A crescente utilização de sistemas informatizados para execução das atividades administrativas, atendimento à população e gestão dos serviços públicos torna indispensável a adoção de mecanismos capazes de prevenir, detectar e responder a incidentes de segurança cibernética, reduzindo riscos relacionados a acessos não autorizados, indisponibilidade de serviços, perda de informações, ataques cibernéticos e demais vulnerabilidades que possam comprometer o funcionamento da Administração Pública Municipal.

A solução pretendida contempla recursos tecnológicos integrados destinados à proteção do ambiente computacional do Município, permitindo gerenciamento centralizado, monitoramento contínuo dos eventos de segurança, proteção dos ativos tecnológicos e maior eficiência na administração da infraestrutura de tecnologia da informação.

A contratação também permitirá a atualização tecnológica da infraestrutura atualmente utilizada, assegurando que o Município disponha de solução compatível com as necessidades atuais e futuras da Administração Pública, observando critérios de eficiência, economicidade, continuidade dos serviços públicos e interesse público.

A estimativa das necessidades foi elaborada pela Secretaria Municipal de Administração e Modernização, unidade responsável pela gestão centralizada da infraestrutura de tecnologia da informação do Município, considerando o histórico de utilização da solução atualmente contratada, as previsões constantes no Plano de Contratações Anual (PCA), as demandas formalizadas pela unidade demandante, a evolução da infraestrutura tecnológica municipal e as necessidades projetadas para o período de vigência da futura contratação.

3.1.1. Justificativa da Secretaria Municipal de Administração e Modernização:

O município de Sinop-MT possui uma grande quantia de dados e informações que são coletados, armazenados, usados e que trafegam em sua infraestrutura de Tecnologia e da Informação. Esses dados são essenciais para o devido funcionamento e atingimento dos objetivos do poder público.

Atualmente, temos mais de uma centena de unidades espalhadas pelo município (escolas, creches, unidades básicas de saúde, CRAAs, CREAs, postos da guarda municipal, secretarias etc), que possuem apenas um link de fibra ótica mantida pelo município.

Os dados e informações que são produzidos, tratados e utilizados nestas unidades, também necessitam ser devidamente protegidos, além de garantir maior disponibilidade de tráfego e compartilhamento



entre os departamentos da administração pública e outras entidades governamentais, visando garantir a eficiência dos serviços públicos, razão pela qual, este município necessita estabelecer, adequar e implementar medidas relacionadas à segurança da informação (cibersegurança), de acordo com as melhores práticas e procedimentos de governança, em referidos locais.

Neste sentido, estabelecendo um arcabouço de tecnologia da informação mais moderno, prático, viável e seguro, também nas unidades descentralizadas, estaremos cumprindo ainda, com os termos exigidos na Lei Geral de Proteção de Dados (Lei nº 13.709/18), Marco Civil da Internet (Lei nº 12.965/14) e diretrizes da Política Nacional de Cibersegurança (Decreto n. 11.856/23).

Na sede do paço municipal e em algumas secretarias do município já possuem infraestrutura experimentada de segurança dentro dos parâmetros das boas práticas, o qual estabelece um norte de comportamento para a administração pública, no sentido de implementar e ampliar as soluções de segurança da informação, nas demais unidades descentralizadas.

Esses órgãos e secretarias que já são atendidos por uma infraestrutura adequada, são conectados por enlaces dedicados de fibra óptica e links de internet de operadoras de telefonia e possuem uma solução SD-Wan baseada em Firewalls NGFW do fabricante Fortinet.

Essas redes conectam os servidores públicos e munícipes às aplicações hospedadas em servidores no Data Center da Prefeitura, onde uma solução de segurança baseada em Switchs Core, do fabricante Fortinet, protege o núcleo da rede, razão pela qual, a solução ora licitada, deve ser compatível tecnicamente com a infraestrutura existente. Desse modo, é recomendável a visita local dos interessados.

Com esta contratação haverá a ampliação das possibilidades de coleta, tratamento, proteção, tráfego e disponibilização dos dados e informações visando aperfeiçoar a eficiência deste município na oferta dos serviços públicos através de uma infraestrutura de segurança da informação moderna.

Esses objetivos podem ser alcançados com a ampliação e implementação de melhorias tecnológicas que permitam oferecer tal disponibilidade e gestão, seja por aquisição de novos serviços correlatos, ou com tecnologias já embarcadas em equipamentos/sistemas de alta capacidade de proteção (Firewall NGFW), com funcionalidades tecnológicas, como a SD-WAN, que serve para realização de contingência para internet, facilitando o gerenciamento e monitoramento da rede, além da alta disponibilidade de conectividade.

Atualmente, há uma rede cabeada interligando as unidades descentralizadas, contudo, há necessidade de que a mesma possua redundância, capaz de manter as disponibilizações dos serviços públicos, mesmo com a interrupção da rede cabeada (rompimento, por exemplo), razão pela qual o estabelecimento da SD-WAN nas unidades descentralizadas, juntamente com links redundantes de internet (podendo incluir solução satelital), gerará segurança operacional dentro das melhores práticas e padrões robustos de tecnologia e conectividade, que elevarão o nível de conformidade e disponibilidade de serviços públicos deste município.

Além do mais, há imperiosa necessidade de aquisição de antivírus corporativo (Endpoint) para instalações nos equipamentos (computadores, notebooks e servidores), que possibilite escalada na



superfície deste segurança de município, com funcionalidades como: ZTNA universal (acesso seguro a sistemas via VPN SSL e DNAT), Filtragem e gerenciamento web SaaS, Gerenciamento de vulnerabilidades, Prevenção de malware e exploit, VPN SSL e IPSec com cliente gerenciado e Proteção contra ransomware.

Esta gamificação de dados e logs gerados na infraestrutura tecnológica do município também devem ser armazenadas e gerenciadas em appliance compatível com as soluções existentes atualmente.

Considerando ainda que, um dos pontos de vulnerabilidades mais sensíveis deste município é o site, também há necessidade de aquisição de solução para a proteção web do mesmo, contra ataques cibernéticos.

Para a efetiva implementação destas soluções e ampliação da visão da infraestrutura da rede deste município, os serviços devem compor a realização de Mapeamento de Vulnerabilidades, através de software licenciado, que permite o levantamento das possíveis inconsistências e irregularidades nas redes locais, possibilitando correção e bloqueio de falhas de segurança. Através de uma varredura em todo o ambiente computacional da prefeitura é possível avaliar ameaças e manter o ambiente mais seguro.

Com o serviço de captive portal disponibilizaremos acesso à internet para a população, através de uma rede própria e isolada para visitantes, com conexão segura e autenticada, além do atendimento ao Marco Civil da Internet, no que se refere à identificação do usuário nas conexões e registros dos referidos logs, que visam trazer inclusão digital aos munícipes e facilitação de acesso aos serviços públicos digitais (gov.br, serviços notariais, detran, concessionários de serviços de água e esgoto, secretarias fazendárias etc).

Além do mais, com a estabelecimento de medidas técnicas e administrativas de proteção cibernética, imperioso é treinar e capacitar os servidores a respeito da conscientização em proteção de dados, através de plataforma que viabilize campanhas de phishing e treinamentos sobre a matéria.

O estabelecimento de tais serviços vai de encontro às melhores práticas de Governança de Tecnologia e Segurança da Informação, indicadas pela ISO 27001 (Sistema de Gestão de Segurança da Informação - SGSI), ISO 27002 (Controles do SGSI); 27701 (Gestão da Privacidade da Informação) e ISO 29100 (Estrutura de Proteção de Dados Pessoais, dentro de Sistemas de Tecnologia da Informação - TI), uma organização deve estabelecer e implementar, operar, monitorar, analisar criticamente, manter e melhorar o seu SGSI, para garantir a efetividade das medidas de segurança administrativas e operacionais, em obediência ainda, aos preceitos e normas legais, incluindo a LGPD, Marco Civil da Internet e a própria Constituição Federal, além das diretrizes dispostas no Decreto n. 11.856/23 (PNCiber).

Esclarece-se que, o Departamento de T.I. deste município, é responsável pelo direcionamento técnico da infraestrutura tecnológica do município. Nos últimos anos, está sendo necessária uma coordenação técnica cada vez maior, com o objetivo de padronizar a infraestrutura e as soluções de informática que atendem ao município (hardwares e softwares). Essa padronização possibilita a otimização da aplicação de recursos financeiros e de pessoal (capacitação, treinamento, eficiência de atendimento etc). Em respeito ao determinado na alínea "a", inciso V, do art. 40, da Lei



14.133/21, as soluções que já se mostraram exitosas são grandes candidatas a se tornarem padrão para os demais.

Para alcançar um maior nível de maturidade técnica é necessário aumentar o nível de padronização, especialmente as soluções de segurança (Firewall, EDR, WAF, Analyzer e Access Point), que devem ser do mesmo fabricante das soluções já utilizadas, experimentadas e com resultados satisfatórios - Fortinet. Essa padronização também proporcionará um incremento na governança de TI por meio da homogeneização de processos, treinamento de equipes e simplificação da topologia, aumentando a maturidade operacional e otimizando a aplicação dos recursos.

Em virtude da crescente demanda por recursos de rede e computacionais, dos serviços oferecidos pelo Departamento de TI em modalidade eletrônica, da crescente quantidade de dispositivos conectados, da integração de sistemas cada vez mais necessários e visando longevidade de solução, torna-se imprescindível a disponibilidade de aquisição de 2 (dois) tipos de soluções, cuja diferença é o dimensionamento da capacidade computacional.

Ante a diversidade de soluções a serem contratadas e implementadas, necessária a contratação de serviços, através de Unidade de Serviço Técnico - UST.

Por fim, cabe destacar que, a evolução das plataformas de TI tem proporcionado, além de uma evolutiva integração homem-tecnologia, a abertura de diversas ações maliciosas que atentam contra a infraestrutura computacional de centenas de milhares de empresas e órgãos públicos, em todo o mundo. Em razão da tamanha evolução dos índices de sucesso nos ataques/sequestros/vazamentos de arquivos, torna-se imperativa a decisão de instalar sistemas de cibersegurança robustos, que possam garantir a continuidade dos serviços públicos e manter informações de caráter confidencial e sigilosos, devidamente protegidos.

3.2. Justificativa da Elaboração do Gerenciamento de Riscos: Em atendimento às disposições da Lei nº 14.133/2021 e da regulamentação municipal aplicável, foi elaborado o Gerenciamento de Riscos da presente contratação, contemplando a identificação dos principais riscos relacionados às fases de planejamento, seleção do fornecedor, execução contratual e encerramento do contrato.

O referido documento integra os autos do processo administrativo e servirá como instrumento de apoio ao acompanhamento da execução contratual, permitindo a adoção de medidas preventivas e corretivas destinadas à mitigação dos riscos identificados.

3.3. Justificativa da não Elaboração do Mapa de Risco: Embora tenha sido elaborado o Gerenciamento de Riscos da presente contratação, entende-se não ser necessária a elaboração do Mapa de Riscos.

A contratação possui objeto de natureza comum, com especificações técnicas claramente definidas, responsabilidades objetivamente delimitadas e execução amplamente conhecida pela Administração Pública, não apresentando grau de



complexidade que justifique a elaboração de Mapa de Riscos específico.

Além disso, os riscos inerentes à contratação foram devidamente identificados e tratados no documento de Gerenciamento de Riscos, que integra os autos do processo administrativo e estabelece as medidas preventivas e mitigadoras aplicáveis às fases de planejamento, seleção do fornecedor e execução contratual.

Assim, considerando as características do objeto e a regulamentação municipal aplicável, conclui-se que a elaboração do Mapa de Riscos mostra-se dispensável para a presente contratação, permanecendo preservado o adequado gerenciamento dos riscos por meio do documento específico elaborado para esse fim.

Considerando as características da presente contratação e as disposições do Decreto Municipal nº 359/2023, verifica-se que a elaboração do Mapa de Riscos poderá ser dispensada nas hipóteses previstas em seu art. 521, § 2º, o qual dispõe:

O gerenciamento dos riscos poderá ser dispensado nos casos envolvendo contratação de objetos de baixo valor, baixa complexidade e contratações de fornecimento e serviços normalmente utilizados pela Administração Pública com potencial de risco raro ou pouco provável ou de escala muito baixa ou baixa.

Portanto, o mapa de riscos acima citado não constará neste processo, pois não é o caso, conforme documento em anexo (gerenciamento de riscos).

3.4. Justificativa da Não Elaboração da Matriz de Risco Específica: Embora a contratação envolva solução tecnológica integrada e serviços especializados, os riscos identificados foram avaliados e tratados no documento de Gerenciamento de Riscos que integra os autos, com definição de medidas preventivas e mitigadoras para as etapas de planejamento, seleção do fornecedor e execução contratual.

Considerando a natureza do objeto, a definição objetiva das responsabilidades da contratada, os mecanismos de fiscalização previstos e a ausência de circunstâncias que demandem alocação extraordinária de riscos entre as partes, entende-se não necessária a elaboração de Matriz de Alocação de Riscos específica, sem prejuízo do gerenciamento dos riscos já realizado.

Dessa forma, os riscos relacionados à execução do contrato serão tratados por meio das cláusulas contratuais ordinárias, da fiscalização contratual e do Gerenciamento de Riscos elaborado durante a fase de planejamento, mostrando-se desnecessária a formalização de Matriz de Alocação de Riscos específica.

A matriz de risco definida no inciso XXVII do art. 6º da Lei 14.133/2021 e necessária nos contratos administrativos, quando for o caso, de acordo com o art. 92, inciso IX da mesma lei, não será adotada neste processo, levando em consideração



que em determinadas contratações, notadamente comuns e simples, tais como o processo em questão não é empregada. A matriz de risco é obrigatória, sobretudo em obras e serviços e fornecimentos de grande vulto, cujo valor estimado seja superior a R\$ 200.000.000,00 (duzentos milhões) de reais, vejamos.

Art. 22, § 3º Quando a contratação se referir a obras e serviços de grande vulto ou forem adotados os regimes de contratação integrada e semi-integrada, o edital obrigatoriamente contemplará matriz de alocação de riscos entre o contratante e o contratado.

Art. 6º, Inciso XXII - obras, serviços e fornecimentos de grande vulto: aqueles cujo valor estimado supera R\$ 200.000.000,00 (duzentos milhões de reais).

Decreto Municipal 359/2023 dispõe no art. 521, § 2º: O gerenciamento dos riscos poderá ser dispensado nos casos envolvendo contratação de objetos de baixo valor, baixa complexidade e contratações de fornecimento e serviços normalmente utilizados pela Administração Pública com potencial de risco raro ou pouco provável ou de escala muito baixa ou baixa.

Sendo assim, vê-se que não é o caso da contratação em trâmite, de forma que o referido documento não constará neste processo.

3.5. Fundamentação da Contratação: No ato da elaboração do Estudo Técnico Preliminar, foi observado o disposto no art. 85 do Decreto Municipal nº 359/2023, que estabelece:

Art. 85. Nas contratações de itens de consumo comuns, sistêmicos e geral a todos os órgãos da mesma Administração Pública ou que tenham sido objeto de planejamento anual, as Solicitações de Demanda/Documento de Formação de Demanda deverão partir de forma individualizada de cada uma das áreas demandantes para a Área Gestora, que ficará responsável por coordenar, padronizar e supervisionar o processo de contratação, assim como será a responsável para elaborar o Estudo Técnico Preliminar.

Parágrafo único. No âmbito do Poder Executivo Municipal, a Área Gestora será de responsabilidade da Diretoria Executiva de Administração.

Em observância ao disposto no art. 85 do Decreto Municipal nº 359/2023, a presente contratação possui caráter sistêmico e atendimento centralizado, tendo sua condução concentrada na Secretaria Municipal de Administração e Modernização, unidade responsável pela gestão da infraestrutura tecnológica do Município e pela consolidação das necessidades relacionadas à segurança da informação.

Embora a solução pretendida tenha por finalidade atender às necessidades de segurança da informação de toda a estrutura administrativa do Município de Sinop-MT, a condução centralizada do procedimento decorre da própria natureza do objeto e da necessidade de tratamento integrado da infraestrutura tecnológica e dos



mecanismos de proteção das informações municipais. Dessa forma, a contratação não se caracteriza como demanda exclusiva de uma única unidade administrativa quanto aos seus efeitos, mas como solução de caráter sistêmico, cuja gestão técnica e operacional será centralizada pela Secretaria Municipal de Administração e Modernização, com acompanhamento da equipe responsável pela infraestrutura de tecnologia da informação.

A centralização também permite consolidar as necessidades das diferentes unidades administrativas, promovendo maior padronização tecnológica, racionalização dos recursos, simplificação da gestão e melhor aproveitamento da contratação, sem prejuízo de que os serviços e soluções contratados sejam utilizados em benefício das demais Secretarias Municipais.

Tal sistemática encontra-se alinhada ao art. 19, inciso I, da Lei Federal nº 14.133/2021, que estabelece a preferência pela centralização dos procedimentos de aquisição e contratação de bens e serviços. Também se mostra compatível com o art. 18 da mesma Lei, segundo o qual a fase preparatória da contratação é caracterizada pelo planejamento e deve considerar as questões técnicas, mercadológicas e de gestão que possam interferir na contratação.

Art. 18. A fase preparatória do processo licitatório é caracterizada pelo planejamento e deve compatibilizar-se com o plano de contratações anual de que trata o inciso VII do caput do art. 12 desta Lei, sempre que elaborado, e com as leis orçamentárias, bem como abordar todas as considerações técnicas, mercadológicas e de gestão que podem interferir na contratação, compreendidos.

Art. 19. Os órgãos da Administração com competências regulamentares relativas às atividades de administração de materiais, de obras e serviços e de licitações e contratos deverão:

I - instituir instrumentos que permitam, preferencialmente, a centralização dos procedimentos de aquisição e contratação de bens e serviços;

Assim, ainda que a solução contratada produza efeitos e benefícios para as demais Secretarias Municipais, a presente demanda é formalizada e conduzida de maneira centralizada, cabendo à Secretaria Municipal de Administração e Modernização a coordenação da necessidade, a consolidação das demandas e a gestão da infraestrutura tecnológica relacionada ao objeto, observada a sistemática estabelecida pelo Decreto Municipal nº 359/2023 e as competências administrativas previstas na estrutura organizacional do Município.

Este Termo de Referência, portanto, tem como fundamento principal as conclusões do Estudo Técnico Preliminar, o qual, em sua Declaração de Viabilidade



da Contratação, concluiu pela necessidade e adequação da presente contratação.

Este Termo de Referência, portanto, tem por base, primeiramente, a conclusão do ETP, que na Declaração de Viabilidade ou não da Contratação concluiu:

Com fundamento nas análises técnicas, operacionais, econômicas e mercadológicas realizadas no presente Estudo Técnico Preliminar, conclui-se que a contratação pretendida é viável, mostrando-se adequada para atender às necessidades da Administração Pública Municipal.

O levantamento de mercado demonstrou a existência de fornecedores aptos a executar o objeto, bem como a disponibilidade de soluções compatíveis com as especificações técnicas pretendidas. Da mesma forma, a pesquisa de preços permitirá a definição de valor estimado compatível com os preços praticados no mercado, observados os critérios estabelecidos pela legislação aplicável.

A solução proposta apresenta viabilidade técnica, operacional e econômica, sendo capaz de atender às necessidades relacionadas à proteção da infraestrutura de tecnologia da informação, à continuidade dos serviços públicos, ao fortalecimento da segurança cibernética e ao aprimoramento da gestão da segurança da informação no âmbito do Município.

Além disso, verificou-se que a adoção do Sistema de Registro de Preços, na modalidade Pregão Eletrônico, com julgamento pelo critério de menor preço por lote único, representa a alternativa mais vantajosa para a Administração, conciliando competitividade, eficiência, economicidade e adequada gestão contratual.

Diante do exposto, este Estudo Técnico Preliminar conclui pela viabilidade da contratação, recomendando o prosseguimento do procedimento administrativo, com a elaboração do Termo de Referência e a adoção das demais providências necessárias à realização do procedimento licitatório, observadas as disposições da Lei nº 14.133/2021 e da regulamentação municipal aplicável.

Sendo assim, evidencia-se que o Estudo Técnico Preliminar considerou positiva a viabilidade da contratação em curso, com base no problema a ser resolvido.

No ato da elaboração do Estudo Técnico Preliminar foi observado o art. 85 do Decreto Municipal 359/2023. Conforme já visto.

Sendo assim, o ETP foi elaborado com base nos Documentos de Oficialização de Demanda e Solicitações de Demanda da Secretaria Municipal de Administração e Modernização, com complementações por suporte técnico das demais unidades municipais, mediante juntada de informações documentais e/ou diálogos administrativamente estabelecidos.

3.6. Da Metodologia de Consolidação das Demandas: O presente Termo de Referência é estruturado com base no Estudo Técnico que analisou os Documentos de Oficialização de Demanda (DOD), Documentos de Formalização da Demanda (DFD) e nas solicitações da Secretaria Municipal de Administração e Modernização, contando com suporte técnico e informações complementares das demais unidades

Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



municipais, quando necessário ou quando solicitado. A metodologia adotada assegura que a solução técnica proposta atenda aos requisitos transversais da estrutura administrativa, garantindo a coesão do planejamento e a aderência das especificações às necessidades reais dos órgãos envolvidos.

3.7. Da Comunicação Institucional: Em observância ao disposto no Art. 464 do Decreto Municipal nº 359/2023 e na Lei nº 14.133/2021, foi realizada a consulta às Autarquias (Ager Sinop - Agência Reguladora de Serviços Públicos Delegados do Município de Sinop e Previ Sinop - Instituto de Previdência Social dos Servidores Municipais de Sinop) e à Câmara Municipal acerca da intenção de participação no certame, cujas manifestações e respostas integram os autos deste processo, garantindo a transparência e a oportunidade de adesão à contratação centralizada.

3.7.1. Da Manifestação das Entidades Consultadas: Em resposta à consulta formalizada, as entidades supracitadas informaram não possuir interesse ou necessidade de adesão à presente contratação neste momento, seja por possuírem contratos vigentes para soluções similares, por disporem de infraestrutura própria ou por não vislumbrarem demanda imediata para o objeto deste certame. Dessa forma, a presente licitação prosseguirá focada exclusivamente no atendimento às necessidades das Secretarias Municipais integrantes do Poder Executivo Municipal, conforme definido no planejamento deste ETP.

3.8. Das Justificativas por Unidade Demandante: A estimativa e a necessidade técnica apresentada pela secretaria signatária são justificadas e consolidadas conforme a especificidade de área, detalhada no item 3.1. e 3.1.1.

3.9. Justificativa da adoção do Registro de Preços: Para as futuras contratações será adotado o Sistema de Registro de Preços, previsto na Lei 14.133/2021 como Procedimento Auxiliar no artigo 78, sendo pertinente a adoção do mesmo, sobretudo pelo fato de que, pelas características do objeto em comento, haverá a necessidade de aquisições frequentes, conforme necessidade, para atender a mais de um órgão, com a demanda centralizada na Secretaria de Administração e Modernização. Confirma-se ainda, que é conveniente a aquisição com previsão de ser de forma parcelada e pela impossibilidade de prever com exatidão a quantidade a ser demandada, visando minimizar os riscos de desabastecimento e reduzir os custos necessários.

Conforme o Decreto Municipal 359/2023, no Art. 460, § 1º, o Sistema de Registro de Preços poderá ser usado e será pertinente nas seguintes situações:



- I. Quando, pelas características do bem ou serviço, houver necessidade de contratações frequentes, caso em que poderá ser adotado o sistema de registro de preços permanente como forma de aproveitamento da fase de planejamento da contratação;
- II. Quando for mais conveniente a aquisição de bens com entrega parcelada ou contratação eventual de serviços remunerados por unidade de medida;
- III. Quando for conveniente a aquisição ou a locação de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade, por meio de contratação compartilhada;
- IV. Quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.

Art. 460. O sistema de Registro de Preços poderá ser usado, quando pertinente, para:

§ 1º Entende-se como pertinente a utilização do Sistema de Registro de Preços nas seguintes situações:

I - Quando, pelas características do bem ou serviço, houver necessidade de contratações frequentes, caso em que poderá ser adotado o sistema de registro de preços permanente como forma de aproveitamento da fase de planejamento da contratação;

II - Quando for mais conveniente a aquisição de bens com entrega parcelada ou contratação eventual de serviços remunerados por unidade de medida;

III - Quando for conveniente a aquisição ou a locação de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade, por meio de contratação compartilhada;

IV - Quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração; e

Nesse sentido, corrobora-se que, além de viável e pertinente a opção por Registro de Preços por meio de Pregão Eletrônico, a referida licitação, que tem por objeto contratação de empresa especializada para prestação de serviços, visando estabelecer medidas técnicas e de segurança aptas a proteger os dados e as informações coletados, tratados e utilizados pelo Município de Sinop-MT se enquadra como tal, conforme o §1º do Art. 460 do Decreto Municipal 359/2023.

3.10. Justificativa da licitação por grupo, lote único: A referida licitação será realizada por grupo (lote único), em razão da natureza sistêmica e integrada da solução de segurança da informação pretendida. A contratação reúne componentes de hardware, software, licenças, subscrições e serviços especializados que deverão operar de forma integrada, observadas as especificações técnicas e os requisitos de interoperabilidade estabelecidos no edital e no Termo de Referência.



Dessa forma, a subdivisão do objeto entre diferentes empresas poderá aumentar a complexidade da implantação, da integração, do gerenciamento e da fiscalização contratual, além de dificultar a definição de responsabilidades em situações que envolvam mais de um componente da solução. A concentração da execução em um único fornecedor permite estabelecer responsabilidade técnica unificada pela implantação, configuração, integração, suporte e manutenção da solução.

A licitação por grupo mostra-se, portanto, a alternativa mais adequada para assegurar a eficiência operacional e a gestão integrada da solução, especialmente pelos seguintes aspectos:

Unificação da Responsabilidade: a responsabilidade pela implantação, suporte e manutenção da solução será centralizada, reduzindo conflitos de competência e facilitando a identificação e correção de eventuais falhas;

Integração Tecnológica: os componentes deverão operar de forma compatível e integrada, permitindo o compartilhamento de políticas, informações e mecanismos de segurança, independentemente da marca ofertada, desde que comprovado o atendimento aos requisitos estabelecidos pela Administração;

Eficiência na Gestão de Riscos: a centralização da operação possibilita maior controle sobre os mecanismos de proteção, monitoramento e resposta a incidentes, facilitando a atuação da equipe técnica responsável pela infraestrutura de tecnologia da informação do Município.

Dito isso, é importante observar a definição de Estudo Técnico Preliminar (ETP), conforme o art. 2º, inciso IX, do Decreto Municipal nº 359/2023:

DECRETO Nº 359/2023 - DATA: 22 DE DEZEMBRO DE 2023
Regulamenta as regras e diretrizes de Licitações de que trata a Lei Federal nº 14.133, de 01 de abril de 2021, no âmbito da Administração Pública Municipal de SINOP/MT, e da outras providências.

CAPÍTULO II - DAS DEFINIÇÕES

Art. 2º Para efeito deste Decreto adotam-se as seguintes definições:
IX - Estudo Técnico Preliminar - ETP: documento constitutivo da primeira etapa do planejamento de uma contratação que caracteriza o interesse público envolvido e a sua melhor solução, demonstrando a real necessidade que justifica a contratação ou aquisição, analisando a viabilidade técnica de implementá-la, bem como, construindo toda a estrutura básica para a elaboração do Anteprojeto, do Termo de Referência ou do Projeto Básico;

Diante do exposto, considerando as características técnicas e operacionais da solução pretendida, a necessidade de integração entre seus componentes, a



centralização da gestão da infraestrutura de segurança da informação e a concentração da responsabilidade pela implantação, configuração, suporte e manutenção, conclui-se que a contratação em grupo, mediante lote único, mostra-se a alternativa mais adequada para o atendimento do interesse público.

A adoção dessa forma de contratação busca assegurar a interoperabilidade dos componentes, a continuidade e disponibilidade dos serviços, a eficiência na gestão da solução e a definição clara de responsabilidades perante a Administração, sem prejuízo da competitividade do certame, uma vez que será admitida a apresentação de soluções equivalentes, desde que comprovadamente atendam aos requisitos técnicos, de compatibilidade, interoperabilidade e desempenho estabelecidos no edital e no Termo de Referência

3.11. Justificativa das assinaturas do Termo de Referência: O presente Termo de Referência possui duas assinaturas, sendo uma do servidor integrante da Equipe de Planejamento e Pesquisa de Preços, designada por meio da Portaria nº 571/2026, e outra de servidor integrante da área técnica de Tecnologia da Informação, cuja participação decorre de designação específica para atuação na especificação técnica dos itens, em apoio à Comissão Permanente de Licitações e aos Pregoeiros.

A assinatura do servidor integrante da área técnica de Tecnologia da Informação não implica sua inclusão ou substituição como membro da Equipe de Planejamento responsável pela elaboração do Termo de Referência, mas representa sua manifestação técnica quanto aos aspectos relacionados à especificação, características e requisitos técnicos dos serviços de Tecnologia da Informação que compõem a contratação.

Dessa forma, a participação do servidor da área técnica encontra fundamento na necessidade de que a elaboração dos documentos da contratação conte com o apoio dos profissionais que detenham conhecimento técnico específico acerca do objeto, especialmente considerando a natureza especializada da presente contratação, que envolve soluções de segurança da informação, infraestrutura de rede, gerenciamento, proteção de endpoints, proteção de aplicações, análise de logs e demais serviços correlatos.

Assim, as assinaturas constantes do presente Termo de Referência possuem finalidades distintas e complementares: a primeira representa a atuação da Equipe de Planejamento na elaboração e consolidação do documento, enquanto a segunda representa o apoio e a validação técnica da área especializada quanto às características e especificações do objeto.



A participação técnica do servidor do CPD, portanto, não altera a responsabilidade atribuída à Equipe de Planejamento pela elaboração do Termo de Referência, mas assegura que os requisitos técnicos estabelecidos estejam adequadamente alinhados às necessidades da Administração e às características do objeto pretendido.

É fundamental observar o regramento completo disposto no decreto Municipal 359/2023.

Vejamos:

Art. 142. O Termo de Referência/Projeto Básico será elaborado por uma equipe de planejamento de contratação, designada por portaria, que reúna as competências necessárias sobre aspectos técnicos e de uso comum do objeto, licitações e contratos, dentre outros, e seguirá as informações já determinadas pela área demandante e/ou gestora na Solicitação da Demanda/Documento de Formação de Demanda e Estudo Técnico Preliminar, bem como a Pesquisa de Preços realizada em etapas anteriores, **a fim** de orientar a equipe de licitação para a elaboração do Edital e a condução do certame.

§ 1º. Considerando a complexidade e infinidade de objetos a serem contratados que não são conhecidos com profundidade pelos responsáveis designados pela elaboração do Termo de Referência, **estes** deverão ser auxiliados pela área demandante, através da sua área requisitante ou área técnica, de acordo com o objeto, ou **pela** área gestora quando se tratar de licitação para todas as unidades da mesma Administração Pública Municipal.

O processo em tela é rotineiro para a Administração Pública Municipal, sendo realizado ao longo dos anos e contando, em algumas oportunidades, ou com a participação e análise de todas as Secretarias Municipais, ou com a análise e participação centralizada, desde a provocação de abertura do processo de levantamento. Chamamos a atenção para o fato de que os servidores lotados nas secretarias municipais, ao atuarem próximos dos fiscais de atas e contratos, têm a oportunidade de observar problemas durante a execução e podem solicitar auxílio técnico para melhor especificação dos itens ou demais necessidades no momento da elaboração de uma nova demanda, seja no Planejamento de Contratações Anual (PCA) ou nos documentos iniciais do processo.

Embora o art. 142 determine que o Termo de Referência seja elaborado por uma equipe de planejamento de contratação, esse dispositivo deve ser considerado em conjunto com o art. 85 e 103, que estabelecem regras específicas para a elaboração do Estudo Técnico Preliminar para as contratações de itens de consumo comuns, sistêmicos e de uso geral para todos os órgãos da Administração Pública.

Vejamos:



Art. 85. Nas contratações de itens de consumo comuns, sistêmicos e **de uso geral a todos os órgãos** da mesma Administração Pública ou que tenham sido objeto de planejamento anual, as Solicitações de Demanda/Documento de Formação de Demanda deverão partir de forma individualizada de cada uma das áreas demandantes para a Área Gestora, que ficará responsável por coordenar, padronizar e supervisionar o processo de contratação, assim como será **responsável por elaborar** o Estudo Técnico Preliminar.

Parágrafo único. No âmbito do Poder Executivo Municipal, a Área Gestora será de responsabilidade da Diretoria Executiva de Administração.

Art. 103. Após a realização da Solicitação da Demanda/Documento e Formação de Demanda e do Estudo Técnico Preliminar, a Área Demandante deverá realizar a pesquisa de preços que, após finalizada, será anexada, em documento apartado, ao Estudo Técnico Preliminar, dando sequência à elaboração do Termo de Referência/Projeto Básico.

Parágrafo único. Nos casos em que se tratar de contratações de itens de consumo comuns, sistêmicos e **de uso geral a todos os órgãos** da mesma Administração Pública ou que tenham sido objeto de planejamento anual, após a realização da Solicitação da Demanda/Documento e Formação de Demanda, caberá à Área Gestora **a realização do Estudo Técnico Preliminar e a realização da Pesquisa de Preços, que, após finalizada, será anexada, em documento apartado, ao Estudo Técnico Preliminar, dando sequência à elaboração do Termo de Referência/Projeto Básico.**

Dito isso, é importante observarmos a definição de Estudo Técnico Preliminar (ETP), conforme o art. 2º, inciso IX:

"Documento constitutivo da primeira etapa do planejamento de uma contratação que caracteriza o interesse público envolvido e a sua melhor solução, demonstrando a real necessidade que justifica a contratação ou aquisição, analisando a viabilidade técnica de implementá-la, bem como construindo toda a estrutura básica para a elaboração do Anteprojeto, do Termo de Referência ou do Projeto Básico."

Nessa toada, **é necessário** analisar a definição de Termo de Referência (TR), conforme o art. 2º, inciso XVIII:

"Instrumento de planejamento, pertencente à fase preparatória do processo licitatório, elaborado a partir dos estudos técnicos preliminares, com elementos necessários e suficientes capazes de caracterizar com precisão e informar a terceiros a aquisição de bens e a contratação de serviços comuns."

Seguindo a análise do regramento, chamamos a atenção para os critérios de pesquisa de preços, especialmente o previsto no art. 133:

Art. 133. No âmbito do Poder Executivo Municipal, a pesquisa de preços será realizada pela Área Demandante, posterior à Solicitação da Demanda/Documento e Formação de Demanda e Estudo Técnico Preliminar.



Parágrafo único. Nos casos em que se tratar de contratações de itens de consumo comuns, sistêmicos e de uso geral a todos os órgãos da mesma Administração Pública ou que tenham sido objeto de Planejamento Anual, a Pesquisa de Preços ficará sob a responsabilidade da Diretoria Executiva de Administração, designada como Área Gestora da Administração Pública.

Dessa forma, observa-se que o Departamento de Pré-Licitação, responsável pela elaboração do Termo de Referência, está lotado na Diretoria Executiva de Administração, que é a responsável por coordenar, padronizar e supervisionar o processo, além de elaborar o Estudo Técnico Preliminar em conjunto com a(s) área(s) demandante(s). O Departamento de Pré-Licitação também procedeu com a pesquisa de preços.

Portanto, a elaboração do presente Termo de Referência, utilizando como base as informações elencadas pelos técnicos lotados nas Secretarias Municipais e descritas nos Estudos Técnicos Preliminares, bem como contando com a participação da área técnica especializada de Tecnologia da Informação para a análise e especificação dos aspectos técnicos do objeto, encontra-se de acordo com a legislação vigente e com o regramento aplicável a este tipo de contratação.

As assinaturas apostas no presente Termo de Referência possuem, portanto, caráter complementar, correspondendo à atuação da Equipe de Planejamento e à manifestação técnica da área especializada, conforme as respectivas designações administrativas, não se fazendo necessária a constituição de uma equipe específica exclusivamente para esta contratação.

Para fins de formalização, ficam definidos para assinatura do presente Termo de Referência:

Daniel Jose Sepi de Lima - Matrícula nº 7230: integrante da equipe técnica de Tecnologia da Informação, designada pela Portaria nº 0172/2021;

Gabriel Araújo da Silva - Matrícula nº 18702-1: integrante da Equipe de Planejamento e Pesquisa de Preços, designada pela Portaria nº 571/2026.

4. DESCRIÇÃO DA SOLUÇÃO (QUANDO APLICÁVEL)

A solução pretendida consiste na contratação de empresa especializada para prestação de serviços de segurança da informação, compreendendo o fornecimento, implantação, configuração, integração, suporte técnico, manutenção preventiva e corretiva, atualização tecnológica, monitoramento e gerenciamento de solução



corporativa destinada à proteção da infraestrutura de tecnologia da informação do Município de Sinop-MT.

A contratação abrangerá o fornecimento de equipamentos do tipo appliance, licenças, subscrições, softwares, plataformas tecnológicas e serviços técnicos necessários ao pleno funcionamento e à manutenção da solução durante o período em que os serviços e soluções estiverem efetivamente contratados e em execução, observadas as especificações técnicas que serão detalhadas no Termo de Referência.

A solução deverá contemplar, de forma integrada, mecanismos de proteção perimetral da rede, gerenciamento centralizado dos equipamentos de segurança, análise e armazenamento de eventos (logs), proteção de estações de trabalho e servidores contra ameaças cibernéticas, proteção das aplicações disponibilizadas em ambiente web, bem como serviços especializados de implantação, configuração, migração (quando aplicável), suporte técnico e manutenção da solução.

A infraestrutura deverá operar de forma integrada, quando aplicável à composição da solução demandada, permitindo o compartilhamento de políticas de segurança, inteligência contra ameaças, monitoramento contínuo, gerenciamento centralizado e resposta a incidentes, proporcionando maior eficiência operacional, disponibilidade dos serviços, rastreabilidade dos eventos de segurança e redução dos riscos relacionados à indisponibilidade dos sistemas e ao comprometimento das informações institucionais.

A solução também deverá possibilitar escalabilidade tecnológica, permitindo sua evolução conforme o crescimento da infraestrutura computacional do Município, sem comprometer a compatibilidade entre seus componentes, garantindo maior vida útil ao investimento realizado pela Administração Pública.

Além do fornecimento da solução tecnológica, a contratação deverá contemplar serviços especializados de suporte técnico, atualizações de software e firmware, atendimento às ocorrências, substituição de equipamentos quando necessário, acompanhamento técnico e demais atividades indispensáveis à manutenção da disponibilidade, desempenho e segurança da infraestrutura de tecnologia da informação.

Por se tratar de solução corporativa de segurança da informação, sua gestão será realizada de forma centralizada pela Secretaria Municipal de Administração e Modernização, responsável pela administração da infraestrutura tecnológica do Município. Embora a gestão contratual permaneça concentrada nessa unidade administrativa, os benefícios decorrentes da contratação alcançarão toda a

Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



Administração Pública Municipal, proporcionando maior padronização tecnológica, fortalecimento da segurança cibernética, otimização da gestão dos ativos de tecnologia da informação e continuidade dos serviços públicos suportados por recursos tecnológicos.

Dessa forma, a solução proposta atende às necessidades identificadas durante o planejamento da contratação, apresentando-se como alternativa tecnicamente adequada, operacionalmente eficiente e compatível com os objetivos institucionais da Administração Pública Municipal, garantindo elevados níveis de disponibilidade, integridade, confidencialidade e segurança das informações tratadas pelo Município.

De forma resumida, os principais componentes da solução e suas respectivas funções são apresentados a seguir:

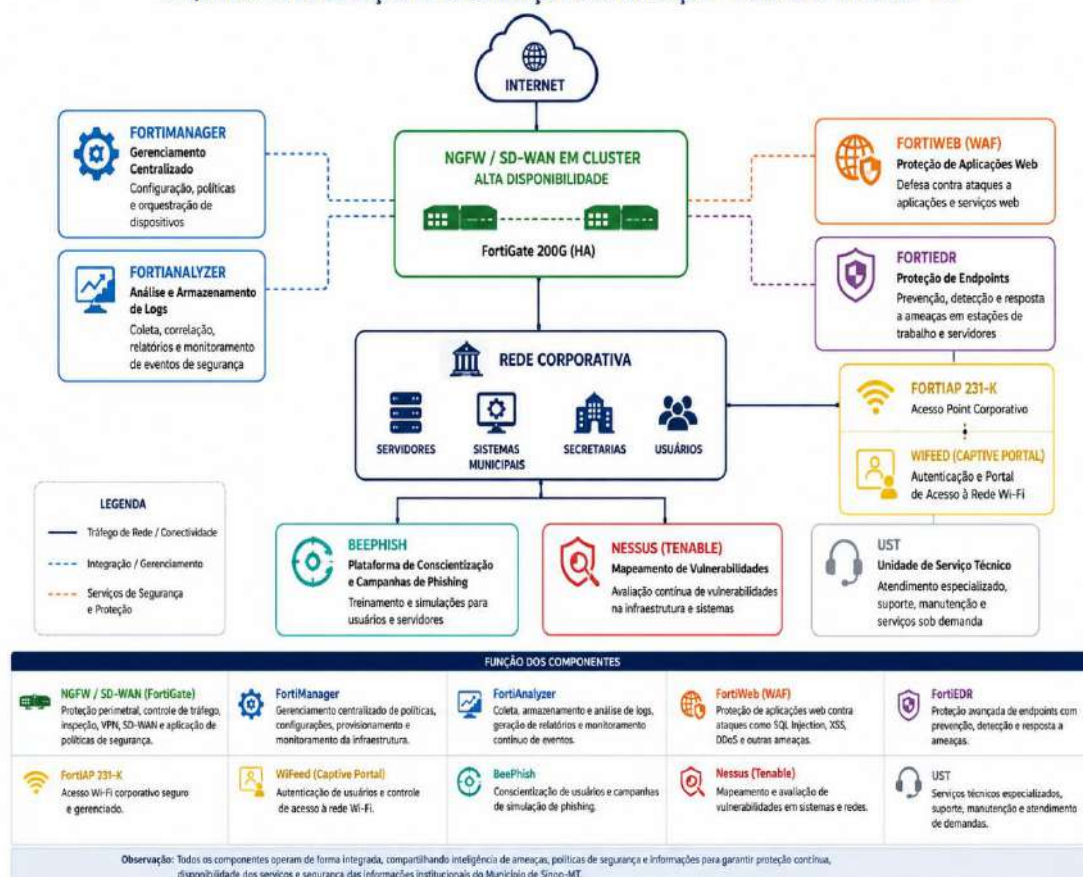
COMPONENTE	FUNÇÃO NA SOLUÇÃO	RELAÇÃO COM A ARQUITETURA
NGFW/SD-WAN	Proteção perimetral, controle de tráfego e conectividade	Atua como principal camada de proteção e controle do tráfego entre a rede interna e as redes externas, constituindo o núcleo da segurança perimetral.
FortiManager	Gerenciamento centralizado de políticas e equipamentos	Centraliza a administração, configuração e aplicação de políticas dos equipamentos de segurança, reduzindo a complexidade operacional.
FortiAnalyzer	Coleta, armazenamento, análise e monitoramento de logs	Recebe e correlaciona eventos e registros gerados pelos componentes da solução, permitindo monitoramento, análise e rastreabilidade.
FortiWeb	Proteção das aplicações e serviços web	Atua como camada de proteção das aplicações disponibilizadas em ambiente web, complementando a proteção realizada pelo NGFW.
FortiEDR	Proteção de endpoints e servidores	Estende a proteção da arquitetura para estações de trabalho e servidores, atuando diretamente nos dispositivos finais.
FortiAP	Conectividade de rede sem fio corporativa	Proporciona acesso à rede sem fio corporativa, integrando os dispositivos de acesso à infraestrutura de rede e às políticas de segurança.
Captive Portal	Autenticação e gerenciamento do acesso à rede	Atua no controle e autenticação dos usuários que acessam a rede, complementando os mecanismos de controle de acesso.
Plataforma de conscientização e phishing	Conscientização dos usuários e campanhas de segurança	Atua na camada de pessoas e processos, reduzindo riscos associados a comportamentos inadequados e ataques de engenharia social.



Plataforma de avaliação de vulnerabilidades	Identificação, avaliação e mapeamento de vulnerabilidades	Permite identificar vulnerabilidades na infraestrutura tecnológica, subsidiando ações preventivas e corretivas de segurança.
UST	Atividades técnicas especializadas sob demanda	Complementa toda a arquitetura por meio de suporte, configuração, manutenção, ajustes e demais intervenções técnicas necessárias ao funcionamento da solução.

Os componentes apresentados possuem funções complementares e poderão ser acionados de forma individual ou integrada, conforme a necessidade da Administração. Quando a demanda envolver componentes que dependam de integração entre si, caberá à contratada assegurar a interoperabilidade, a configuração e o pleno funcionamento do conjunto, observadas as especificações estabelecidas no Termo de Referência.

ARQUITETURA DA SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO – MUNICÍPIO DE SINOP-MT



- IMAGEM ILUSTRATIVA DISPONÍVEL NO ESTUDO TÉCNICO PRELIMINAR - ETP. LOCALIZADA NO TÓPICO 8. “DESCRIÇÃO DA SOLUÇÃO COMO UM TODO”, PÁGINA 40 (QUARENTA) DO DOCUMENTO EM PDF/DIGITAL.



5. REQUISITOS DO OBJETO DA CONTRATAÇÃO

5.1. Natureza do Objeto: A presente contratação tem por objeto a prestação de serviços especializados de segurança da informação, compreendendo o fornecimento e a disponibilização dos equipamentos, licenças, softwares, plataformas e demais recursos necessários, bem como a implantação, instalação, configuração, integração, suporte técnico, manutenção, atualização tecnológica, gerenciamento, monitoramento e demais serviços indispensáveis ao pleno funcionamento de solução corporativa destinada à proteção da infraestrutura de tecnologia da informação do Município de Sinop-MT.

5.1.1. A solução de segurança da informação será composta, conforme os itens efetivamente demandados pela Administração, por:

- equipamentos do tipo appliance;
- licenças de uso e subscrições;
- softwares e plataformas especializadas;
- serviços de implantação, configuração, integração e ativação;
- suporte técnico e manutenção;
- serviços de monitoramento e gerenciamento;
- serviços de avaliação de vulnerabilidades e conscientização em segurança da informação; e
- demais recursos necessários ao pleno funcionamento da solução.

5.1.2. Os componentes da solução possuem funções distintas e complementares, compondo diferentes camadas da arquitetura corporativa de segurança da informação do Município, incluindo, conforme aplicável:

- proteção perimetral da rede;
- gerenciamento centralizado dos recursos de segurança;
- monitoramento e análise de eventos;
- proteção de estações de trabalho e servidores;
- segurança de aplicações disponibilizadas em ambiente web;
- conectividade sem fio corporativa;
- avaliação de vulnerabilidades;
- conscientização em segurança da informação; e
- suporte técnico especializado.



5.1.3. A composição da solução será definida conforme a necessidade da Administração, não sendo obrigatória a utilização simultânea de todos os componentes em cada solicitação, observados os itens e quantitativos estabelecidos neste Termo de Referência.

5.1.4. Os componentes que integrarem uma mesma solicitação deverão operar de forma compatível e interoperável, cabendo à CONTRATADA assegurar a adequada integração entre os recursos disponibilizados, observados os requisitos técnicos estabelecidos neste Termo de Referência.

5.1.5. Da responsabilidade pela disponibilização e funcionamento:

5.1.5.1. A CONTRATADA será responsável por disponibilizar todos os recursos necessários à execução dos serviços contratados, incluindo, quando aplicável:

- equipamentos e appliances;
- acessórios;
- componentes;
- módulos;
- cabos;
- fontes de alimentação;
- suportes;
- cases;
- antenas;
- licenças;
- subscrições;
- softwares;
- plataformas; e
- demais recursos materiais ou tecnológicos necessários ao funcionamento da solução.

5.1.5.2. Os recursos necessários à execução dos serviços deverão ser disponibilizados pela CONTRATADA ainda que não estejam individualmente relacionados no quantitativo dos itens, quando forem indispensáveis à instalação, configuração, integração ou funcionamento da solução contratada.

5.1.5.3. Não caberá à Administração providenciar separadamente equipamentos, componentes, acessórios ou outros recursos indispensáveis à operacionalização dos serviços que sejam de responsabilidade da CONTRATADA.



5.1.5.4. Sempre que houver solicitação da Administração, a solução correspondente deverá ser disponibilizada de forma completa, instalada, configurada, integrada, testada e em pleno funcionamento, conforme aplicável ao respectivo item.

5.1.6. Da contratação em lote único e da responsabilidade integral:

5.1.6.1. A contratação será realizada em lote único, abrangendo os 11 (onze) itens que compõem a solução de segurança da informação.

5.1.6.2. Caberá à CONTRATADA assegurar, relativamente aos componentes que forem demandados:

- compatibilidade;
- interoperabilidade;
- integração;
- implantação;
- configuração;
- manutenção;
- suporte técnico; e
- pleno funcionamento da solução.

5.1.6.3. A CONTRATADA será a responsável pela coordenação técnica necessária à integração dos componentes da solução, não podendo atribuir à Administração eventual incompatibilidade ou falha de funcionamento entre recursos que compõem os serviços contratados.

5.1.7. Da gestão, fiscalização e acompanhamento técnico:

5.1.7.1. A Secretaria Municipal de Administração e Modernização será responsável pela gestão centralizada da contratação.

5.1.7.2. O Centro de Processamento de Dados - CPD prestará apoio técnico à Administração, podendo:

- acompanhar a execução dos serviços;
- fiscalizar a conformidade da solução;
- realizar verificações técnicas;
- acompanhar instalações e configurações;
- realizar ou acompanhar testes;
- verificar a integração dos componentes; e
- avaliar o pleno funcionamento da solução.

5.1.7.3. O acompanhamento, a fiscalização e a realização de testes pela Administração não transferem, reduzem ou afastam a responsabilidade da



CONTRATADA pela instalação, configuração, integração, manutenção, suporte e funcionamento dos serviços e componentes disponibilizados.

5.1.8. PRAZO DE EXECUÇÃO E DISPONIBILIDADE DO OBJETO: As demandas decorrentes da contratação serão formalizadas pela Secretaria Municipal de Administração e Modernização, mediante emissão da respectiva Nota de Autorização de Despesa - NAD, observados os procedimentos administrativos e autorizações pertinentes.

5.1.8.1. IMPLANTAÇÃO INICIAL DA SOLUÇÃO: A CONTRATADA deverá realizar a *implantação inicial*.

A CONTRATADA deverá realizar a *implantação inicial* da solução de segurança da informação no prazo máximo de **30 (trinta) dias corridos**, contados a partir da emissão da Ordem de Início dos Serviços.

5.1.8.2. O prazo de implantação inicial compreenderá todas as etapas necessárias à disponibilização da solução em pleno funcionamento, incluindo, conforme aplicável, o planejamento técnico, instalação física dos equipamentos, configuração, parametrização, integração, ativação, realização de testes, homologação e demais procedimentos necessários à adequada entrada em operação da solução.

5.1.8.3. Após a implantação inicial da solução, as demandas decorrentes da contratação deverão ser atendidas pela CONTRATADA no prazo máximo de **48 (quarenta e oito) horas** corridas, contado a partir do recebimento da respectiva NAD, observadas as condições estabelecidas neste Termo de Referência.

5.1.8.4. A CONTRATADA deverá atender cada demanda no prazo máximo de **48 (quarenta e oito) horas** corridas, contado a partir do recebimento da NAD, **ressalvado o prazo específico estabelecido para a implantação inicial da solução** (subitem 5.1.8.1 previsto neste presente tópico de PRAZO DE EXECUÇÃO E DISPONIBILIDADE DO OBJETO).

5.1.8.5. O prazo de **48 (quarenta e oito) horas** corridas compreenderá, para as demandas cuja execução não esteja abrangida pelo prazo de implantação inicial (subitem 5.1.8.1.), todas as providências necessárias à efetiva disponibilização da solução solicitada, incluindo, conforme aplicável:

- fornecimento/disponibilização dos equipamentos e demais recursos necessários;
- instalação;
- configuração;
- parametrização;
- integração;



- ativação;
- realização de testes; e
- disponibilização da solução em pleno funcionamento.

5.1.8.6. A simples entrega ou disponibilização física de equipamentos, licenças, softwares ou componentes não será considerada conclusão da demanda, quando forem necessárias instalação, configuração, integração, ativação ou outras providências técnicas para o funcionamento da solução.

5.1.8.7. A demanda será considerada concluída somente quando a solução estiver instalada, configurada, testada, operacional e apta à utilização pela Administração, observados os requisitos e especificações estabelecidos neste Termo de Referência.

5.1.8.8. A CONTRATADA será responsável por providenciar, dentro do prazo estabelecido, todos os recursos necessários à execução da demanda, inclusive equipamentos, licenças, softwares, acessórios, componentes, materiais e demais recursos indispensáveis ao funcionamento da solução.

5.1.8.9. O Centro de Processamento de Dados - CPD, com apoio dos servidores responsáveis pela fiscalização, poderá acompanhar a execução e realizar verificações e testes destinados a confirmar a conformidade e o pleno funcionamento da solução.

5.1.8.10. A constatação de falhas ou inconsistências durante a instalação, configuração ou testes deverá ser imediatamente comunicada pela CONTRATADA à Administração, acompanhada da justificativa e das providências necessárias para sua correção.

5.1.9. Da integralidade da execução:

5.1.9.1. A CONTRATADA será responsável pela execução integral dos serviços correspondentes aos itens efetivamente solicitados pela Administração, incluindo todas as atividades, recursos e providências necessárias à sua disponibilização e funcionamento, ainda que determinadas etapas não estejam individualmente discriminadas na solicitação.

5.1.9.2. A disponibilização de equipamentos, appliances, licenças, softwares, plataformas, acessórios e demais componentes pela CONTRATADA não caracteriza aquisição ou transferência de propriedade à Administração, permanecendo tais recursos sob responsabilidade e propriedade da CONTRATADA durante a execução, conforme a natureza de cada solução.

5.1.9.3. A aceitação ou o recebimento dos serviços pela Administração não afasta a responsabilidade da CONTRATADA pela correção de falhas, desconformidades ou



defeitos identificados posteriormente, observados os prazos, níveis de serviço e demais condições estabelecidos neste Termo de Referência.

5.1.10. Da prorrogação do prazo

5.1.10.1. Quando houver motivo técnico devidamente justificado que impossibilite o atendimento da demanda no prazo de **48 (quarenta e oito) horas corridas**, a CONTRATADA deverá solicitar a prorrogação antes do término do prazo originalmente estabelecido, mediante apresentação de justificativa circunstanciada e indicação do prazo adicional necessário.

5.1.10.2. O pedido de prorrogação será submetido à análise da Administração, que poderá deferi-lo ou indeferi-lo, considerando a justificativa apresentada, as circunstâncias da demanda e o impacto sobre a continuidade dos serviços.

5.1.10.3. A eventual concessão de prazo adicional não afasta a responsabilidade da CONTRATADA pela adoção das medidas necessárias à conclusão da demanda no menor prazo possível.

5.1.11. Os prazos e níveis de serviço específicos relativos a atendimento de chamados, criticidade de incidentes, solução de contorno, substituição de equipamentos, suporte técnico, manutenção, monitoramento e demais serviços observarão os requisitos estabelecidos nas respectivas seções deste Termo de Referência.

5.1.12. DA FORMA DE FORNECIMENTO E EXECUÇÃO DO OBJETO

5.1.12.1. A contratação será realizada mediante Ata de Registro de Preços - ARP, com **vigência de um (1) ano**, durante a qual os serviços poderão ser solicitados de forma parcelada, conforme a necessidade da Administração e observados os quantitativos e condições estabelecidos no Edital e neste Termo de Referência.

5.1.12.2. A gestão administrativa da Ata será centralizada na Secretaria Municipal de Administração e Modernização, responsável pela consolidação das demandas relacionadas à infraestrutura de tecnologia da informação do Município, com apoio técnico do Centro de Processamento de Dados - CPD.

5.1.12.3. As demais Secretarias e unidades administrativas serão atendidas por meio da gestão centralizada da contratação, não sendo necessária a realização de contratações individualizadas por unidade.

5.1.12.4. Das solicitações

As solicitações dos serviços registrados serão realizadas conforme a necessidade da Administração, mediante:

- emissão da Nota de Autorização de Despesa - NAD;



- observância das autorizações administrativas pertinentes;
- indicação dos itens e quantitativos necessários; e
- demais procedimentos internos aplicáveis.

5.1.12.5. A existência da Ata de Registro de Preços não obriga a Administração à contratação integral dos quantitativos registrados, ficando a utilização dos serviços condicionada à efetiva necessidade administrativa e aos limites estabelecidos na Ata e no instrumento convocatório.

5.1.12.6. As demandas poderão ocorrer de forma parcelada e variável durante a vigência da Ata, conforme as necessidades identificadas e consolidadas pela Secretaria Municipal de Administração e Modernização.

5.1.12.7. Da execução dos serviços

5.1.12.7.1. A CONTRATADA será responsável pela execução integral dos serviços efetivamente solicitados, incluindo, conforme aplicável:

- disponibilização dos equipamentos e appliances;
- disponibilização de licenças, subscrições, softwares e plataformas;
- fornecimento dos acessórios e componentes necessários;
- instalação;
- configuração;
- parametrização;
- integração;
- ativação;
- realização de testes;
- suporte técnico;
- manutenção; e
- demais providências necessárias ao pleno funcionamento da solução.

5.1.12.7.2. A solicitação de apenas parte dos itens que compõem a solução não afasta a responsabilidade da CONTRATADA pela compatibilidade, interoperabilidade e adequado funcionamento dos componentes efetivamente demandados.

5.1.12.7.3. Quando a execução de determinado item depender de integração com outros recursos da solução, caberá à CONTRATADA realizar os procedimentos técnicos necessários à adequada integração e ao pleno funcionamento do conjunto.

5.1.12.7.4. A execução dos serviços deverá observar os requisitos, especificações técnicas, prazos e níveis de serviço estabelecidos neste Termo de Referência.

5.1.12.8. Dos Itens 2 e 7



5.1.12.8.1. Para os Itens 2 e 7, cuja medição considera unidade-mês, a capacidade contratada corresponde a até 15 (quinze) pontos/unidades simultaneamente, pelo período estimado de 12 (doze) meses.

5.1.12.8.2. O quantitativo de 180 (cento e oitenta) unidade-mês corresponde à memória de cálculo de 15 (quinze) unidades × 12 (doze) meses, não representando prazo de execução ou vigência contratual de 180 meses.

5.1.12.8.3. O valor mensal estabelecido para os Itens 2 e 7 corresponde à disponibilização da respectiva solução para até 15 (quinze) pontos/unidades, não havendo alteração do valor mensal em razão da utilização de quantidade inferior ou igual ao limite de capacidade contratado.

5.1.12.9. Do acompanhamento e da fiscalização

5.1.12.9.1. A Secretaria Municipal de Administração e Modernização será responsável pela gestão da contratação, com apoio técnico do Centro de Processamento de Dados - CPD.

5.1.12.9.2. O CPD e os agentes responsáveis pela fiscalização poderão:

- acompanhar a execução dos serviços;
- verificar o atendimento das especificações;
- acompanhar instalações e configurações;
- realizar ou acompanhar testes técnicos;
- verificar a disponibilidade e o funcionamento da solução; e
- registrar eventuais inconformidades.

5.1.12.9.3. O acompanhamento e a fiscalização realizados pela Administração não transferem nem reduzem a responsabilidade da CONTRATADA pela execução, instalação, configuração, integração, manutenção, suporte e funcionamento dos serviços contratados.

5.1.13. Providências a serem adotadas pela Administração previamente à celebração do contrato: Previamente e durante a execução das contratações decorrentes da Ata de Registro de Preços, a Administração deverá adotar as providências necessárias à adequada execução da solução, incluindo a designação dos responsáveis pela gestão e fiscalização, a formalização das demandas mediante os instrumentos administrativos pertinentes, a emissão da Nota de Autorização de Despesa - NAD, a disponibilização dos acessos e informações necessárias à execução dos serviços, o acompanhamento técnico das atividades pelo CPD, o acompanhamento da instalação e configuração dos componentes, a realização de



verificações e testes técnicos, o recebimento e acompanhamento da solução disponibilizada e a participação dos servidores indicados nos treinamentos previstos.

5.1.13.1. A gestão e o acompanhamento técnico da solução permanecerão centralizados na Secretaria Municipal de Administração e Modernização, por meio da unidade responsável pela infraestrutura de tecnologia da informação, sem prejuízo da atuação dos fiscais e demais responsáveis formalmente designados. As demandas das demais unidades administrativas serão consolidadas e encaminhadas pela unidade centralizadora, conforme a necessidade identificada.

5.1.14. Providências a serem adotadas pela Contratada previamente à celebração do contrato: A contratada será responsável por fornecer todos os equipamentos, licenças, subscrições, softwares, componentes, acessórios e demais recursos necessários à plena execução dos serviços contratados, ainda que determinados componentes acessórios não estejam individualmente discriminados nos quantitativos do objeto, desde que sejam indispensáveis ao funcionamento da solução ofertada e estejam abrangidos pelas especificações e obrigações estabelecidas no Termo de Referência.

5.1.14.1. Caberá à contratada realizar, conforme a demanda formalizada pela Administração, a entrega, instalação, configuração, integração, quando aplicável, realização dos testes necessários, disponibilização para uso, suporte técnico, manutenção e demais atividades necessárias ao pleno funcionamento da solução.

5.1.14.2. A responsabilidade pela disponibilização e funcionamento da solução permanecerá integralmente com a contratada, não sendo atribuída à Administração a obrigação de fornecer equipamentos, cabos, fontes, racks, cases, módulos, antenas, acessórios ou outros componentes necessários à instalação e operacionalização dos serviços, ressalvados os recursos de infraestrutura expressamente disponibilizados pela Administração e previstos no Termo de Referência.

5.1.15. Providências a serem adotadas pela Contratada - Visita Técnica e Acompanhamento da Solução:

5.1.15.1. Da visita técnica presencial e acompanhamento da solução

5.1.15.1.1. Durante a execução dos serviços, a CONTRATADA deverá realizar no mínimo 01 (uma) visita técnica presencial por mês à estrutura da Administração, em local e data previamente acordados com a Secretaria Municipal de Administração e Modernização.

5.1.15.1.2. A visita técnica terá como objetivos:

- acompanhar as condições de funcionamento da solução;



- verificar as condições da infraestrutura relacionada aos serviços contratados;
- identificar eventuais necessidades de ajustes, correções ou melhorias;
- prestar orientações técnicas relacionadas à utilização e operação da solução;
- esclarecer dúvidas apresentadas pela Administração;
- avaliar eventuais ocorrências ou situações identificadas durante a execução;
- alinhar procedimentos técnicos e operacionais necessários à adequada prestação dos serviços; e
- contribuir para a manutenção da disponibilidade, desempenho, segurança e continuidade da solução.

5.1.15.1.3. Durante a visita, a Administração, por meio dos responsáveis pela gestão e fiscalização da contratação e da equipe técnica do Centro de Processamento de Dados - CPD, poderá apresentar dúvidas, observações, solicitações, reclamações e demais manifestações relacionadas à execução e ao funcionamento dos serviços.

5.1.15.1.4. A visita presencial deverá ser realizada por profissional da CONTRATADA com qualificação técnica compatível com os serviços objeto da contratação, sempre que necessário para o adequado acompanhamento da solução.

5.1.15.1.5. A realização da visita mensal não substitui nem limita os serviços de suporte técnico e atendimento de chamados previstos neste Termo de Referência, especialmente aqueles que, em razão de sua natureza ou criticidade, demandem atendimento em prazo específico.

5.1.15.1.6. A Administração poderá solicitar visitas presenciais adicionais, sempre que identificada necessidade relacionada à execução, funcionamento, manutenção, suporte ou acompanhamento da solução, observados os prazos e condições estabelecidos neste Termo de Referência.

5.1.15.1.7. Cada visita deverá ser registrada pela CONTRATADA, contendo, no mínimo:

- data e horário da visita;
- identificação do profissional responsável;
- atividades realizadas;
- ocorrências identificadas;
- orientações e providências recomendadas; e
- eventuais pendências e respectivos responsáveis.

5.1.15.1.8. O registro da visita deverá ser disponibilizado à fiscalização da contratação para fins de acompanhamento e controle da execução dos serviços.



5.1.15.1.9. A visita técnica prevista neste Termo de Referência constitui obrigação da CONTRATADA durante a execução dos serviços e não será exigida como condição de participação, habilitação ou apresentação de proposta no procedimento licitatório.

5.1.15.1.10. Todos os custos relacionados às visitas presenciais previstas neste Termo de Referência deverão estar incluídos no preço contratado, abrangendo deslocamento, hospedagem, alimentação, mão de obra e demais despesas necessárias à sua realização.

5.2. DA GARANTIA CONTRATUAL

5.2.1. Não será exigida garantia contratual prevista no art. 96 da Lei nº 14.133/2021, considerando as características do objeto, os riscos identificados e os mecanismos de controle e mitigação previstos para a contratação.

5.2.2. A não exigência de garantia contratual considera, especialmente:

- a natureza dos serviços de segurança da informação contratados;
- a execução conforme a necessidade da Administração;
- a disponibilização da solução no prazo máximo de 48 (quarenta e oito) horas corridas após a solicitação;
- a existência de prazos específicos para atendimento de chamados, conforme a criticidade da ocorrência;
- a previsão de solução de contorno para situações emergenciais;
- a obrigação de manutenção e substituição dos equipamentos necessários à prestação dos serviços, inclusive mediante RMA, quando aplicável;
- o acompanhamento e a fiscalização da execução pela Administração, com apoio técnico do CPD;
- a inexistência de pagamento antecipado;
- a realização dos pagamentos condicionada à efetiva execução dos serviços e aos procedimentos de liquidação e pagamento da Administração;
- a possibilidade de aplicação das medidas administrativas e sanções cabíveis em caso de inadimplemento; e
- a responsabilidade da CONTRATADA pela disponibilização, manutenção e substituição dos equipamentos e demais recursos necessários à execução dos serviços.

5.2.3. A ausência de garantia contratual não afasta a responsabilidade da CONTRATADA pelo cumprimento integral das obrigações assumidas, nem prejudica



a aplicação das medidas administrativas, sanções e demais consequências previstas no Edital, neste Termo de Referência e no instrumento contratual.

5.2.4. Eventual atraso, falha, indisponibilidade ou execução inadequada dos serviços ficará sujeito aos procedimentos de fiscalização, correção, aplicação dos níveis de serviço e demais medidas previstas neste Termo de Referência, sem prejuízo das sanções cabíveis.

5.2.4.1. Essas medidas punitivas estão claramente delineadas no regulamento municipal, Decreto 360/2023 e na Lei de Licitação 14.133/2021. Portanto, é imperativo observar com rigor todas as condições do edital para evitar possíveis penalidades, conforme previsto na legislação aplicável.

5.2.5. Os custos decorrentes da execução dos serviços, inclusive aqueles relacionados à disponibilização, manutenção, substituição e suporte dos equipamentos, componentes e demais recursos necessários, deverão estar contemplados nos preços ofertados pela CONTRATADA, conforme as condições estabelecidas neste Termo de Referência.

5.2.6. Dos custos e encargos para a execução do objeto:

5.2.6.1. Os preços contratados deverão contemplar todos os custos necessários à integral execução dos serviços, incluindo, quando aplicáveis, equipamentos, appliances, licenças, subscrições, softwares, acessórios, componentes, módulos, cabos, fontes, suportes, materiais, instalação, configuração, integração, parametrização, testes, ativação, manutenção, substituição, suporte técnico, deslocamentos, mão de obra, encargos trabalhistas, previdenciários e fiscais, tributos, seguros, transporte e demais despesas direta ou indiretamente relacionadas à execução do objeto.

5.2.6.2. Não será admitida a cobrança de valores adicionais pela disponibilização de recursos ou pela realização de atividades que sejam necessárias ao pleno, adequado e desimpedido funcionamento da solução, ainda que não tenham sido individualmente discriminadas na composição dos quantitativos, desde que sejam inerentes às obrigações estabelecidas neste Termo de Referência.

5.2.6.3. A CONTRATADA será responsável por disponibilizar, às suas expensas, todos os recursos materiais e tecnológicos necessários à execução dos serviços, observadas as condições e especificações estabelecidas neste Termo de Referência.

5.3. DURAÇÃO DO CONTRATO: DA VIGÊNCIA DA ATA DE REGISTRO DE PREÇOS E DOS INSTRUMENTOS DECORRENTES

5.3.1. Da Ata de Registro de Preços

Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



5.3.1.1. A Ata de Registro de Preços - ARP terá **vigência de um (1) ano**, contados da data de sua assinatura, observadas as disposições estabelecidas no Edital e na legislação aplicável, principalmente nos termos do art. 84 da Lei Federal nº 14.133/2021.

Art. 84. O prazo de vigência da ata de registro de preços será de 1 (um) ano e poderá ser prorrogado, por igual período, desde que comprovado o preço vantajoso.

Parágrafo único. O contrato decorrente da ata de registro de preços terá sua vigência estabelecida em conformidade com as disposições nela contidas.

5.3.1.2. Durante a vigência da Ata, os serviços registrados poderão ser solicitados pela Administração de forma parcelada e conforme a efetiva necessidade, observados os quantitativos, preços e demais condições registrados.

5.3.1.3. A existência da Ata de Registro de Preços não obriga a Administração a contratar integralmente os quantitativos registrados, inexistindo garantia de consumo mínimo ou de contratação total dos itens.

5.3.1.3.1. Para as futuras contratações será adotado o Sistema de Registro de Preços (SRP), previsto na Lei nº 14.133/2021 como procedimento auxiliar, nos termos dos arts. 78 e 82 a 86, em consonância com o art. 460 do Decreto Municipal nº 359/2023, mostrando-se pertinente à presente contratação em razão das características dos serviços, da possibilidade de contratações frequentes e prestação de forma parcelada, conforme a necessidade da Administração, bem como da demanda centralizada pela Secretaria Municipal de Administração e Modernização para atendimento das diferentes Secretarias e unidades administrativas do Município, e da impossibilidade de determinar previamente, com exatidão, o momento e o quantitativo efetivo de cada demanda durante a vigência da Ata de Registro de Preços.

5.3.1.3.2. *A formalização das contratações decorrentes da Ata observará a disponibilidade orçamentária e os procedimentos administrativos aplicáveis à realização da despesa, não constituindo o registro dos quantitativos e valores na Ata garantia de execução integral da despesa.*

5.3.1.3.3. As solicitações serão centralizadas na Secretaria Municipal de Administração e Modernização, responsável pela gestão administrativa da contratação e pela consolidação das demandas das demais Secretarias e unidades administrativas.



5.3.1.4. As demandas serão formalizadas mediante emissão da Nota de Autorização de Despesa - NAD, ou outro instrumento administrativo aplicável, observadas as autorizações e os procedimentos internos da Administração.

5.3.1.5. A NAD será encaminhada formalmente à CONTRATADA pelos meios oficiais definidos pela Administração, constituindo o marco para o início do atendimento da demanda, observado o prazo máximo de **48 (quarenta e oito) horas** corridas estabelecido neste Termo de Referência.

5.3.2. Das contratações decorrentes da Ata

5.3.2.1. A contratação decorrente da Ata de Registro de Preços será formalizada mediante o instrumento jurídico cabível, conforme a natureza, o valor e as características da demanda, observadas as disposições da Lei nº 14.133/2021, da regulamentação aplicável e das condições estabelecidas no Edital e na Ata.

5.3.2.2. A vigência do instrumento decorrente da Ata será definida de acordo com a natureza do serviço, a necessidade da Administração, as características da demanda e o regime jurídico aplicável, não se confundindo com o prazo de vigência da Ata de Registro de Preços.

5.3.2.3. Quando cabível, os contratos decorrentes poderão possuir prazo de execução superior ao período de vigência da Ata, observadas as condições e os limites estabelecidos na legislação aplicável e no respectivo instrumento contratual.

5.3.2.4. A formalização de contratação decorrente da Ata não ocorrerá automaticamente pelo simples encerramento da vigência da Ata, dependendo de decisão e formalização administrativa próprias, observada a necessidade da Administração e os requisitos legais aplicáveis.

5.3.2.5. Eventual prorrogação dos contratos decorrentes dependerá do atendimento aos requisitos legais e das condições estabelecidas no respectivo instrumento contratual, quando admitida pela legislação.

5.3.2.5.1. Em caso de prorrogação da Ata de Registro de Preços, poderá ser renovado o quantitativo originalmente registrado, conforme Consulta/Processo n.º 196.139-0/2025, TCE/MT, Relator Conselheiro Guilherme Antônio Malouf, desde que:

- a) seja comprovado o preço vantajoso;
- b) a prorrogação da Ata de Registro de Preços ocorra dentro do prazo de vigência;
- c) a renovação não ultrapasse os quantitativos originais dos bens e serviços;
- d) haja prévia consulta e aceitação do fornecedor.

5.3.2.5.2. Parágrafo único: Se houver, o contrato decorrente da ata de registro de preços terá sua vigência estabelecida em conformidade com as disposições nela



contidas. Com efeito, a duração da ata das aquisições/contratações ora pleiteadas será de um (1) ano, podendo ser prorrogado conforme a lei. Ainda, a contratação em questão será enquadrada com base no art. 105 da Lei 14.133/2021, por se tratar de aquisição de serviços de fornecimento contínuo.

Art. 105. A duração dos contratos regidos por esta Lei será a prevista em edital, e deverão ser observadas, no momento da contratação e a cada exercício financeiro, a disponibilidade de créditos orçamentários, bem como a previsão no plano plurianual, quando ultrapassar 1 (um) exercício financeiro.

5.3.2.5.3. A duração da contratação ora pleiteada será de 1 (um) ano, a contar da data de assinatura do contrato, podendo ser prorrogado conforme a lei, até prazo não superior a 10 anos.

5.3.2.5.4. Ainda, a contratação em questão será enquadrada com base nos termos dos artigos 105 a 107 da Lei 14.133/2021, por se tratar de contratação de serviços de fornecimento continuado, podendo, nos termos do mesmo artigo, ser prorrogada, por interesse das partes, mediante atesto da autoridade competente que ratifique que as condições e os preços praticados permanecem vantajosos para a Administração, permitida a negociação com o contratado ou a extinção contratual sem ônus para qualquer das partes.

5.3.2.5.5. Em caso de continuidade da contratação, a Administração deverá atestar, no início de cada exercício, a existência de créditos orçamentários vinculados à contratação e a vantagem em sua manutenção.

5.3.2.5.6. Os serviços fornecidos de forma contínua são aqueles que, caso tenham seu fornecimento interrompido, haverá comprometimento das atividades da Administração. Sendo assim, tem-se a necessidade de a contratação se estender por mais de um exercício financeiro e continuamente. O contrato terá vigência de 1 (um) ano, a contar da data de sua assinatura, podendo ser prorrogado, nos termos do Art. 105 a 107 da Lei nº 14.133/2021.

5.3.2.6. Considerando a natureza continuada dos serviços de segurança da informação e sua relevância para a manutenção da infraestrutura tecnológica municipal, os instrumentos contratuais decorrentes da Ata poderão contemplar prazo compatível com a continuidade da prestação, observados os requisitos, limites e condições estabelecidos na legislação aplicável.

5.3.3. Da manutenção dos preços e atualização



5.3.3.1. Durante a vigência da contratação, serão observadas as hipóteses legais de reajuste, repactuação, revisão ou outro mecanismo de atualização dos valores, quando cabíveis, conforme a natureza do objeto e as condições estabelecidas no instrumento convocatório e no respectivo instrumento contratual.

5.4. Cota Exclusiva / Parcelamento para Microempresas e Empresas de Pequeno

Porte: A contratação será realizada em lote único, não sendo adotado parcelamento do objeto nem reserva de cotas para microempresas e empresas de pequeno porte.

Embora a Lei Complementar nº 123/2006 estabeleça tratamento favorecido às microempresas e empresas de pequeno porte, o parcelamento do presente objeto mostra-se tecnicamente inviável, considerando que a solução pretendida possui natureza integrada e elevada interdependência entre seus componentes.

Art. 47. Nas contratações públicas da administração direta e indireta, autárquica e fundacional, federal, estadual e municipal, deverá ser concedido tratamento diferenciado e simplificado para as microempresas e empresas de pequeno porte objetivando a promoção do desenvolvimento econômico e social no âmbito municipal e regional, a ampliação da eficiência das políticas públicas e o incentivo à inovação tecnológica.

Art. 48. Para o cumprimento do disposto no art. 47 desta Lei Complementar, a administração pública:

I - deverá realizar processo licitatório destinado exclusivamente à participação de microempresas e empresas de pequeno porte nos itens de contratação cujo valor seja de até R\$ 80.000,00 (oitenta mil reais).

III - deverá estabelecer, em certames para aquisição de bens de natureza divisível, cota de até 25% (vinte e cinco por cento) do objeto para a contratação de microempresas e empresas de pequeno porte.

A segregação dos itens entre diferentes fornecedores poderia comprometer a compatibilidade tecnológica da solução, dificultar a gestão contratual, aumentar a complexidade da fiscalização, fragmentar as responsabilidades quanto ao suporte técnico, manutenção e resolução de incidentes, além de elevar os riscos operacionais relacionados à segurança da informação.

Dessa forma, a contratação em lote único revela-se a alternativa mais eficiente para assegurar a plena integração entre os equipamentos, licenças, softwares e serviços especializados, garantindo maior padronização tecnológica, eficiência operacional e responsabilidade única pela execução contratual.

5.5. Contratação Anterior para o Objeto da Demanda

() Não houve contratação anterior.

(x) Houve contratação anterior.



O Município possui contratação anterior, em 2021, relacionada ao objeto da presente demanda, a qual atendeu às necessidades institucionais durante sua vigência.

Entretanto, considerando o encerramento da Ata de Registro de Preços do Pregão Eletrônico 70/2021 com objeto de Contratação de empresa especializada para fornecimento de Serviços de Solução Integrada de SD-WAN Segura e EDR (provimento de serviços de segurança, administração dos serviços providos, gestão de vulnerabilidades da rede Municipal em resposta a incidentes de segurança com transferência de conhecimento), para atender as demandas das Secretarias Municipais da Prefeitura Municipal Sinop/MT, por um período de 12 meses e a inexistência de condições para sua continuidade, torna-se necessária a realização de novo procedimento licitatório, assegurando a continuidade dos serviços essenciais de segurança da informação.

A nova contratação contempla aperfeiçoamentos decorrentes da experiência obtida na execução anterior, especialmente quanto à previsão de mecanismos de atualização dos valores contratuais, observadas as disposições legais aplicáveis aos contratos administrativos de natureza continuada.

Registra-se, ainda, que a presente contratação encontra-se prevista no Plano de Contratações Anual do Município e decorre de demanda formalizada pela Secretaria Municipal de Administração e Modernização, responsável pela gestão centralizada da infraestrutura tecnológica municipal.

5.6. Legislação Específica sobre o Objeto da Contratação:

() Não

(x) Sim

A legislação abaixo não constitui, por si só, exigência de apresentação documental para fins de habilitação, salvo quando determinada exigência decorrer expressamente de lei. Sua indicação tem por finalidade estabelecer o conjunto normativo que deverá ser observado na elaboração da solução, na execução dos serviços e na fiscalização contratual.

A contratação observará a legislação aplicável às contratações públicas e às soluções de tecnologia da informação, bem como as normas relacionadas à segurança da informação, proteção de dados pessoais e governança em tecnologia da informação, destacando-se a **Lei nº 14.133/2021**, a **Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD)**, a **Lei nº 12.965/2014 (Marco Civil da Internet)**, além das demais normas, regulamentos, diretrizes e atos administrativos

Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



aplicáveis à Administração Pública e às contratações de Tecnologia da Informação e Comunicação (TIC).

Também deverão ser observadas as normas técnicas, regulamentares e orientações emitidas pelos órgãos competentes, sempre que pertinentes ao objeto da contratação, especialmente aquelas relacionadas à segurança cibernética, proteção da infraestrutura tecnológica e boas práticas de governança em tecnologia da informação.

A presente contratação deverá observar, durante o planejamento, fornecimento, implantação, configuração, operação, manutenção, suporte técnico e demais atividades relacionadas à execução do objeto, a legislação, regulamentação e normas técnicas aplicáveis à segurança da informação, à segurança cibernética, à proteção de dados pessoais, à utilização de redes e sistemas informatizados e à governança de Tecnologia da Informação e Comunicação.

A indicação dos instrumentos normativos realizada no Estudo Técnico Preliminar (ETP) e neste Termo de Referência (TR) tem por finalidade estabelecer os parâmetros legais e técnicos que deverão nortear a execução da solução contratada, servindo de fundamento para a elaboração das especificações técnicas, obrigações da contratada, critérios de aceitação, fiscalização e demais condições que serão detalhadas neste documento (Termo de Referência) e no instrumento contratual.

A observância da legislação e das normas relacionadas ao objeto constitui obrigação de execução contratual, não implicando, por si só, a exigência de apresentação de documentos, certificados ou declarações específicas como condição de habilitação, ressalvadas aquelas exigências que decorram expressamente de disposição legal ou que sejam devidamente justificadas como indispensáveis à comprovação de requisito de habilitação previsto na legislação de licitações.

Para fins de planejamento da contratação, deverão ser consideradas, especialmente, as seguintes referências normativas:

A) Lei Federal nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente quanto às medidas técnicas e administrativas destinadas à proteção dos dados pessoais e à prevenção de acessos não autorizados e demais situações de tratamento inadequado ou ilícito;

Lei Federal nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD): aplicável ao tratamento de dados pessoais realizado no âmbito da solução, devendo a execução contratual observar medidas técnicas e administrativas aptas a proteger os dados contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer



outra forma de tratamento inadequado ou ilícito, especialmente considerando que a solução poderá realizar coleta, processamento, armazenamento, monitoramento e análise de informações relacionadas à infraestrutura tecnológica municipal.

B) Lei Federal nº 12.965/2014 - Marco Civil da Internet, quando aplicável às atividades relacionadas à utilização de redes, acesso à internet, registros e tratamento de informações abrangidos pela execução dos serviços;

Lei Federal nº 12.965/2014 - Marco Civil da Internet: aplicável às atividades relacionadas à utilização de redes, acesso à internet, registros e tratamento de informações decorrentes da utilização dos recursos tecnológicos abrangidos pela contratação, observadas as disposições pertinentes ao objeto e à natureza dos serviços efetivamente executados.

C) Decreto Municipal nº 092/2023, que regulamenta a aplicação da LGPD no âmbito do Poder Executivo Municipal de Sinop-MT, quando as atividades da CONTRATADA envolverem tratamento de dados pessoais ou acesso a informações abrangidas pela regulamentação;

Decreto Municipal nº 092/2023: regulamenta a aplicação da Lei Geral de Proteção de Dados Pessoais no âmbito do Poder Executivo Municipal de Sinop-MT, devendo suas disposições ser observadas pela contratada sempre que suas atividades envolverem tratamento de dados pessoais ou acesso a informações abrangidas pela regulamentação municipal.

D) Decreto Federal nº 11.856/2023, referente à Política Nacional de Cibersegurança - PNCiber, como referência para diretrizes e práticas relacionadas à segurança cibernética, prevenção, detecção, resposta e mitigação de riscos e incidentes cibernéticos, observada sua aplicabilidade ao Município;

Decreto Federal nº 11.856/2023 - Política Nacional de Cibersegurança (PNCiber): considerado como referência para as diretrizes e práticas relacionadas à segurança cibernética, prevenção, detecção, resposta e mitigação de riscos decorrentes de incidentes cibernéticos, observada a sua aplicabilidade ao contexto da Administração Pública Municipal.

E) Lei Federal nº 14.133/2021, especialmente quanto às regras aplicáveis à contratação, execução, fiscalização, responsabilidades da CONTRATADA, recebimento do objeto e aplicação das medidas administrativas cabíveis;

Lei Federal nº 14.133/2021: aplicável ao processo de contratação e à execução do contrato administrativo, especialmente quanto ao planejamento, definição dos requisitos da contratação, fiscalização, responsabilidades da contratada, recebimento do objeto e aplicação das medidas administrativas cabíveis em caso de descumprimento contratual.



F) Decreto Municipal nº 359/2023 e suas alterações, no que couber aos procedimentos de contratação e à gestão e execução contratual no âmbito do Poder Executivo Municipal de Sinop-MT;

Decreto Municipal nº 359/2023 e suas alterações: aplicável ao procedimento de contratação e à gestão dos contratos administrativos no âmbito do Poder Executivo Municipal de Sinop-MT, devendo ser observado em conjunto com a Lei Federal nº 14.133/2021.

G) Normas técnicas e boas práticas reconhecidas de segurança da informação, especialmente aquelas relacionadas à gestão da segurança da informação, controles de segurança, proteção de dados, gestão de vulnerabilidades, gerenciamento de incidentes, registros de eventos e continuidade dos serviços, incluindo, quando aplicáveis, as normas da família ISO/IEC 27000 e demais padrões técnicos reconhecidos; e

Normas técnicas e boas práticas reconhecidas de segurança da informação: deverão ser consideradas na execução da solução, quando pertinentes ao objeto, especialmente as normas e referências técnicas relacionadas à gestão da segurança da informação, controles de segurança, proteção de dados, gestão de vulnerabilidades, gerenciamento de incidentes, registros de eventos e continuidade dos serviços, incluindo, conforme aplicabilidade, as normas da família ISO/IEC 27000 e demais padrões técnicos reconhecidos.

H) demais normas, regulamentos, atos e orientações oficiais dos órgãos competentes que sejam aplicáveis às atividades efetivamente desempenhadas pela CONTRATADA.

Normas, regulamentos e orientações dos órgãos competentes: deverão ser observados, durante a execução contratual, os atos normativos e orientações oficiais que sejam aplicáveis às atividades efetivamente desempenhadas pela contratada, inclusive aqueles relacionados à segurança cibernética, proteção de dados, registros de eventos, gestão de incidentes e preservação da segurança da infraestrutura tecnológica.

As referências acima deverão ser interpretadas de acordo com sua respectiva natureza jurídica e âmbito de aplicação, não sendo presumida a obrigatoriedade de normas destinadas especificamente a órgãos ou entidades da Administração Pública Federal quando não houver previsão de sua incidência sobre o Município de Sinop-MT. Quando utilizadas como referência técnica, deverão orientar a definição dos requisitos e das boas práticas aplicáveis à solução.



Dessa forma, a futura contratada deverá executar o objeto em conformidade com a legislação e os parâmetros técnicos aplicáveis, ficando sujeita à fiscalização da Administração e às medidas administrativas e contratuais cabíveis caso sejam identificadas desconformidades na execução dos serviços.

5.7. Necessidade de Consolidação para Toda a Estrutura:

(x) Contratação/Aquisição consolidada para toda a estrutura

() Contratação/Aquisição exclusiva da unidade administrativa demandante

A presente contratação caracteriza-se como aquisição consolidada para atendimento de toda a estrutura administrativa do Município de Sinop-MT, tendo em vista que a solução de segurança da informação será destinada à proteção da infraestrutura tecnológica corporativa utilizada pelas diversas Secretarias e unidades administrativas do Poder Executivo Municipal.

Embora a Secretaria Municipal de Administração e Modernização seja a unidade responsável pela centralização da demanda, pelo planejamento e pela gestão da contratação, a solução não se restringirá aos ativos ou às necessidades exclusivas dessa Secretaria. Sua finalidade é proporcionar proteção integrada à infraestrutura tecnológica corporativa que dá suporte às atividades desenvolvidas pelas diferentes unidades administrativas do Município.

A adoção da contratação de forma centralizada justifica-se pela própria natureza da solução, considerando que os componentes de segurança da informação, tais como firewall, gerenciamento, monitoramento, proteção de endpoints, análise de eventos e demais recursos previstos no objeto, deverão operar de forma integrada e sob uma arquitetura única de segurança.

A centralização da contratação proporciona maior padronização tecnológica, uniformidade das políticas de segurança, racionalização da gestão contratual, simplificação da fiscalização, otimização dos recursos públicos e centralização da responsabilidade técnica, além de reduzir os riscos decorrentes da adoção de soluções distintas ou desconectadas entre as unidades administrativas.

Dessa forma, a Secretaria Municipal de Administração e Modernização figura como unidade gestora e centralizadora da contratação, em razão da competência administrativa para coordenação e gestão da demanda, sem que isso caracterize aquisição exclusiva para essa unidade, uma vez que a solução será disponibilizada para atendimento da infraestrutura tecnológica corporativa e proteção dos ativos de tecnologia da informação utilizados pelas demais Secretarias e unidades integrantes da estrutura administrativa municipal.



Nº	ETAPAS ATENDIDAS
1	MUNICÍPIO DE SINOP-MT
2	SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO E MODERNIZAÇÃO - CENTRALIZAÇÃO DA DEMANDA, PLANEJAMENTO E GESTÃO DA CONTRATAÇÃO
3	CONTRATAÇÃO CONSOLIDADA: SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO

4	GABINETE DO CHEFE DO EXECUTIVO	FINANÇAS E ORÇAMENTO	OBRAS E SERVIÇOS URBANOS	SEGURANÇA E TRÂNSITO	MEIO AMBIENTE E DESENVOLVIMENTO SUSTENTÁVEL	EDUCAÇÃO	ASSISTÊNCIA SOCIAL	DESENVOLVIMENTO ECONÔMICO	SAÚDE	GOVERNO E PLANEJAMENTO ESTRATÉGICO	CULTURA, ESPORTE E TURISMO	PLANEJAMENTO URBANO E HABITAÇÃO	PROCURADORIA GERAL DO MUNICÍPIO
---	-----------------------------------	----------------------	--------------------------	----------------------	---	----------	--------------------	---------------------------	-------	---------------------------------------	----------------------------	------------------------------------	------------------------------------





- IMAGEM ILUSTRATIVA DISPONÍVEL NO ESTUDO TÉCNICO PRELIMINAR - ETP. LOCALIZADA NO TÓPICO 4.7. “NECESSIDADE DE CONSOLIDAÇÃO PARA TODA A ESTRUTURA”, PÁGINA 34 (TRINTA E QUATRO) DO DOCUMENTO EM PDF/DIGITAL.

5.8. Viabilidade da Adoção da Modalidade na Forma Eletrônica

(x) Sim

() Não

Justificativa: Considerando a natureza comum do objeto, a ampla oferta de fornecedores especializados no mercado e a necessidade de ampliar a competitividade, a transparência, economicidade e a eficiência da contratação, conclui-se pela plena viabilidade da realização do procedimento licitatório na forma eletrônica.

A utilização da modalidade eletrônica possibilita maior participação de licitantes, amplia a competitividade do certame e contribui para a obtenção da proposta mais vantajosa para a Administração Pública, observados os princípios previstos na Lei nº 14.133/2021.

5.9. EVENTUAL NECESSIDADE DE APRESENTAÇÃO DE AMOSTRA, PROTÓTIPO, CATÁLOGO, FOLDERS E ETC: (Não se aplica). Não se aplica a apresentação de amostra ou protótipo como condição prévia à participação no certame, considerando a natureza do objeto, composto por serviços especializados de segurança da informação, com disponibilização de equipamentos, licenças, softwares e demais recursos tecnológicos.

A comprovação do atendimento aos requisitos técnicos da solução poderá ocorrer por meio da documentação técnica pertinente, catálogos, fichas técnicas, declarações do fabricante, demonstrações, esclarecimentos e, quando necessário, testes técnicos, conforme previsto no Termo de Referência e solicitado pela Administração.

5.10. EVENTUAL NECESSIDADE DE VISITA TÉCNICA:

5.10.1. Não será exigida visita técnica prévia como condição de participação, habilitação ou apresentação de proposta no certame.

5.10.2. Durante a execução contratual, contudo, será obrigatória a realização de no mínimo 01 (uma) visita técnica presencial mensal, conforme condições estabelecidas neste Termo de Referência, destinada ao acompanhamento da solução, verificação das condições de funcionamento, esclarecimento de dúvidas, identificação de
Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



necessidades de ajustes e orientações técnicas relacionadas à execução dos serviços.

5.10.3. A Administração poderá solicitar visitas presenciais adicionais sempre que for identificada necessidade relacionada à execução, funcionamento, manutenção, suporte ou acompanhamento da solução.

5.10.4. Os custos decorrentes das visitas técnicas, inclusive deslocamento, transporte, alimentação, hospedagem e demais despesas necessárias, deverão estar incluídos nos preços ofertados pela CONTRATADA, não sendo admitida cobrança adicional à Administração.

5.11. EVENTUAL NECESSIDADE DE REGISTRO E LICENÇAS QUANDO OBRIGATÓRIO POR LEI:

5.11.1. A CONTRATADA deverá providenciar e manter, durante todo o período de execução dos serviços, os registros, licenças, autorizações e demais documentos eventualmente exigidos por lei ou por órgão competente, quando aplicáveis às atividades, equipamentos, softwares ou serviços integrantes da solução.

5.11.2. Os registros, licenças e autorizações exigíveis em razão da execução do objeto não serão considerados, por si só, documentos de habilitação, devendo ser apresentados pela CONTRATADA quando necessários ao início ou à continuidade da execução dos serviços, ressalvadas as hipóteses em que a legislação específica determine expressamente sua apresentação como condição de habilitação ou contratação.

5.11.3. Caberá exclusivamente à CONTRATADA manter válidos, durante toda a execução contratual, os registros, licenças e autorizações de sua responsabilidade, não sendo admitida a execução de atividades que dependam de autorização legal sem a respectiva regularidade.

5.11.4. A eventual necessidade de registro, licença ou autorização não transfere à Administração a responsabilidade por obrigações que, por sua natureza legal ou regulamentar, sejam de responsabilidade da CONTRATADA.

5.11.5. Da Matriz de Criticidade e Níveis de Serviço (SLA) por Objeto

5.11.5.1. Em razão da natureza integrada da solução de segurança da informação, a definição dos Níveis de Serviço (SLA), dos tempos de resposta inicial e dos prazos para solução de contorno observará a criticidade e a relevância de cada solução no ambiente tecnológico municipal, considerando o impacto de eventual indisponibilidade na continuidade dos serviços públicos, conforme os seguintes parâmetros:



I. Atendimento Inicial de Demandas / Emissão de NAD: A disponibilização física/lógica de novos itens solicitados via Nota de Autorização de Despesa (NAD) observará o prazo regular de até **48 (quarenta e oito) horas corridas** (todos os dias, das 00h00min às 24h00min), ressalvada a etapa de implantação inicial da solução, que observará o prazo de **30 (trinta) dias corridos**.

II. Suporte Técnico 24x7 para Soluções Perimetrais e Infraestrutura Crítica (Itens 1 a 6 - NGFW, WAF, EDR, Base de Logs e Gerenciador Centralizado):

A) Criticidade Emergencial (Paralisação total do perímetro ou indisponibilidade de serviços essenciais): Tempo de resposta inicial de até 15 (quinze) minutos; atualização de status a cada 3 (três) horas; e provimento de solução de contorno em até 4 (quatro) horas.

B) Criticidade Alta (Degradação relevante de performance ou perda parcial de redundância/funcionalidade): Tempo de resposta inicial de até 15 (quinze) minutos; atualização de status de até 2 (duas) vezes ao dia; e provimento de solução de contorno em até 24 (vinte e quatro) horas.

III. Suporte Técnico para Soluções Acessórias e Complementares (Itens 7, 8, 9, 10 e 11 - Access Points, Captive Portal, Conscientização/Phishing, Mapeamento de Vulnerabilidades e USTs):

As solicitações de suporte e atendimento observarão a criticidade moderada de cada ferramenta, aplicando-se os prazos regulares de atendimento em expediente comercial (ou conforme especificado no tópico individual de cada item), salvo quando a indisponibilidade afetar diretamente a infraestrutura crítica descrita no inciso II.

5.11.5.2. A diferenciação dos prazos de atendimento entre os componentes da contratação fundamenta-se na diversidade técnica do objeto e no impacto operacional de cada solução sobre a continuidade dos serviços públicos prestados pelo Município.

5.12. ATESTADO DE CAPACIDADE TÉCNICA, NOS TERMOS DO REGULAMENTO PRÓPRIO INSTITUÍDO PELO MUNICÍPIO:

5.12.1. Para fins de comprovação da qualificação técnico-operacional, a licitante deverá apresentar **atestado(s)** ou certidão(ões) de capacidade técnica, emitido(s) por pessoa jurídica de direito público ou privado, que comprove(m) a execução anterior de serviços compatíveis em características, natureza e complexidade com as parcelas de maior relevância técnica e/ou valor significativo do objeto, nos termos do art. 67 da Lei nº 14.133/2021 - Lei de Licitações e Contratos Administrativos.



Art. 67. A documentação relativa à qualificação técnico-profissional e técnico-operacional será restrita a:

I - apresentação de profissional, devidamente registrado no conselho profissional competente, quando for o caso, detentor de atestado de responsabilidade técnica por execução de obra ou serviço de características semelhantes, para fins de contratação;

II - certidões ou atestados, regularmente emitidos pelo conselho profissional competente, quando for o caso, que demonstrem capacidade operacional na execução de serviços similares de complexidade tecnológica e operacional equivalente ou superior, bem como documentos comprobatórios emitidos na forma do § 3º do art. 88 desta Lei;

III - indicação do pessoal técnico, das instalações e do aparelhamento adequados e disponíveis para a realização do objeto da licitação, bem como da qualificação de cada membro da equipe técnica que se responsabilizará pelos trabalhos;

IV - prova do atendimento de requisitos previstos em lei especial, quando for o caso;

V - registro ou inscrição na entidade profissional competente, quando for o caso;

VI - declaração de que o licitante tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação.

§ 1º A exigência de atestados será restrita às parcelas de maior relevância ou valor significativo do objeto da licitação, assim consideradas as que tenham valor individual igual ou superior a 4% (quatro por cento) do valor total estimado da contratação.

Na descrição deverá conter informações que permitam o entendimento dos trabalhos realizados, bem como aferir a semelhança ou afinidade com o serviço/objeto licitado, devendo o(s) atestado(s) conter:

- a) CNPJ da licitante e endereço atualizado da empresa;
- b) Relatório do objeto fornecido e/ou serviços realizados;
- c) Nome completo, telefone e assinatura do responsável pela sua emissão.
- d) Em se tratando de atestado fornecido por pessoa jurídica de direito privado, a assinatura do responsável deverá ser feita com reconhecimento de firma.
- e) *Comprovação de experiência anterior na execução de serviços compatíveis em características e complexidade com as parcelas de maior relevância técnica ou valor significativo da presente contratação, conforme os **requisitos e critérios estabelecidos neste Termo de Referência, especialmente aqueles detalhados na planilha constante do item 5.12.27.;***

5.12.2. Para fins deste Termo de Referência, serão consideradas parcelas de maior relevância técnica e/ou valor significativo, em razão de sua importância para a arquitetura de segurança da informação, complexidade operacional e/ou representatividade econômica, os serviços relacionados aos seguintes componentes:

**Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br**



a) Item 1 - NGFW/SD-WAN: execução de serviços especializados de segurança da informação envolvendo solução de NGFW/Firewall ou tecnologia equivalente, compreendendo atividades de implantação, configuração, gerenciamento, operação, monitoramento, suporte ou manutenção;

b) Item 2 - NGFW/SD-WAN: execução de serviços especializados de segurança da informação envolvendo solução de NGFW/Firewall, SD-WAN ou tecnologia equivalente, compreendendo atividades de implantação, configuração, gerenciamento, operação, monitoramento, suporte ou manutenção;

c) Item 3 - Base de dados analíticos e logs: execução de serviços relacionados ao gerenciamento, armazenamento, monitoramento, análise ou tratamento de logs e eventos de segurança da informação, mediante solução própria ou equivalente;

d) Item 4 - Gerenciamento de NGFW: execução de serviços relacionados ao gerenciamento centralizado de soluções de segurança de rede, incluindo administração, configuração, monitoramento ou atividades equivalentes;

e) Item 5 - EDR: execução de serviços especializados relacionados à proteção, monitoramento ou gerenciamento de endpoints por meio de soluções de segurança da informação compatíveis com a natureza do serviço contratado;

f) Item 6 - WAF: execução de serviços relacionados à proteção de aplicações ou ambientes web por meio de WAF ou tecnologia equivalente;

g) Item 9 - Conscientização em segurança da informação: execução de serviços relacionados à conscientização, capacitação, campanhas de segurança da informação, simulações de phishing ou atividades tecnicamente equivalentes.

5.12.3. A licitante poderá comprovar sua capacidade técnico-operacional mediante um ou mais atestados, sendo admitida a apresentação de documentos que demonstrem, individualmente ou em conjunto, experiência compatível com as parcelas relevantes do objeto.

5.12.4. Não será exigida a comprovação de experiência anterior na execução de todos os 11 (onze) itens que compõem a contratação, nem a comprovação de identidade entre os serviços anteriormente executados e a solução pretendida pela Administração, considerando a natureza integrada do objeto e a possibilidade de utilização de tecnologias, fabricantes, marcas, modelos ou plataformas distintas.

5.12.5. Para os serviços que possuam quantitativo definido no presente Termo de Referência, a análise da compatibilidade poderá considerar a dimensão da experiência anteriormente comprovada, observando-se os quantitativos efetivamente necessários à execução do objeto.



5.12.6. A Administração não exigirá que os atestados apresentem os mesmos valores financeiros, marcas, fabricantes, modelos, equipamentos, licenças ou plataformas previstos neste Termo de Referência, desde que seja possível verificar a **compatibilidade** da experiência comprovada com a natureza, as **características**, a **complexidade** e a **dimensão** dos serviços objeto da contratação.

5.12.7. Para fins de análise dos atestados, serão considerados compatíveis os serviços que demonstrem experiência efetiva da licitante na execução de atividades de segurança da informação de natureza semelhante às parcelas relevantes do objeto, independentemente da nomenclatura comercial utilizada para a solução anteriormente contratada.

5.12.8. A mera comprovação de fornecimento ou comercialização de equipamentos, licenças ou softwares, desacompanhada de **elementos que demonstrem a efetiva execução de serviços compatíveis com as atividades** objeto desta contratação, não será considerada, isoladamente, suficiente para comprovar a capacidade técnico-operacional exigida neste item.

5.12.9. Os atestados deverão conter informações suficientes para permitir a identificação do contratante, da contratada, do objeto executado, do período de execução e das características dos serviços realizados, podendo a Administração solicitar esclarecimentos ou documentação complementar quando necessária à verificação da autenticidade e da compatibilidade da experiência apresentada, observados os limites da legislação aplicável.

5.12.10. No caso de atestado que contenha diversos serviços, a Administração poderá considerar apenas as parcelas efetivamente executadas e compatíveis com o objeto desta contratação.

5.12.11. A análise da qualificação técnico-operacional deverá observar a compatibilidade entre a experiência comprovada e as características efetivamente exigidas na presente contratação, vedada a imposição de requisitos que resultem em exigência de experiência superior, desnecessária ou desproporcional à dimensão e à complexidade do objeto.

5.12.12. A comprovação de capacidade técnica prevista neste item tem por finalidade assegurar que a futura contratada possua experiência operacional suficiente para executar os serviços especializados de segurança da informação de forma adequada, integrada e contínua, sem restringir a participação de empresas que possuam experiência em soluções tecnicamente equivalentes às referências utilizadas pela Administração.



5.12.13. Considerando o valor total estimado da contratação, de **R\$ 3.168.167,64 (três milhões cento e sessenta e oito mil cento e sessenta e sete reais e sessenta e quatro centavos)**, a Administração analisou individualmente os itens que compõem a solução, considerando, além do aspecto econômico, a relevância técnica, a complexidade, a criticidade e a necessidade de experiência compatível com a execução dos serviços.

5.12.14. Para fins de aplicação do §1º do art. 67 da Lei nº 14.133/2021, considera-se como referência para identificação das parcelas de maior relevância ou valor significativo o percentual mínimo de 4% do valor total estimado da contratação, correspondente a **R\$ 126.726,71 (cento e vinte e seis mil setecentos e vinte e seis reais e setenta e um centavos)**.

5.12.15. A análise das parcelas relevantes resultou na seguinte classificação:

ITEM	SOLUÇÃO	VALOR ESTIMADO ANUAL	EXIGÊNCIA DE ATESTADO
1	NGFW/SD-WAN em cluster de alta disponibilidade - appliance Tipo 1	R\$ 434.124,00	SIM
2	NGFW/SD-WAN - appliance Tipo 2	R\$ 207.245,40	SIM
3	Base de dados analíticos e logs - appliance	R\$ 242.747,76	SIM
4	Gerenciamento de NGFW - appliance	R\$ 221.531,04	SIM
5	Endpoint corporativo - EDR	R\$ 874.440,00	SIM
6	WAF - appliance	R\$ 328.857,00	SIM
7	Access Point corporativo	R\$ 118.126,20	NÃO
8	Captive Portal	R\$ 65.493,36	NÃO
9	Plataforma de conscientização e campanhas de phishing	R\$ 390.197,88	SIM
10	Mapeamento de vulnerabilidades	R\$ 9.774,00	NÃO
11	Unidade de Serviço Técnico - UST	R\$ 275.631,00	NÃO

5.12.16. A exigência de atestado será concentrada nas parcelas que apresentam maior relevância econômica e/ou técnica para a execução da solução, especialmente aquelas relacionadas à proteção perimetral, gerenciamento e análise da infraestrutura de segurança, proteção de endpoints, proteção de aplicações e conscientização em segurança da informação.

5.12.17. Para o **Item 1 - NGFW/Firewall**, não será exigida comprovação de quantitativo correspondente a 02 (dois) appliances, nem experiência anterior em arquitetura de cluster ou alta disponibilidade, sendo suficiente a demonstração de experiência anterior na prestação de serviços de NGFW/Firewall compatíveis com a natureza e a complexidade da solução pretendida.



5.12.18. Para o Item 2 - NGFW/SD-WAN, será considerada suficiente a demonstração de experiência anterior na prestação de serviços de NGFW/Firewall e/ou SD-WAN, ou solução tecnicamente equivalente, não sendo exigida comprovação de experiência anterior com quantidade, arquitetura, fabricante, marca ou modelo idênticos aos previstos na contratação.

5.12.18.1. Considerando que o Item 2 corresponde à prestação continuada de serviços pelo período de 12 (doze) meses, com quantitativo total de 180 (cento e oitenta) unidade-mês, será exigida, para fins de comprovação da capacidade técnico-operacional, experiência anterior compatível com a natureza, as características e a complexidade do serviço, observando-se o quantitativo mínimo de 90 (noventa) unidade-mês, correspondente a 50% (cinquenta por cento) do quantitativo previsto para a contratação, nos termos do § 2º do art. 67 da Lei nº 14.133/2021.

5.12.18.2. Para fins de aferição do período mínimo de experiência, os 90 (noventa) unidade-mês correspondem a 6 (seis) meses de execução de serviço, considerando o dimensionamento de até 15 (quinze) pontos pelo período de 12 (doze) meses, não sendo exigida, para fins de habilitação, a reprodução integral da quantidade física de pontos, equipamentos ou demais componentes da solução prevista nesta contratação.

5.12.19. Para os Itens 3 e 4 - Logs e Gerenciamento

5.12.19.1. Para o Item 3 - Solução de coleta, armazenamento, gerenciamento e análise de logs e eventos, será considerada suficiente a demonstração de experiência anterior na prestação de serviços de coleta, armazenamento, gerenciamento, correlação ou análise de logs e eventos de segurança da informação, ou solução tecnicamente equivalente, não sendo exigida comprovação de experiência anterior com fabricante, marca, modelo, plataforma, arquitetura ou tecnologia idênticos aos previstos na contratação.

5.12.19.2. Considerando que o Item 3 corresponde à prestação continuada de serviços pelo período de 12 (doze) meses, será exigida, para fins de comprovação da capacidade técnico-operacional, experiência anterior compatível com a natureza, as características e a complexidade do serviço, em quantitativo mínimo de 6 (seis) unidade-mês, correspondente a 50% (cinquenta por cento) do quantitativo previsto, nos termos do §2º do art. 67 da Lei nº 14.133/2021.

5.12.19.3. Para fins de aferição do período mínimo de experiência, nos termos do §5º do art. 67 da Lei nº 14.133/2021, será exigida comprovação de execução de serviços similares por período mínimo de 6 (seis) meses, sucessivos ou não, não sendo necessária a reprodução integral do quantitativo, da infraestrutura física, do volume de

**Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br**



armazenamento, da quantidade de eventos ou da composição tecnológica previstos na presente contratação.

5.12.19.4. Para o **Item 4** - Gerenciamento da solução NGFW, será considerada suficiente a demonstração de experiência anterior na prestação de serviços de gerenciamento, administração, monitoramento, configuração ou operação de soluções NGFW/Firewall, ou solução tecnicamente equivalente, não sendo exigida comprovação de experiência anterior com fabricante, marca, modelo, plataforma, arquitetura ou tecnologia idênticos aos previstos na contratação.

5.12.19.5. Considerando que o Item 4 corresponde à prestação continuada de serviços pelo período de 12 (doze) meses, será exigida, para fins de comprovação da capacidade técnico-operacional, experiência anterior compatível com a natureza, as características e a complexidade do serviço, em quantitativo mínimo de seis (seis) unidade-mês, correspondente a 50% (cinquenta por cento) do quantitativo previsto, nos termos do §2º do art. 67 da Lei nº 14.133/2021.

5.12.19.6. Para fins de aferição do período mínimo de experiência, nos termos do §5º do art. 67 da Lei nº 14.133/2021, será exigida comprovação de execução de serviços similares por período mínimo de 6 (seis) meses, sucessivos ou não, não sendo necessária a reprodução integral da quantidade de equipamentos, da arquitetura, da infraestrutura ou da composição tecnológica previstas na presente contratação.

5.12.20. Para o **Item 5** - Solução de proteção e detecção e resposta em endpoints (EDR), será considerada suficiente a demonstração de experiência anterior na prestação de serviços de proteção, monitoramento, detecção, gerenciamento ou resposta a incidentes em endpoints, mediante solução EDR, EPP/EDR ou solução tecnicamente equivalente, compatível com a natureza e a complexidade do serviço previsto na contratação.

5.12.20.1. A comprovação da experiência relativa ao Item 5 deverá demonstrar, de forma integral e individualizada, a execução anterior de serviços de proteção ou gerenciamento de endpoints, não sendo admitida a utilização de atestados que, isoladamente ou por mera soma de experiências distintas e não relacionadas, não demonstrem a execução efetiva do serviço de proteção ou gerenciamento de endpoints.

5.12.20.2. Considerando que o Item 5 corresponde à prestação continuada de serviços pelo período de 12 (doze) meses, será exigida, para fins de comprovação da capacidade técnico-operacional, experiência anterior compatível com a natureza, as características e a complexidade do serviço, em quantitativo mínimo de seis (seis)



unidade-mês, correspondente a 50% (cinquenta por cento) do quantitativo previsto, nos termos do §2º do art. 67 da Lei nº 14.133/2021.

5.12.20.3. Para fins de aferição do período mínimo de experiência, nos termos do §5º do art. 67 da Lei nº 14.133/2021, será exigida comprovação de execução de serviços similares por período mínimo de 6 (seis) meses, sucessivos ou não, não sendo exigida comprovação de experiência com quantidade específica de endpoints, fabricante, marca, modelo, plataforma ou solução tecnológica idêntica à prevista na contratação.

5.12.21. Para o **Item 6** - Solução de Web Application Firewall (WAF), será considerada suficiente a demonstração de experiência anterior na prestação de serviços de proteção, monitoramento, gerenciamento ou operação de soluções WAF, destinadas à proteção de aplicações, sistemas ou serviços web, ou solução tecnicamente equivalente, não sendo exigida comprovação de experiência anterior com fabricante, marca, modelo, plataforma, arquitetura ou tecnologia idênticos aos previstos na contratação.

5.12.21.1. Considerando que o Item 6 corresponde à prestação continuada de serviços pelo período de 12 (doze) meses, será exigida, para fins de comprovação da capacidade técnico-operacional, experiência anterior compatível com a natureza, as características e a complexidade do serviço, em quantitativo mínimo de 6 (seis) unidade-mês, correspondente a 50% (cinquenta por cento) do quantitativo previsto, nos termos do §2º do art. 67 da Lei nº 14.133/2021.

5.12.21.2. Para fins de aferição do período mínimo de experiência, nos termos do §5º do art. 67 da Lei nº 14.133/2021, será exigida comprovação de execução de serviços similares por período mínimo de 6 (seis) meses, sucessivos ou não, não sendo necessária a reprodução integral da quantidade de aplicações, sistemas, serviços web, equipamentos, infraestrutura ou composição tecnológica previstas na presente contratação.

5.12.22. Para o **Item 9** – Serviços de conscientização em segurança da informação e simulação de phishing, será considerada suficiente a demonstração de experiência anterior na prestação de serviços de conscientização e treinamento em segurança da informação, campanhas de sensibilização, simulações de phishing, engenharia social ou atividades correlatas, ou solução tecnicamente equivalente, não sendo exigida comprovação de experiência anterior com fabricante, marca, modelo, plataforma ou metodologia idênticos aos previstos na contratação.

5.12.22.1. Considerando que o Item 9 corresponde à prestação continuada de serviços pelo período de 12 (doze) meses, será exigida, para fins de comprovação da

Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



capacidade técnico-operacional, experiência anterior compatível com a natureza, as características e a complexidade do serviço, em quantitativo mínimo de 6 (seis) unidade-mês, correspondente a 50% (cinquenta por cento) do quantitativo previsto, nos termos do §2º do art. 67 da Lei nº 14.133/2021.

5.12.22.2. Para fins de aferição do período mínimo de experiência, nos termos do §5º do art. 67 da Lei nº 14.133/2021, será exigida comprovação de execução de serviços similares por período mínimo de 6 (seis) meses, sucessivos ou não, não sendo necessária a reprodução integral da quantidade de campanhas, simulações, usuários, participantes ou ciclos de conscientização previstos na presente contratação.

5.12.23. Forma de comprovação e critérios de aceitação

Para que o(s) atestado(s) seja(m) considerado(s) apto(s) à comprovação da capacidade técnico-operacional, deverá(ão) demonstrar, de forma clara, a execução anterior de serviços compatíveis com as parcelas exigidas, observados os seguintes critérios:

- a)** o atestado deverá ser emitido por pessoa jurídica de direito público ou privado, identificando a contratante, a contratada e o objeto executado;
- b)** deverá ser possível identificar, no atestado ou em documentação complementar admitida pela Administração, a natureza dos serviços efetivamente executados;
- c)** a experiência comprovada deverá ser compatível em características e complexidade com a parcela do objeto para a qual está sendo apresentada;
- d)** será admitida a apresentação de um ou mais atestados de capacidade técnica, inclusive decorrentes de contratos distintos, desde que, em conjunto ou individualmente, conforme o caso, demonstrem a experiência compatível com as parcelas exigidas para a execução do objeto, ressalvado o Item 5 - EDR, cuja comprovação deverá ser realizada por atestado(s) que demonstre(m), de forma integral, a execução anterior de serviços de proteção ou gerenciamento de endpoints, não sendo admitida a fragmentação da comprovação da experiência específica exigida para esse item
- e)** não será exigida identidade entre a solução anteriormente executada e a solução objeto desta contratação, sendo admitida experiência com soluções de fabricantes, marcas, modelos ou plataformas diferentes, desde que tecnicamente compatíveis com a parcela que se pretende comprovar;

f) não será exigida, para fins de habilitação, a comprovação de utilização das marcas ou modelos indicados como referência no Termo de Referência;

g) não será exigida comprovação de que a experiência anterior tenha sido executada exatamente nas mesmas condições de arquitetura, quantidade de equipamentos ou



composição tecnológica da presente contratação, desde que demonstrada experiência compatível com a parcela relevante;

h) a Administração poderá realizar diligências para esclarecer ou confirmar as informações constantes dos documentos apresentados, observados os limites estabelecidos pela legislação aplicável.

5.12.24. Dimensão mínima da experiência

5.12.24.1. A comprovação da capacidade técnico-operacional observará, para os itens 1, 2, 3, 4, 5, 6 e 9, os quantitativos mínimos e períodos mínimos de experiência estabelecidos neste Termo de Referência, correspondentes a 50% (cinquenta por cento) do quantitativo previsto para cada parcela e período mínimo de 6 (seis) meses de execução de serviços similares, conforme aplicável a cada item.

5.12.24.2. A exigência de quantitativo mínimo será aferida sobre a unidade de medida prevista para cada serviço, não sendo exigida a reprodução da quantidade física de equipamentos, pontos, endpoints, aplicações, usuários, campanhas, componentes ou demais elementos da solução contratada.

5.12.24.3. Para os itens 7, 8, 10 e 11, não será exigida comprovação específica de capacidade técnico-operacional, conforme os critérios de relevância e natureza dos respectivos serviços estabelecidos neste Termo de Referência.

5.12.25. Parcelas não sujeitas à exigência de atestado

Não será exigida comprovação específica de capacidade técnico-operacional para os **Itens 7, 8, 10 e 11**, considerando suas características, valores individualizados, natureza complementar ou eventual dos serviços e a ausência de necessidade de demonstração específica de experiência anterior como condição de habilitação.

A ausência de exigência de atestado específico para essas parcelas não afasta a obrigação da contratada de executar integralmente os respectivos serviços, observando todas as especificações, requisitos técnicos, níveis de serviço e demais condições estabelecidas no Termo de Referência.

5.12.25.1. Os Itens 7, 8 e 10, em razão de sua menor representatividade econômica no conjunto da contratação, não constituirão, isoladamente, parcela para a qual será exigida comprovação específica de capacidade técnico-operacional, sem prejuízo de poderem ser considerados na avaliação conjunta da experiência apresentada pela licitante.

5.12.25.2. O Item 11 - Unidade de Serviço Técnico (UST), por possuir natureza eventual e consumo condicionado à necessidade da Administração, não será utilizado, isoladamente, como fundamento para exigência de comprovação específica de

Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



quantitativo de horas, sem prejuízo da possibilidade de serem considerados, para fins de avaliação da capacidade técnica geral, serviços anteriormente executados que apresentem natureza compatível.

5.12.25.3. A exigência de comprovação de experiência para o Item 11 não implica a fixação de quantitativo mínimo de horas ou UST, uma vez que o §2º do art. 67 da Lei nº 14.133/2021 estabelece que a exigência de quantitativos mínimos constitui faculdade da Administração, limitada a até 50% da parcela considerada relevante ou de valor significativo. Considerando a natureza eventual do serviço, opta-se pela comprovação da experiência compatível, sem vinculação a quantitativo mínimo ou período específico de execução.

5.12.26. Ausência de vinculação a fabricante ou solução específica

Os atestados apresentados serão analisados quanto à experiência efetivamente demonstrada, e não pela identidade de fabricante, marca, modelo, plataforma ou tecnologia utilizada no contrato anterior.

Dessa forma, será considerada válida a experiência anterior com solução tecnicamente equivalente à parcela objeto da comprovação, desde que demonstre **capacidade compatível com as características e complexidade dos serviços** pretendidos pela Administração.

5.12.27. Quadro exemplificativo dos critérios de comprovação da capacidade técnica

Para fins de consolidação dos requisitos de capacidade técnico-operacional, os serviços considerados relevantes e os respectivos parâmetros de experiência são:

ITEM	SERVIÇO	EXPERIÊNCIA EXIGIDA	QUANTITATIVO MÍNIMO	PERÍODO MÍNIMO
1	NGFW/SD-WAN em cluster de alta disponibilidade – Tipo 1	NGFW/Firewall ou solução tecnicamente equivalente	6 unidade-mês	6 meses
2	NGFW/SD-WAN – Tipo 2	NGFW/Firewall e/ou SD-WAN ou solução tecnicamente equivalente	90 unidade-mês	6 meses
3	Coleta, armazenamento, gerenciamento e análise de logs/eventos	Serviços de gerenciamento, coleta, armazenamento, correlação ou análise de logs/eventos ou solução equivalente	6 unidade-mês	6 meses
4	Gerenciamento da solução NGFW	Serviços de gerenciamento, administração, monitoramento,	6 unidade-mês	6 meses



		configuração ou operação de NGFW/Firewall ou solução equivalente		
5	Proteção e detecção e resposta em endpoints – EDR	Serviços de proteção, monitoramento, detecção, gerenciamento ou resposta em endpoints, mediante EDR/EPP ou solução equivalente	6 unidade-mês	6 meses
6	Web Application Firewall – WAF	Serviços de proteção, monitoramento, gerenciamento ou operação de WAF ou solução equivalente	6 unidade-mês	6 meses
7	Access Point	Não será exigida comprovação específica	—	—
8	Captive Portal	Não será exigida comprovação específica	—	—
9	Conscientização em segurança da informação e simulação de phishing	Serviços de conscientização, treinamento, campanhas de sensibilização, simulações de phishing ou atividades correlatas	6 unidade-mês	6 meses
10	Mapeamento de vulnerabilidades	Não será exigida comprovação específica	—	—
11	Unidade de Serviço Técnico – UST	Não será exigida comprovação específica	—	—

5.12.27.1. As exigências estabelecidas neste item têm por finalidade assegurar que a futura contratada possua experiência compatível com as parcelas de maior relevância do objeto, sem impor requisitos excessivos ou desproporcionais que possam restringir indevidamente a competitividade do certame.

5.12.27.2. A comprovação da capacidade técnica deverá ser interpretada de forma compatível com a natureza integrada da contratação, admitindo-se experiências anteriores realizadas com diferentes fabricantes, tecnologias e arquiteturas, desde que demonstrada capacidade técnica suficiente para a execução das parcelas relevantes do objeto.

5.12.27.3. Para as parcelas em que houver exigência de comprovação de experiência, os critérios de dimensão da experiência serão estabelecidos de forma proporcional à natureza, às características e à complexidade dos respectivos serviços, quando tecnicamente necessários, não sendo exigida a reprodução integral da dimensão econômica ou operacional da presente contratação, nem a comprovação de valor mínimo de contrato ou de período de execução equivalente ao prazo integral da

Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



contratação, salvo quando expressamente justificado e estabelecido neste Termo de Referência.

5.12.27.4. Para os itens sujeitos à comprovação de dimensão mínima da experiência, serão considerados os quantitativos mínimos expressamente estabelecidos no quadro de qualificação técnica, correspondentes a 50% (cinquenta por cento) dos quantitativos previstos para as respectivas parcelas, observadas as unidades de medida aplicáveis a cada serviço. Não será exigida a reprodução integral da quantidade física ou da composição tecnológica da solução prevista na contratação.

5.12.27.5. Serão admitidos atestados que comprovem a execução de serviços com características, dimensões, períodos, valores, arquiteturas, tecnologias ou condições de execução distintas das previstas na contratação, desde que demonstrada a compatibilidade com a natureza, as características e a complexidade do serviço, observados, quando aplicáveis, os quantitativos mínimos e períodos mínimos de experiência expressamente estabelecidos neste Termo de Referência.

5.12.27.6. Não será exigida comprovação de experiência correspondente ao período integral de 12 (doze) meses previsto para a contratação. Para as parcelas sujeitas à exigência de período mínimo de experiência, será suficiente a comprovação de execução de serviços similares pelo período mínimo de 6 (seis) meses, sucessivos ou não, observados os demais critérios estabelecidos neste Termo de Referência.

5.12.27.7. No caso dos Itens 2 e 7, cuja prestação possui relação entre si, a Administração observará a natureza integrada da solução na execução contratual. Para fins de habilitação, contudo, a comprovação da capacidade técnica será analisada de acordo com a experiência efetivamente demonstrada pela licitante, não sendo exigida reprodução integral da composição tecnológica atualmente utilizada ou da quantidade de pontos prevista na contratação.

5.12.27.8. Para o Item 1, especificamente, a experiência anterior com NGFW/Firewall será considerada suficiente para fins de comprovação da capacidade técnica, não sendo exigido que o serviço anteriormente executado tenha sido prestado em arquitetura de cluster ou alta disponibilidade, considerando que tais características integram a solução atualmente pretendida, mas não são indispensáveis para demonstrar, isoladamente, a experiência operacional da licitante com a tecnologia de firewall.

5.12.27.9. A análise dos atestados deverá considerar o conteúdo efetivamente comprovado, admitindo-se experiências realizadas com diferentes fabricantes, marcas,
Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



modelos, plataformas e arquiteturas, desde que demonstrada compatibilidade com a parcela relevante do objeto.

5.12.28. Fundamentação da exigência de qualificação técnico-operacional:

Os requisitos de qualificação técnico-operacional estabelecidos neste Termo de Referência fundamentam-se no art. 67 da Lei nº 14.133/2021, especialmente em seus §§1º, 2º e 5º. A exigência de atestados está restrita às parcelas consideradas relevantes para a execução do objeto, enquanto os quantitativos mínimos, quando exigidos, observam o limite de até 50% (cinquenta por cento) das respectivas parcelas, conforme autorizado pelo §2º do referido artigo.

§ 1º A exigência de atestados será restrita às parcelas de maior relevância ou valor significativo do objeto da licitação, assim consideradas as que tenham valor individual igual ou superior a 4% (quatro por cento) do valor total estimado da contratação.

§ 2º Observado o disposto no caput e no § 1º deste artigo, será admitida a exigência de atestados com quantidades mínimas de até 50% (cinquenta por cento) das parcelas de que trata o referido parágrafo, vedadas limitações de tempo e de locais específicos relativas aos atestados.

Para os serviços de natureza continuada, a exigência de período mínimo de experiência de 6 (seis) meses fundamenta-se no §5º do art. 67, que permite a exigência de comprovação de execução de serviços similares, em períodos sucessivos ou não, por prazo mínimo, limitado pela própria legislação a 3 (três) anos.

§ 5º Em se tratando de serviços contínuos, o edital poderá exigir certidão ou atestado que demonstre que o licitante tenha executado serviços similares ao objeto da licitação, em períodos sucessivos ou não, por um prazo mínimo, que não poderá ser superior a 3 (três) anos.

Os requisitos foram dimensionados de forma proporcional às características e à complexidade dos serviços, sem exigir identidade de fabricante, marca, modelo, plataforma, arquitetura ou composição tecnológica. Busca-se, dessa forma, comprovar experiência efetiva na execução dos serviços relevantes, preservando a possibilidade de participação de empresas que tenham utilizado soluções tecnológicas distintas, desde que tecnicamente equivalentes.

5.12.28.1. Quantitativo e período mínimo de experiência:

A Lei nº 14.133/2021 não estabelece percentual obrigatório para os quantitativos mínimos de experiência, mas admite, no §2º do art. 67, a exigência de quantidades mínimas de até 50% (cinquenta por cento) das parcelas de maior relevância ou valor significativo. Assim, para os itens sujeitos à comprovação de



dimensão mínima, foi adotado o percentual de 50% (cinquenta por cento), considerado compatível com a natureza e a complexidade dos serviços pretendidos.

§ 2º Observado o disposto no caput e no § 1º deste artigo, será admitida a exigência de atestados com quantidades mínimas de até 50% (cinquenta por cento) das parcelas de que trata o referido parágrafo, vedadas limitações de tempo e de locais específicos relativas aos atestados.

Nos itens em que o quantitativo total corresponde a 12 (doze) unidade-mês, o requisito mínimo corresponde a 6 (seis) unidade-mês. No Item 2, cujo quantitativo total corresponde a 180 (cento e oitenta) unidade-mês, o requisito mínimo corresponde a 90 (noventa) unidade-mês.

A exigência de 6 (seis) meses de experiência decorre do §5º do art. 67 e refere-se ao período mínimo de execução de serviços similares, não constituindo limitação temporal dos atestados para fins do §2º. Dessa forma, os critérios de quantitativo e de período de experiência são aplicados de maneira distinta e complementar, sem exigir que a experiência anterior reproduza integralmente os 12 (doze) meses da contratação ou a quantidade física dos componentes da solução.

5.12.29. QUALIFICAÇÃO TÉCNICA

a) Comprovação de aptidão da LICITANTE para a execução de serviços compatíveis com o objeto da contratação, mediante apresentação de atestado(s) de capacidade técnica, fornecido(s) por pessoa jurídica de direito público ou privado, que demonstre(m) experiência anterior na execução de serviços de natureza compatível com as parcelas de maior relevância técnica e/ou valor significativo definidas neste Termo de Referência.

b) A comprovação de capacidade técnica será exigida exclusivamente para as parcelas classificadas como de maior relevância técnica e/ou valor significativo, conforme definido no item **5.12.2. deste Termo de Referência**, correspondentes aos seguintes serviços:

- I.** NGFW/SD-WAN em cluster de alta disponibilidade - Appliance Tipo 1;
- II.** NGFW/SD-WAN - Appliance Tipo 2;
- III.** Base de dados analíticos e logs - Appliance;
- IV.** Gerenciamento de NGFW - Appliance;
- V.** Endpoint corporativo - EDR;
- VI.** WAF - Appliance; e
- VII.** Plataforma de conscientização e campanhas de phishing.

c) Os atestados deverão demonstrar experiência anterior em serviços de natureza compatível com os serviços a serem executados, admitindo-se a comprovação por
Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



meio de soluções tecnicamente equivalentes, não sendo exigida experiência anterior em marca, fabricante, modelo ou arquitetura específica, conforme apresentado no **subitem “e” do item 5.12.1. neste Termos de Referência;**

Comprovação de experiência anterior na execução de serviços compatíveis em características e complexidade com as parcelas de maior relevância técnica ou valor significativo da presente contratação, conforme os requisitos e critérios estabelecidos neste Termo de Referência, especialmente aqueles detalhados na planilha constante do item 5.12.27.;

d) Para o Item 1 - NGFW/SD-WAN em cluster de alta disponibilidade - Appliance Tipo 1, será admitido atestado que comprove experiência na execução de serviços de NGFW ou Firewall, não sendo exigida experiência anterior especificamente em arquitetura de cluster ou alta disponibilidade, conforme o **item 5.12.17. deste Termo de Referência.**

Para o Item 1, será admitido atestado que comprove a execução de serviços de NGFW/Firewall, não sendo exigida, como condição mínima, a comprovação de experiência anterior em solução composta por cluster ou alta disponibilidade. A exigência será limitada à comprovação de experiência compatível com a prestação de serviços de firewall/NGFW, independentemente de a solução anteriormente executada possuir ou não arquitetura em alta disponibilidade.

e) Para o Item 2 - NGFW/SD-WAN - Appliance Tipo 2, será admitido atestado que comprove experiência na execução de serviços de NGFW ou Firewall, admitindo-se soluções tecnicamente equivalentes, conforme o **item 5.12.18. e seu subitem apresentado neste Termo de Referência.**

f) Para os itens sujeitos à comprovação de dimensão mínima da experiência, serão observados os quantitativos mínimos expressamente estabelecidos neste Termo de Referência, sem exigência de reprodução integral da quantidade física de equipamentos, pontos, endpoints, aplicações, usuários, campanhas ou demais componentes da solução prevista na contratação.

g) Será admitida a apresentação de um ou mais atestados de capacidade técnica, inclusive relativos a contratos distintos, desde que, em conjunto, demonstrem a experiência compatível e atendam aos quantitativos e períodos mínimos estabelecidos para cada item, ressalvado o Item 5 – EDR, que observará o critério específico de comprovação integral da experiência previsto neste Termo de Referência.

h) Não será exigida comprovação de experiência anterior em marca, fabricante, modelo ou solução específica, sendo admitida a comprovação mediante serviços



executados com soluções tecnicamente equivalentes, desde que compatíveis com as características e funcionalidades exigidas neste Termo de Referência.

i) A análise da documentação de qualificação técnica deverá observar a compatibilidade entre a experiência comprovada e as características efetivamente exigidas na contratação, vedada a imposição de requisitos de experiência superior, desnecessária ou desproporcional à dimensão e à complexidade do objeto.

j) A comprovação da qualificação técnica não se confunde com a comprovação do atendimento às especificações técnicas da solução ofertada, cuja análise será realizada conforme os procedimentos estabelecidos neste Termo de Referência e em seu **Apêndice**.

J.1) Solução de NGFW/SD-WAN em cluster fornecidos em appliance Tipo 1: o atendimento deverá observar os requisitos estabelecidos nos subitens 2.2.4.25 a 2.2.4.279 deste Termo de Referência e as características técnicas detalhadas no **item 5.1 e respectivos subitens do Apêndice**.

J.2) Solução de NGFW/SD-WAN fornecidos em appliance Tipo 2: o atendimento deverá observar os requisitos estabelecidos nos subitens 2.2.4.280 a 2.2.4.532 deste Termo de Referência e as características técnicas detalhadas no **item 5.2 e respectivos subitens do Apêndice**.

J.3) Solução da base de dados analíticos e logs fornecidos em appliance: o atendimento deverá observar os requisitos estabelecidos nos subitens 2.2.4.533 a 2.2.4.615 deste Termo de Referência e as características técnicas detalhadas no **item 5.3 e respectivos subitens do Apêndice**.

J.4) Solução de gerenciamento de NGFW fornecidos em appliance: o atendimento deverá observar os requisitos estabelecidos nos subitens 2.2.4.616 a 2.2.4.683 deste Termo de Referência e as características técnicas detalhadas no **item 5.4 e respectivos subitens do Apêndice**.

J.5) Solução de Endpoint corporativo do tipo EDR: o atendimento deverá observar os requisitos estabelecidos nos subitens 2.2.4.684 a 2.2.4.818 deste Termo de Referência e as características técnicas detalhadas no **item 5.5 e respectivos subitens do Apêndice**.

J.6) Solução de WAF appliance: o atendimento deverá observar os requisitos estabelecidos nos subitens 2.2.4.819 a 2.2.4.1.017 deste Termo de Referência e as características técnicas detalhadas no **item 5.6 e respectivos subitens do Apêndice**.

J.7) Solução de Access Point corporativo: o atendimento deverá observar os requisitos estabelecidos nos subitens 2.2.4.1.018 a 2.2.4.1.076 deste Termo de



Referência e as características técnicas detalhadas no **item 5.7 e respectivos subitens do Apêndice.**

J.8) Solução de Captive Portal: o atendimento deverá observar os requisitos estabelecidos nos subitens 2.2.4.1.077 a 2.2.4.1.206 deste Termo de Referência e as características técnicas detalhadas no **item 5.8 e respectivos subitens do Apêndice.**

J.9) Plataforma de conscientização e campanhas de phishing: o atendimento deverá observar os requisitos estabelecidos nos subitens 2.2.4.1.207 a 2.2.4.1.226 deste Termo de Referência e as características técnicas detalhadas no **item 5.10 e respectivos subitens do Apêndice.**

J.10) Mapeamento de Vulnerabilidades: o atendimento deverá observar os requisitos estabelecidos nos subitens 2.2.4.1.227 a 2.2.4.1.262 deste Termo de Referência e as características técnicas detalhadas no **item 5.11 e respectivos subitens do Apêndice.**

J.11) Unidade de Serviço Técnico - UST: o atendimento deverá observar os requisitos estabelecidos nos subitens 2.2.4.1.263 a 2.2.4.1.282 deste Termo de Referência e as características técnicas e condições de execução detalhadas no **item 5.12 e respectivos subitens do Apêndice.**

5.12.30. Para a solução de NGFW, deverão ser demonstrados os índices de eficácia e desempenho da solução do fabricante, mediante apresentação de relatório ou teste de laboratório independente (nacional ou internacional), ou documentação técnica oficial do fabricante, que evidencie a capacidade da solução de:

- a)** Prevenir no mínimo 70% (setenta por cento) dos malwares testados;
- b)** Prevenir no mínimo 70% (setenta por cento) de variantes de malwares conhecidos;
- c)** Possuir taxa de falso positivo na detecção de malware menor que 1% (um por cento);
- d)** Possuir taxa de prevenção de phishing e URLs maliciosas maior que 90% (noventa por cento).

5.12.30.1. As referências aos testes da empresa Miercom (a exemplo do relatório nº SR220915Q - NGFW Firewall Security Benchmark) possuem caráter meramente referencial, exemplificativo e orientativo, destinado a balizar os parâmetros mínimos de eficácia pretendidos pela Administração.

5.12.30.2. Serão aceitos para comprovação dos indicadores de desempenho:

- I.** Relatórios emitidos por outros laboratórios ou institutos independentes reconhecidos no mercado de tecnologia e cibersegurança (tais como NSS Labs, ICSA Labs, Virus Bulletin, Gartner, entre outros equivalentes);



- II. Fichas técnicas, datasheets, certidões ou documentações oficiais emitidas pelo próprio fabricante da solução ofertada que comprovem o atendimento às taxas e requisitos de prevenção exigidos.

5.12.30.3. As informações relativas aos indicadores de eficácia e desempenho da solução de NGFW (como taxas de prevenção de malware, controle de falsos positivos e bloqueio de phishing) apresentadas neste presente item (5.12.30) ou no 2.2.4.1.300 ao 2.2.4.1.305 possuem caráter técnico-referencial, orientativo e subsidiário, destinando-se a fornecer parâmetros de comparação para a equipe técnica do Município.

5.12.30.4. A apresentação de relatórios de testes de laboratórios independentes (a exemplo dos estudos da empresa Miercom, NSS Labs, ICSA Labs, Gartner, entre outros equivalentes) ou de documentação técnica do fabricante servirá exclusivamente como elemento de consulta, conferência e avaliação orientativa pela área de Tecnologia da Informação (TI/CPD).

5.12.30.5. A ausência de relatório emitido por laboratório específico ou eventuais divergências pontuais nos percentuais indicados não constituirão motivo para desclassificação da licitante, cabendo ao setor técnico responsável (TI/CPD) analisar o conjunto da documentação e certificar a equivalência e a compatibilidade da solução proposta com as necessidades do ambiente municipal

5.13. DAS CONDIÇÕES PARA PARTICIPAÇÃO DE EMPRESAS EM CONSÓRCIO:

5.13.1. Poderão participar deste processo quaisquer empresas interessadas que se enquadrem no ramo de atividade pertinente ao objeto da licitação e que atenderem a todas as exigências, inclusive quanto à documentação.

5.13.2. Não poderão participar deste processo:

5.13.2.1. Empresas que não atenderem às condições do Edital e seus Anexos;

5.13.2.2. Empresas que estejam em processo de falência ou concordata, sob concurso de credores, em dissolução ou em liquidação;

5.13.2.3. Pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

5.13.2.4. Empresas inadimplentes em obrigações assumidas com a Prefeitura Municipal de Sinop/MT;

5.13.2.5. Empresas cujo objeto social não seja pertinente e compatível com o objeto desta licitação;



5.13.2.6. Aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão da Ata de Registro de Preços, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

5.13.2.7. Empresas estrangeiras não autorizadas a funcionar no país;

5.13.2.8. Que constem nos cadastros oficiais: Certidão de Licitantes Inidôneos – TCU (Tribunal de Contas da União); CNIA – Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa e Inelegibilidade – CNJ (Conselho Nacional de Justiça); CEIS - Cadastro Nacional de Empresas Inidôneas e Suspensas – CJU (Controladoria Geral da União); CNEP – Cadastro Nacional de Empresas Punidas - CJU (Controladoria Geral da União) e; Comissão Processante Permanente da Prefeitura Municipal de Sinop/MT.

5.13.2.9. Autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre serviços ou fornecimento de bens a ele relacionados;

5.13.2.10. Empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre serviços ou fornecimento de bens a ela necessários;

5.13.2.11. Empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404/1976, concorrendo entre si;

5.13.2.12. Pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do Edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

5.13.2.13. Agente público do órgão ou entidade licitante;

5.13.2.14. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

5.13.2.15. Não poderá participar, direta ou indiretamente, da licitação ou da execução da Ata de Registro de Preços agente público do órgão ou entidade contratante, devendo ser observadas as situações que possam configurar conflito de interesses no



exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º do art. 9º da Lei Federal nº 14.133/2021.

5.13.3. O impedimento de que trata o item **5.13.2.3.** será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

5.13.4. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens **5.13.2.9. e 5.13.2.10.** poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão da Ata de Registro de Preços, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

5.13.5. Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

5.13.6. O disposto nos itens **5.13.2.9 e 5.13.2.10.** não impede a licitação ou a contratação de serviço que inclua como encargo da Contratada a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

5.13.7. Em licitações e contratações realizadas no âmbito de projetos e programas parcialmente financiados por agência oficial de cooperação estrangeira ou por organismo financeiro internacional com recursos do financiamento ou da contrapartida nacional, não poderá participar pessoa física ou jurídica que integre o rol de pessoas sancionadas por essas entidades ou que seja declarada inidônea nos termos da Lei Federal nº 14.133/2021.

5.13.8. A vedação de que trata o item **5.13.2.13.** estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de Equipe de Apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

5.13.9. Será permitida a participação de consórcio de empresas, sendo exigidas:

5.13.9.1. A comprovação da existência de compromisso público ou particular de constituição de consórcio, com indicação da empresa líder, que atenderá às condições de liderança estabelecidas no Edital e representará as consorciadas perante o município;

5.13.9.2. A apresentação da documentação de habilitação especificada no Edital por empresa consorciada;



5.13.9.3. A comprovação da capacidade técnica do consórcio pela somatória dos quantitativos de cada empresa consorciada, na forma estabelecida no Edital;

5.13.9.4. A demonstração, por cada empresa consorciada, do atendimento aos índices contábeis definidos no Edital, para fins de qualificação econômico-financeira;

5.13.9.5. A responsabilidade solidária das empresas consorciadas pelas obrigações do consórcio, nas etapas da licitação e durante a vigência da Ata de Registro de Preços ou Contrato, quando for o caso;

5.13.9.6. A obrigatoriedade de liderança por empresa brasileira no consórcio formado por empresas brasileiras e estrangeiras;

5.13.9.7. A constituição e o registro do consórcio antes da celebração da Ata de Registro de Preços ou Contrato, quando for o caso.

5.13.10. Fica vedada a participação de empresa consorciada, na mesma licitação, por meio de mais de um consórcio ou isoladamente.

5.13.11. Sob pena de inabilitação ou desclassificação, todos os documentos apresentados deverão referir-se ao mesmo CNPJ constante no credenciamento junto à plataforma eletrônica.

5.13.12. Será concedido tratamento favorecido para as Microempresas e Empresas de Pequeno Porte, para as Sociedades Cooperativas mencionadas no artigo 16 da Lei Federal nº 14.133/2021, para o Agricultor Familiar, o Produtor Rural pessoa física e para o Microempreendedor Individual - MEI, nos limites previstos da Lei Complementar nº 123/2006 e do Decreto nº 8.538/2015.

5.13.13. A obtenção do benefício a que se refere o item anterior fica limitada às Microempresas e às Empresas de Pequeno Porte que, no ano-calendário de realização da licitação, ainda não tenham celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como Empresa de Pequeno Porte.

5.13.14. Não será concedido tratamento diferenciado no caso de licitação para aquisição de bens ou contratação de serviços comuns, até mesmo de engenharia, ao item ou lote cujo valor estimado for superior à receita bruta máxima admitida para fins de enquadramento como Empresa de Pequeno Porte.

5.14. DA SUSTENTABILIDADE E IMPACTOS AMBIENTAIS

A presente contratação observará, no que couber, o princípio do desenvolvimento nacional sustentável, nos termos da Lei nº 14.133/2021, da Lei nº 12.305/2010 - Política Nacional de Resíduos Sólidos, e do Decreto Municipal nº 359/2023, considerando as características e a natureza dos serviços de segurança da

Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



informação contratados.

Considerando que o objeto consiste predominantemente na prestação de serviços especializados, com disponibilização de equipamentos, appliances, licenças, softwares, subscrições e demais recursos tecnológicos pela contratada, não foram identificados impactos ambientais significativos diretamente decorrentes da contratação que justifiquem a imposição de requisitos ambientais específicos como condição de participação ou de aceitação das soluções ofertadas.

Sem prejuízo disso, deverão ser observadas, durante a execução contratual, as seguintes medidas, quando aplicáveis:

a) adoção de práticas que promovam o uso racional de recursos materiais e energéticos empregados na execução dos serviços;

b) utilização, sempre que tecnicamente viável, de equipamentos e componentes que apresentem características de eficiência energética e compatibilidade com as normas técnicas e ambientais aplicáveis;

c) adoção de medidas destinadas à redução da geração de resíduos decorrentes da instalação, manutenção, substituição ou desmobilização dos equipamentos e componentes utilizados na prestação dos serviços;

d) realização do descarte, tratamento ou destinação ambientalmente adequada de equipamentos, componentes, materiais, embalagens, cabos, fontes, baterias e demais resíduos eventualmente gerados pela contratada durante a execução dos serviços, observada a legislação aplicável;

e) quando houver substituição ou retirada de equipamentos e componentes de propriedade da contratada, caberá a esta adotar as providências necessárias à sua destinação ambientalmente adequada, não sendo transferida à Administração a responsabilidade pelo descarte de materiais de propriedade da contratada.

As medidas acima serão aplicadas de acordo com a natureza das atividades efetivamente executadas, sem prejuízo da continuidade, disponibilidade, segurança e desempenho da solução contratada, não sendo admitida a adoção de práticas ambientais que comprometam os requisitos técnicos e operacionais estabelecidos neste Termo de Referência.

Dessa forma, embora não tenham sido identificados impactos ambientais relevantes que demandem requisitos específicos para a seleção da proposta, a execução contratual deverá observar práticas de sustentabilidade compatíveis com a natureza dos serviços, especialmente quanto ao uso racional de recursos, à eficiência dos equipamentos e à adequada destinação dos resíduos eventualmente gerados.



6. EXECUÇÃO DO OBJETO DO CONTRATO

6.1. OBRIGAÇÕES DAS PARTES:

6.1.1. OBRIGAÇÕES DA CONTRATADA:

6.1.1.1. Antes do início da execução da avença, designar formalmente (mediante comunicação escrita, através de correio eletrônico ao fiscal do contrato ou gestor da ata) preposto responsável por representar a contratada durante esse período;

6.1.1.2. Responsabilizar-se pelas despesas dos tributos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, fretes, seguros, deslocamento de pessoal, prestação de garantia e quaisquer outras que incidam ou venham a incidir na execução da ata ou contrato, inclusive nos casos relacionados à execução/substituição de equipamentos e componentes ou qualquer eventualidade que possa ocorrer;

6.1.1.3. Arcar com toda e qualquer despesa relativa à contratação ora pactuada, dentre elas, carga, transportes horizontais ou verticais, descarga, frete, impostos, mão de obra, contribuições e encargos sociais, *especialmente para serviços, deslocamento, instalação, etc.*;

6.1.1.4. Manter, durante toda a execução da ata/contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação ou na contratação;

6.1.1.5. Responsabilizar-se pelos vícios e danos decorrentes do objeto, *principalmente quanto às falhas, danos e prejuízos decorrentes da execução*, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

6.1.1.6. Atender prontamente a quaisquer exigências da Administração, inerentes ao objeto (serviços/contratação) da presente licitação;

6.1.1.7. Comunicar imediatamente à Administração, tão logo tenha conhecimento de qualquer fato ou circunstância que possa comprometer ou impedir o cumprimento dos prazos, condições ou obrigações assumidas, apresentando, no prazo que lhe for determinado, a devida justificativa e os documentos comprobatórios pertinentes, sem prejuízo da adoção imediata de todas as medidas necessárias para evitar ou reduzir os impactos decorrentes da ocorrência.

6.1.1.7.1. A comunicação de fato superveniente, imprevisível ou alheio à vontade da contratada não afastará, por si só, suas responsabilidades contratuais e legais,
Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



cabendo à Administração avaliar, diante das circunstâncias concretas, a ocorrência, os efeitos produzidos, as medidas adotadas pela contratada para prevenir ou mitigar os prejuízos e a eventual incidência das hipóteses legais aplicáveis.

6.1.1.7.2. A contratada permanecerá responsável pelos danos que causar diretamente à Administração ou a terceiros em razão da execução do contrato, nos termos da legislação aplicável, sem prejuízo do direito de buscar eventual ressarcimento perante terceiros que tenham contribuído para a ocorrência do fato, quando cabível.

6.1.1.7.3. A ocorrência de circunstâncias que possam comprometer o cumprimento dos prazos não exime a contratada do dever de ***adotar medidas alternativas e razoáveis para assegurar a continuidade ou conclusão da execução no menor prazo possível***, inclusive mediante substituição de pessoal, reorganização logística ou utilização de meios alternativos de deslocamento ou execução, quando tecnicamente e operacionalmente viáveis.

6.1.1.8. Não transferir a terceiros, por qualquer forma, as obrigações assumidas, nem subcontratar qualquer das prestações a que está obrigada;

6.1.1.9. Destacar e discriminar a retenção a que está sujeita, informando de forma clara e inequívoca todos os impostos e alíquotas incidentes, cabendo a ela toda a responsabilidade pela eventual ausência dessa informação ou pela informação incorreta;

6.1.1.10. As notas fiscais não poderão ter rasuras e deverão descrever corretamente o serviço/item, o número de empenho, o número do processo de compras e dados bancários para depósito. As notas fiscais serão liberadas para pagamento somente quando estiverem devidamente assinadas e carimbadas pelo servidor responsável;

6.1.1.11. As notas fiscais deverão ser encaminhadas à Prefeitura de Sinop, por meio do Portal do Fornecedor, disponível no endereço eletrônico: https://www.gp.srv.br/portalfornecedor_sinop/servlet/home, conforme Decreto 230/2023 de 06 de setembro de 2023.

6.1.1.12. O protocolo deverá ser realizado separadamente por Secretaria e Empenho/Nad;

6.1.1.12.1. ***A presente demanda será centralizada na gestão da Secretaria Municipal de Administração e Modernização de Sinop-MT;***

6.1.1.13. As certidões deverão ser juntadas ao protocolo e são obrigatórias para a liquidação da despesa;



6.1.1.14. Todos os documentos são obrigatórios, especialmente os citados no edital de licitação e os que constam na instrução normativa 038/2009, atualizada no decreto 118/2022;

6.1.1.15. Caso o protocolo não esteja de acordo com o solicitado, o mesmo será devolvido para correção, sendo válida a data de protocolo corrigida para fins de prazo de pagamento;

6.1.1.16. A(s) licitante(s) vencedora(s) se obriga(m) a entregar os serviços desta licitação sem ônus, mediante a emissão de ordem de fornecimento pelas Secretarias Municipais, a partir da data da assinatura do contrato;

6.1.1.16.1. *A presente demanda será centralizada na gestão da Secretaria Municipal de Administração e Modernização de Sinop-MT;*

6.1.1.17. Executar o objeto (serviços) desta licitação nos preços, prazos e forma estipulados na proposta durante a vigência da contratação;

6.1.1.18. Trocar, reparar, corrigir, remover, reconstituir ou substituir, às expensas próprias, no total ou em parte, o objeto (serviços) deste termo de referência, qualquer situação onde se verifiquem vícios, defeitos ou incorreções resultantes da sua fabricação e fornecimento que não atendam às exigências fixadas no termo de referência, edital e seus anexos, principalmente quanto a correção de falhas, indisponibilidades, configurações inadequadas, etc.;

6.1.1.19. Assumir todas as despesas relativas a pessoal e quaisquer outras oriundas, derivadas ou conexas com a contratação, ficando, ainda, para todos os efeitos legais, declaradas pela LICITANTE VENCEDORA a inexistência de qualquer vínculo empregatício entre seus empregados e/ou prepostos e a Administração Municipal;

6.1.1.20. Responsabilizar-se por todo e qualquer dano e/ou prejuízo que, eventualmente, venha a sofrer os objetos (serviços) desta licitação, em decorrência do transporte dos mesmos;

6.1.1.21. PROTEÇÃO DE DADOS PESSOAIS (LGPD): Cumprir, durante toda a execução contratual, as disposições da Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), bem como da regulamentação aplicável, sempre que houver tratamento de dados pessoais no âmbito da execução dos serviços, adotando medidas técnicas e administrativas adequadas à proteção dos dados contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito.



6.1.1.21.1. Utilizar os dados pessoais e demais informações eventualmente acessados em razão da execução contratual exclusivamente para as finalidades necessárias ao cumprimento das obrigações assumidas, observando as orientações e instruções da Administração e abstendo-se de utilizá-los para finalidade diversa, salvo quando houver fundamento legal que autorize o tratamento.

6.1.1.22. SEGURANÇA DE CREDENCIAIS E ACESSOS: Manter sob sigilo e utilizar de forma adequada todas as credenciais, senhas, chaves de acesso, certificados, tokens, contas administrativas e demais mecanismos de autenticação disponibilizados ou utilizados para acesso aos recursos tecnológicos do Município, permitindo seu uso somente por profissionais devidamente autorizados e na medida necessária à execução dos serviços.

6.1.1.22.1. Adotar medidas para impedir o compartilhamento indevido, uso não autorizado, exposição ou comprometimento das credenciais utilizadas na execução dos serviços, comunicando imediatamente à Administração qualquer suspeita ou ocorrência de comprometimento de credenciais ou acessos.

6.1.1.22.2. Encerrar ou solicitar o encerramento dos acessos de profissionais que deixem de atuar na execução dos serviços, sempre que tais acessos estiverem sob responsabilidade ou gestão da contratada.

6.1.1.23. COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA: Comunicar imediatamente à Administração qualquer incidente de segurança da informação, vulnerabilidade crítica, comprometimento de credenciais, acesso não autorizado, indisponibilidade relevante ou outra ocorrência identificada durante a execução dos serviços que possa comprometer a segurança, integridade, confidencialidade ou disponibilidade da infraestrutura tecnológica ou das informações do Município.

6.1.1.23.1. Adotar, sem prejuízo das demais obrigações contratuais, as medidas técnicas necessárias para contenção, mitigação, correção e restabelecimento da normalidade da solução, mantendo a Administração informada acerca das providências adotadas e da evolução da ocorrência.

6.1.1.23.2. Sempre que solicitado pela Administração, apresentar informações técnicas relacionadas ao incidente, incluindo sua natureza, recursos afetados, medidas adotadas e providências necessárias para prevenção de ocorrências semelhantes, observadas as limitações decorrentes da própria segurança da informação.

6.1.1.24. SIGILO E CONFIDENCIALIDADE: Manter sigilo e confidencialidade sobre todas as informações, dados, documentos, credenciais, configurações,



registros, topologias, endereçamentos, políticas de segurança e demais informações a que tiver acesso em razão da execução dos serviços, não as divulgando, reproduzindo, disponibilizando ou utilizando para finalidade diversa daquela necessária à execução contratual.

6.1.1.24.1. As obrigações de sigilo e confidencialidade permanecerão aplicáveis durante toda a execução contratual e, quando cabível em razão da natureza das informações, após o encerramento da contratação, sem prejuízo das responsabilidades legais e contratuais decorrentes de eventual divulgação ou utilização indevida.

6.1.1.25. REGISTROS, LOGS E INFORMAÇÕES PARA FISCALIZAÇÃO: Manter, quando tecnicamente aplicável e pelo período necessário à execução e à fiscalização dos serviços, os registros e informações técnicas decorrentes das atividades realizadas na solução, incluindo logs, registros de alterações, eventos de segurança e demais informações necessárias ao acompanhamento, diagnóstico e fiscalização contratual.

6.1.1.25.1. Disponibilizar à Administração, quando solicitado e observados os requisitos de segurança e confidencialidade, os registros e informações técnicas necessários à fiscalização, análise de ocorrências, verificação do funcionamento da solução e acompanhamento da execução contratual.

6.1.1.26. ENCERRAMENTO E TRANSIÇÃO DA SOLUÇÃO: Ao término da execução dos serviços ou da vigência da contratação, prestar o apoio técnico necessário ao encerramento ou à transição da solução, quando aplicável, de modo a evitar interrupções indevidas dos serviços e assegurar a continuidade operacional da infraestrutura de segurança da informação do Município.

6.1.1.26.1. Fornecer à Administração, quando cabível, as informações técnicas, configurações, registros e demais elementos necessários à continuidade, manutenção ou substituição da solução, observadas as condições estabelecidas no Termo de Referência e os requisitos de segurança da informação.

6.1.1.26.2. Encerrar, após o término da execução e conforme orientação da Administração, os acessos, credenciais e demais mecanismos de acesso aos ambientes municipais que tenham sido disponibilizados à contratada ou a seus profissionais exclusivamente para execução dos serviços.

6.1.1.27. RETIRADA E DEVOLUÇÃO DE EQUIPAMENTOS: Ao término da utilização dos equipamentos disponibilizados pela contratada para execução dos serviços, quando estes forem de sua propriedade ou estiverem sob sua

Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



responsabilidade, realizar sua retirada ou devolução, conforme orientação da Administração, sem causar interrupção indevida ou prejuízo ao funcionamento dos demais componentes da solução.

6.1.1.27.1. A retirada dos equipamentos deverá ser previamente coordenada com a Administração e realizada de forma tecnicamente segura, cabendo à contratada adotar as providências necessárias para preservar a integridade dos demais equipamentos, sistemas, configurações e infraestrutura do Município.

6.1.1.27.2. Quando houver informações, dados, registros ou configurações armazenados nos equipamentos retirados, a contratada deverá observar as orientações da Administração quanto à preservação, transferência, eliminação ou tratamento dessas informações, em conformidade com a legislação aplicável e os requisitos de segurança da informação.

6.1.2. OBRIGAÇÕES DA CONTRATANTE:

6.1.2.1. Atestar as Notas Fiscais e/ou faturas relativas aos serviços efetivamente executados e disponibilizados pela contratada, após a verificação de sua conformidade com as condições e especificações estabelecidas no Termo de Referência e no instrumento contratual;

6.1.2.2. Promover o acompanhamento e a fiscalização da execução dos serviços objeto da contratação, sob os aspectos quantitativo e qualitativo, inclusive quanto ao atendimento dos prazos, níveis de serviço, condições técnicas e demais requisitos estabelecidos no Termo de Referência, registrando em instrumento próprio as falhas e ocorrências eventualmente detectadas;

6.1.2.3. Comunicar prontamente à contratada qualquer anormalidade ou desconformidade identificada na execução dos serviços, podendo recusar, total ou parcialmente, a execução que não esteja de acordo com as especificações, condições e requisitos estabelecidos no Termo de Referência e no instrumento contratual;

6.1.2.4. A Contratante não responderá por quaisquer compromissos assumidos pela Contratada com terceiros, bem como por danos causados a terceiros em decorrência de atos praticados pela Contratada, seus empregados, prepostos ou subordinados, observadas as responsabilidades legalmente atribuídas à Administração;

6.1.2.5. Fornecer as informações, orientações e acessos internos que sejam necessários e pertinentes à execução dos serviços, observadas as condições de segurança da informação, as regras internas da Administração e os limites de acesso previamente estabelecidos;



6.1.2.6. Conferir a documentação, os relatórios, registros, informações técnicas, evidências de execução e demais elementos apresentados pela contratada durante a execução dos serviços, efetuando o respectivo atesto quando estiverem em conformidade com os padrões, requisitos e condições estabelecidos no Termo de Referência e no instrumento contratual;

6.1.2.7. Efetuar o pagamento pelos serviços efetivamente executados, de acordo com as condições estabelecidas no Termo de Referência e no instrumento contratual, desde que atendidas as exigências administrativas e fiscais pertinentes e devidamente atestada a execução pelos responsáveis pela gestão e fiscalização da contratação;

6.1.2.8. Aplicar à contratada as penalidades cabíveis, quando constatado o descumprimento das obrigações assumidas, observados o devido processo administrativo, o contraditório e a ampla defesa, nos termos da legislação aplicável;

6.1.2.9. Notificar, por escrito, a contratada acerca da aplicação de qualquer sanção ou medida administrativa decorrente da execução contratual, observados os procedimentos previstos na legislação e no instrumento contratual;

6.1.2.10. Acompanhar, controlar e avaliar a execução e a qualidade dos serviços, por meio da Secretaria Municipal de Administração e Modernização, com apoio da equipe técnica do Centro de Processamento de Dados - CPD e dos servidores formalmente designados para a gestão e fiscalização da contratação;

6.1.2.11. Proporcionar as condições e facilidades necessárias à execução dos serviços, permitindo, quando necessário e previamente autorizado, o acesso dos profissionais da contratada às dependências da Administração. Os profissionais da contratada deverão observar todas as normas internas da Contratante, especialmente aquelas relacionadas à identificação, segurança da informação, controle de acesso, circulação, permanência e utilização das instalações e recursos tecnológicos municipais;

6.1.2.12. *No caso de atraso imputável à Contratante no pagamento de valores regularmente devidos à Contratada, os valores poderão ser atualizados monetariamente entre o termo final do prazo de pagamento e a data de sua efetiva realização, mediante aplicação do índice de correção monetária estabelecido no instrumento contratual, observadas as condições e hipóteses previstas na legislação aplicável.*

6.2. CRITÉRIOS DE RECEBIMENTO PROVISÓRIO E DEFINITIVO DO OBJETO DA CONTRATAÇÃO:

Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



6.2.1. Recebimento Provisório: O recebimento provisório será mediante o registro de recebimento dos serviços pela Fiscalização, para efeito de posterior verificação de sua conformidade com as especificações e condições constantes do Termo de Referência;

6.2.2. Recebimento Definitivo: O recebimento definitivo será mediante recibo, em até 5 (cinco) dias úteis após o recebimento provisório e a verificação da perfeita execução das obrigações contratuais, ocasião em que se fará constar o atesto da nota fiscal e/ou fatura.

6.2.2.1. O registro de recebimento dos serviços em nota fiscal, relatório ou documento similar não configura, por si só, o recebimento definitivo dos serviços;

6.2.2.2. O Recebimento Definitivo não exclui a responsabilidade da contratada por falhas na execução, vícios, indisponibilidades, desconformidades ou demais irregularidades relacionadas aos serviços, ainda que verificadas posteriormente.

6.2.2.3. Acrescenta-se que o recebimento do objeto contratado ocorrerá respeitando o Art. 43 do Decreto Municipal nº 359/2023.

Art. 43. O recebimento do objeto contratado ocorrerá da seguinte forma:

I - Na hipótese de obras ou prestação de serviços:

a) provisoriamente, pelo fiscal, mediante termo detalhado, quando verificado o cumprimento das exigências de caráter técnico previamente definidos no Contrato;

b) definitivamente, pelo gestor em conjunto com a comissão de recebimento, mediante termo detalhado que comprove o atendimento das exigências contratuais.

6.3. LOCAL, HORÁRIO, PERIODICIDADE E FORMA DE ENTREGA/EXECUÇÃO DO OBJETO E CRITÉRIOS DE ACEITAÇÃO OU NÃO DO OBJETO:

6.3.1. O prazo para início da execução e disponibilização da solução deverá ser de até **48 (quarenta e oito) horas** (horário de Cuiabá/MT), a contar do recebimento da Nota de Autorização de Despesa (NAD) pelo responsável da empresa contratada, ficando a solução sujeita à conferência, acompanhamento e aceite pelo fiscal e/ou servidor responsável.

6.3.2. Caso o horário de expediente da Contratante seja alterado por determinação legal ou imposição de circunstâncias supervenientes, deverá ser promovida a adequação dos horários de execução e dos atendimentos presenciais necessários ao cumprimento das obrigações contratuais, sem prejuízo dos prazos e níveis de atendimento estabelecidos neste Termo de Referência.



6.3.3. Caso a execução ou disponibilização da solução não possa ser realizada no prazo previsto, a contratada deverá comunicar imediatamente a Administração, tão logo tenha conhecimento do fato que possa comprometer o cumprimento do prazo, apresentando a respectiva justificativa e documentação comprobatória, quando aplicável, nos termos do subitem **6.1. “OBRIGAÇÕES DAS PARTES”**, especialmente do subitem **6.1.1.7.**, para análise da Administração e adoção das providências cabíveis.

6.1.1.7. Comunicar imediatamente à Administração, tão logo tenha conhecimento de qualquer fato ou circunstância que possa comprometer ou impedir o cumprimento dos prazos, condições ou obrigações assumidas, apresentando, no prazo que lhe for determinado, a devida justificativa e os documentos comprobatórios pertinentes, sem prejuízo da adoção imediata de todas as medidas necessárias para evitar ou reduzir os impactos decorrentes da ocorrência.

6.1.1.7.1. A comunicação de fato superveniente, imprevisível ou alheio à vontade da contratada não afastará, por si só, suas responsabilidades contratuais e legais, cabendo à Administração avaliar, diante das circunstâncias concretas, a ocorrência, os efeitos produzidos, as medidas adotadas pela contratada para prevenir ou mitigar os prejuízos e a eventual incidência das hipóteses legais aplicáveis.

6.1.1.7.2. A contratada permanecerá responsável pelos danos que causar diretamente à Administração ou a terceiros em razão da execução do contrato, nos termos da legislação aplicável, sem prejuízo do direito de buscar eventual ressarcimento perante terceiros que tenham contribuído para a ocorrência do fato, quando cabível.

6.1.1.7.3. A ocorrência de circunstâncias que possam comprometer o cumprimento dos prazos não exime a contratada do dever de adotar medidas alternativas e razoáveis para assegurar a continuidade ou conclusão da execução no menor prazo possível, inclusive mediante substituição de pessoal, reorganização logística ou utilização de meios alternativos de deslocamento ou execução, quando tecnicamente e operacionalmente viáveis.

6.3.4. Os serviços estarão sujeitos à conferência, acompanhamento e aceite pelo fiscal e/ou servidor responsável e, estando em desconformidade com as especificações, condições ou requisitos estabelecidos neste Termo de Referência, a contratada deverá promover, às suas expensas, as correções, ajustes ou providências necessárias à regularização da execução, no prazo estabelecido pela fiscalização, considerando a natureza, a criticidade e o impacto da ocorrência, sem prejuízo da aplicação das medidas administrativas e sanções cabíveis.

6.3.5. Seguem abaixo os endereços/dedes da(s) Secretaria(s):

6.3.5.1. Secretaria Municipal de Administração e Modernização, localizada na Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500.

Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



6.3.6. ENTREGA/EXECUÇÃO EM OUTRO ENDEREÇO: Caso seja solicitada pela Secretaria Municipal de Administração e Modernização a realização de atendimento, instalação, manutenção, suporte técnico, visita ou qualquer outra atividade presencial em endereço diverso daquele indicado no subitem **6.3.5.1.**, desde que situado dentro do perímetro urbano do Município de Sinop-MT, a contratada deverá realizar o atendimento no local indicado pela Administração, sem ônus adicional, observadas as condições e os prazos estabelecidos neste Termo de Referência.

6.3.6.1. Para fins de verificação do cumprimento do prazo de execução, a solução será considerada efetivamente disponibilizada somente após a conclusão das atividades aplicáveis ao item solicitado, incluindo, quando cabível, a instalação, configuração, integração, ativação, realização dos testes necessários e disponibilização dos serviços em condições adequadas de funcionamento, conforme as especificações estabelecidas neste Termo de Referência.

6.4. PRAZO MÍNIMO DE VALIDADE DO PRODUTO/SERVIÇO:

6.4.1. Não se aplica.

6.4.2. *Não se aplica*, tendo em vista que o objeto da contratação consiste na prestação de serviços especializados de segurança da informação e na disponibilização de soluções tecnológicas durante a vigência da contratação, não havendo fornecimento de produtos sujeitos a prazo de validade.

As soluções e serviços deverão permanecer disponíveis, operacionais e em conformidade com as especificações estabelecidas neste Termo de Referência durante todo o período de execução contratual, observadas as condições de suporte, manutenção, atualização e demais obrigações previstas para a contratada.

6.5. ESPECIFICAÇÃO DA GARANTIA EXIGIDA:

6.5.1. Não se aplica.

6.5.2. *Não se aplica garantia contratual específica sobre os equipamentos e soluções disponibilizados pela contratada*, considerando que os recursos tecnológicos empregados na execução permanecerão sob responsabilidade da própria contratada durante a vigência da contratação.

A contratada deverá, contudo, assegurar a continuidade e o adequado funcionamento das soluções disponibilizadas, realizando, às suas expensas, as correções, substituições, atualizações, manutenções e demais providências necessárias ao cumprimento das especificações e níveis de serviço estabelecidos neste Termo de Referência, sem prejuízo das demais responsabilidades decorrentes da execução contratual.



6.6. CONDIÇÕES DE MANUTENÇÃO PREVENTIVA E/OU CORRETIVA E ASSISTÊNCIA TÉCNICA:

As atividades de manutenção preventiva e/ou corretiva, atualização, correção de falhas e assistência técnica necessárias ao adequado funcionamento das soluções disponibilizadas pela contratada deverão ser realizadas pela própria contratada, sempre que necessárias à continuidade e à adequada execução dos serviços.

As condições específicas, prazos e procedimentos para atendimento, correção de falhas, manutenção e suporte serão observados durante a execução contratual, conforme as características de cada solução e as disposições estabelecidas neste Termo de Referência.

A execução dessas atividades constitui obrigação da contratada durante a vigência da contratação e ***não será utilizada, por si só, como requisito adicional de habilitação ou classificação da licitante***, sem prejuízo da verificação, pela Administração, do cumprimento das obrigações previstas durante a execução contratual.

6.7. CRONOGRAMA DE EXECUÇÃO:

6.7.1. Não se aplica.

6.7.2. Não se aplica a elaboração de cronograma físico detalhado previamente à contratação, considerando que a execução dos serviços ocorrerá de acordo com as necessidades da Administração, mediante as solicitações formalizadas e os procedimentos estabelecidos neste Termo de Referência.

O planejamento das atividades de implantação, configuração, disponibilização, manutenção, suporte e demais ações necessárias à execução dos serviços será realizado entre a contratada e a Secretaria Municipal de Administração e Modernização, especialmente por meio do setor técnico responsável, observados os prazos e condições estabelecidos neste Termo de Referência.

A ausência de cronograma prévio não afasta a obrigação da contratada de cumprir os prazos de atendimento e execução estabelecidos para cada solicitação formalizada pela Administração.

6.8. NECESSIDADE DE ACOMPANHAMENTO DOS SERVIÇOS POR PROFISSIONAIS DA “ÁREA” DEMANDANTE:

A execução dos serviços será acompanhada e fiscalizada pela Administração, por meio dos servidores responsáveis e, especialmente, pelo setor técnico de Tecnologia da Informação e Comunicação - CPD, conforme as atribuições definidas para a fiscalização contratual.



A contratada deverá disponibilizar ***profissional técnico devidamente capacitado e apto a executar e acompanhar os serviços objeto da contratação***, sempre que necessário, inclusive para realização das visitas técnicas periódicas e demais atividades presenciais ou remotas necessárias à execução.

A indicação ou disponibilização desse profissional **não constitui exigência de apresentação de documentação específica para fins de habilitação**, quando inexistente conselho profissional ou requisito legal que determine tal comprovação, devendo a capacidade técnica necessária ser demonstrada na própria execução dos serviços.

As visitas técnicas e demais atividades de acompanhamento serão realizadas conforme as necessidades da execução contratual e as condições estabelecidas neste Termo de Referência.

6.9. POSSIBILIDADE DE TROCA DE PEÇAS, SE POR ORIGINAIS OU SIMILARES, E DE PROCESSOS DE REMANUFATURA, RECONDICIONAMENTO, REUTILIZAÇÃO OU REFILAMENTO:

6.9.1. Não se aplica.

6.9.2. Não se aplica como requisito específico, considerando que os equipamentos, componentes e demais recursos tecnológicos utilizados na execução dos serviços serão disponibilizados e permanecerão sob a responsabilidade da contratada.

Eventuais substituições de equipamentos, componentes ou demais recursos necessários à continuidade e ao adequado funcionamento das soluções deverão ser realizadas pela contratada, sem prejuízo da execução dos serviços e sem ônus adicional para a Administração, observadas as especificações e condições estabelecidas neste Termo de Referência.

Quando houver necessidade de substituição, o recurso utilizado deverá ser compatível com a solução contratada e não poderá ocasionar redução de desempenho, segurança, funcionalidade ou qualquer prejuízo à Administração.

6.10. POSSIBILIDADE OU NÃO DE SUBCONTRATAÇÃO:

Não será permitida a subcontratação das obrigações assumidas pela contratada, total ou parcialmente, considerando a natureza integrada da solução de segurança da informação e a necessidade de que a empresa contratada mantenha responsabilidade direta pela execução, operação, suporte, manutenção e continuidade dos serviços.

A vedação busca assegurar que a Administração possua ***um único responsável pela execução e pelo suporte das soluções contratadas***, evitando a fragmentação
Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



das responsabilidades entre diferentes empresas e eventuais dificuldades de comunicação, fiscalização, atendimento e responsabilização decorrentes da utilização de terceiros.

A contratada permanecerá integralmente responsável perante a Administração pelo cumprimento das obrigações assumidas, inclusive quanto à qualidade, continuidade, segurança e adequado funcionamento dos serviços.

6.11. POSSIBILIDADE DE PRORROGAÇÃO CONTRATUAL E REAJUSTE:

A Ata de Registro de Preços terá vigência de **1 (um) ano**, contado da data de sua assinatura, podendo ser prorrogada por igual período, desde que comprovada a vantajosidade dos preços registrados e observadas as demais condições previstas no art. 84 da Lei nº 14.133/2021 e na regulamentação aplicável.

Art. 84. O prazo de vigência da ata de registro de preços será de 1 (um) ano e poderá ser prorrogado, por igual período, desde que comprovado o preço vantajoso.

Parágrafo único. O contrato decorrente da ata de registro de preços terá sua vigência estabelecida em conformidade com as disposições nela contidas.

Na hipótese de prorrogação da Ata de Registro de Preços, ***poderá ser renovado o quantitativo*** originalmente registrado para os itens, observados os limites dos quantitativos inicialmente registrados, desde que atendidas as condições legais e regulamentares aplicáveis, comprovada a vantajosidade dos preços e mediante prévia consulta e anuência do fornecedor. A renovação do quantitativo não implica obrigação de contratação pela Administração, permanecendo as solicitações condicionadas à necessidade administrativa, à formalização das contratações decorrentes e à disponibilidade orçamentária.

6.11.1. O contrato terá vigência de 1 (um) ano, a contar da data de sua assinatura, com eficácia a partir de sua publicação, compreendendo os prazos de instalação e configuração dos procedimentos de recebimento fixados, podendo ser prorrogado, nos termos dos Art. 105 a 107 da Lei nº 14.133/2021;

Art. 105. A duração dos contratos regidos por esta Lei será a prevista em edital, e deverão ser observadas, no momento da contratação e a cada exercício financeiro, a disponibilidade de créditos orçamentários, bem como a previsão no plano plurianual, quando ultrapassar 1 (um) exercício financeiro.

Parágrafo único. Não serão objeto de cancelamento automático os restos a pagar vinculados a contratos de duração plurianual, senão depois de encerrada a vigência destes, nem os vinculados a contratos rescindidos, nos casos dos §§ 8º e 9º do art. 90 desta Lei. (Incluído pela Lei nº 14.770, de 2023)



6.11.2. Conforme o § 3º do artigo 92 da Lei 14.133/2021, independentemente do prazo de duração, o contrato deverá ser reajustado com data-base vinculada à data do orçamento estimado.

Art. 92. São necessárias em todo contrato cláusulas que estabeleçam:

§ 3º Independentemente do prazo de duração, o contrato deverá conter cláusula que estabeleça o índice de reajustamento de preço, com data-base vinculada à data do orçamento estimado, e poderá ser estabelecido mais de um índice específico ou setorial, em conformidade com a realidade de mercado dos respectivos insumos.

6.11.3. Data de finalização da pesquisa estimativa de preços: ***Pesquisa realizada entre 06/08/2026 16:19:49 e 18/08/2026 08:25:49.***

6.11.4. O índice de reajuste se dará com fulcro na IN SGD/ME nº 94, de 23 de dezembro de 2022: Nas contratações de serviços de Tecnologia da Informação em que haja previsão de reajuste de preços por aplicação de índice de correção monetária, é obrigatória a adoção do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA.

Para fins de reajuste em sentido estrito, sua aplicação está vinculada ao prévio requerimento do contratado.

6.12. DA ALTERAÇÃO E DA ATUALIZAÇÃO DOS PREÇOS REGISTRADOS:

6.12.1. Após o interregno de um ano, e independentemente de pedido da Contratada, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do índice ICTI, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade, no que tange aos insumos e demais materiais de mercado.

6.12.2. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

6.12.3. No caso de atraso ou não divulgação do(s) índice(s) de reajustamento, a Contratante pagará à Contratada a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

6.12.4. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

6.12.5. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.



6.12.6. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

6.12.7. O reajuste será realizado por Apostilamento.

6.12.8. No caso do reajustamento, deverá ser respeitada a contagem da anualidade e o índice previstos para a contratação.

6.12.9. No caso da repactuação, poderá ser a pedido do interessado, conforme critérios definidos para a contratação.

6.13. APLICAÇÃO DE SANÇÕES ADMINISTRATIVAS: As sanções de que tratam este Termo de Referência são aquelas descritas nos Art. 155 a 163 da Lei 14.133/2021 e no Decreto 360/2023.

6.14. NECESSIDADE DE APRESENTAÇÃO DE RELATÓRIOS DE MANUTENÇÃO:

Não será estabelecida periodicidade fixa para a apresentação de relatórios de manutenção. Contudo, sempre que solicitado pela Administração, especialmente pelo setor técnico responsável, a contratada deverá apresentar relatório contendo as informações necessárias à comprovação das atividades realizadas, ocorrências identificadas, intervenções efetuadas, medidas corretivas adotadas e demais informações pertinentes à execução dos serviços.

Os relatórios eventualmente solicitados deverão ser apresentados dentro do prazo definido pela Administração, considerando a natureza e a complexidade das informações requeridas.

6.15. MOBILIZAÇÃO E DESMOBILIZAÇÃO DO CANTEIRO DE OBRAS (BARRACÃO, INSTALAÇÕES DE PONTOS DE ÁGUA, ENERGIA E ESGOTO):

6.15.1. Não se aplica.

6.15.2. Não se aplica, considerando que o objeto da contratação não envolve execução de obras ou instalação de canteiro de obras, barracão ou estruturas provisórias dessa natureza.

6.16. LIMPEZA DOS LOCAIS DE INSTALAÇÃO E/OU REMOÇÃO DE ENTULHOS; EXIGÊNCIAS ESPECÍFICAS PARA O OBJETO A SER CONTRATADO:

6.16.1. Não se aplica.

6.16.2. *Não se aplica como obrigação específica*, considerando a natureza do objeto, que consiste na prestação de serviços especializados de segurança da informação e disponibilização de soluções tecnológicas, sem execução de obras ou atividades que impliquem geração significativa de entulhos.



Eventuais resíduos decorrentes de atividades presenciais de instalação, manutenção ou substituição de equipamentos deverão ser devidamente recolhidos e destinados pela contratada, quando aplicável, sem ônus para a Administração.

6.17. NECESSIDADE DE DISPONIBILIZAÇÃO DE SAC E INDICAÇÃO DO NÚMERO PARA ATENDIMENTO COMERCIAL: A contratada deverá disponibilizar canais de comunicação para atendimento da Administração, destinados ao acompanhamento da execução contratual, solicitações, esclarecimentos e demais assuntos relacionados aos serviços contratados.

Deverão ser disponibilizados, no mínimo, **1 (um) número de telefone para atendimento, 1 (um) número para atendimento via WhatsApp e 1 (um) endereço de e-mail**, devendo os respectivos contatos ser formalmente informados à Administração antes do início da execução dos serviços.

Os canais disponibilizados deverão permanecer atualizados durante toda a vigência da contratação, devendo a contratada comunicar previamente qualquer alteração.

6.18. POSSIBILIDADE DE SUPORTE TÉCNICO REMOTO OU PELO SITE ELETRÔNICO, BEM COMO O PRAZO PARA ATENDIMENTO, FORMA DE ATENDIMENTO (0-800, E-MAIL, ETC.), PRAZO E FORMA PARA A SOLUÇÃO DO PROBLEMA, SUBSTITUIÇÃO DO EQUIPAMENTO DEFEITUOSO: A contratada deverá disponibilizar suporte técnico necessário à adequada execução dos serviços e ao funcionamento das soluções contratadas, podendo o atendimento ser realizado de forma remota ou presencial, conforme a natureza da demanda e a necessidade identificada pela Administração.

Os canais de atendimento deverão ser disponibilizados pela contratada e informados formalmente à Administração, podendo compreender telefone, WhatsApp, correio eletrônico, plataforma eletrônica de chamados ou outros meios disponibilizados pela empresa.

As condições, prazos e procedimentos específicos para atendimento e solução das demandas deverão observar as disposições deste Termo de Referência e as necessidades identificadas durante a execução contratual.

A disponibilidade de suporte técnico remoto ou por plataforma eletrônica constitui condição relacionada à execução dos serviços, não sendo exigida, para fins de habilitação ou classificação, a apresentação de comprovação específica de que a licitante dispõe previamente de determinado canal ou plataforma de suporte, ressalvados os requisitos expressamente estabelecidos neste Termo de Referência.



Quando necessária a substituição de equipamento, componente ou recurso tecnológico utilizado na execução dos serviços, caberá à contratada providenciar a substituição ou correção necessária, de modo a assegurar a continuidade e o adequado funcionamento da solução, sem prejuízo das demais responsabilidades contratuais.

Requisitos Gerais

6.18.1. A CONTRATADA deverá informar, em sua proposta, o fabricante e os respectivos modelos dos equipamentos e demais componentes de hardware que serão utilizados na execução da solução, quando aplicável.

6.18.2. Cada equipamento e componente da solução deverá ser fornecido com todos os acessórios, componentes, licenças, subscrições, softwares e demais recursos necessários à sua instalação, configuração, operação, monitoramento e pleno funcionamento, cabendo à CONTRATADA realizar a instalação e configuração das funcionalidades que compõem a solução.

6.18.3. Os equipamentos fornecidos deverão ser novos, sem uso anterior, e estar em linha de comercialização e suporte pelo fabricante na data de apresentação da proposta, não podendo estar oficialmente classificados pelo fabricante como produto em processo de descontinuação de venda ou suporte naquela data.

6.18.4. Os componentes da solução cuja indisponibilidade possa comprometer a continuidade dos serviços de segurança da informação ou o funcionamento da infraestrutura protegida deverão ser disponibilizados em arquitetura de alta disponibilidade, observadas as características e os requisitos técnicos estabelecidos para cada item.

6.18.5. Os gateways de segurança deverão ser fornecidos em appliance de hardware dedicado, não sendo admitida a utilização de servidores de uso genérico para execução das funcionalidades principais de proteção de rede.

6.18.6. A CONTRATADA será integralmente responsável pela disponibilização dos recursos necessários ao funcionamento da solução, inclusive equipamentos, acessórios, licenças, subscrições, softwares e demais componentes previstos nas especificações, não podendo a CONTRATANTE ser onerada por recursos indispensáveis ao pleno funcionamento do objeto que não tenham sido expressamente excluídos da contratação.

6.18.7. Da Implantação da Solução

6.18.7.1. A implantação da solução deverá contemplar todos os serviços técnicos necessários à sua completa disponibilização e entrada em operação, incluindo,

Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



conforme aplicável, planejamento, instalação, configuração, integração, migração, ativação, testes, homologação e demais atividades necessárias ao pleno funcionamento do objeto.

6.18.7.2. A CONTRATADA deverá disponibilizar profissionais tecnicamente capacitados e os recursos necessários para a execução das atividades de implantação, responsabilizando-se integralmente pelo planejamento e pela execução dos serviços sob sua responsabilidade.

6.18.7.3. A implantação deverá ser realizada de forma integrada com a infraestrutura existente da CONTRATANTE, observando os requisitos de compatibilidade, interoperabilidade, segurança e continuidade dos serviços.

6.18.7.4. Quando houver necessidade de migração de configurações, políticas, regras, equipamentos ou demais elementos da infraestrutura existente, a CONTRATADA deverá realizar as atividades necessárias para a transição, de forma planejada e sem prejuízo à continuidade dos serviços.

6.18.7.5. A solução somente será considerada plenamente disponibilizada após a conclusão das atividades de instalação, configuração, integração, ativação, testes e homologação, com as funcionalidades contratadas em condições de operação.

6.18.7.6. Ao término da implantação, a CONTRATADA deverá fornecer à CONTRATANTE as informações e documentações necessárias à operação e administração da solução, incluindo, quando aplicável, manuais, procedimentos operacionais, configurações e demais documentos técnicos pertinentes.

6.18.8. Da Atualização e Manutenção da Solução

6.18.8.1. Durante toda a vigência contratual, a solução deverá permanecer com as licenças, subscrições, atualizações de software, firmware, bases de assinaturas e demais recursos necessários ao pleno funcionamento das funcionalidades contratadas, conforme aplicável a cada solução.

6.18.8.2. As atualizações disponibilizadas pelo fabricante que sejam necessárias à manutenção da segurança, estabilidade, compatibilidade ou funcionamento das funcionalidades contratadas deverão estar contempladas na solução, sem custos adicionais para a CONTRATANTE, observadas as condições de licenciamento e subscrição previstas na contratação.

6.18.8.3. A CONTRATADA deverá realizar ou apoiar tecnicamente a aplicação das atualizações necessárias ao adequado funcionamento da solução, quando demandada pela CONTRATANTE ou quando tecnicamente recomendável.

6.18.9. Da Gestão, Monitoramento e Registros

Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



6.18.9.1. A solução deverá possibilitar a gestão e o monitoramento centralizados dos componentes que a integram, quando tecnicamente aplicável.

6.18.9.2. A solução deverá possibilitar o registro e a consulta dos logs, eventos e alertas relacionados ao funcionamento e à segurança dos componentes contratados.

6.18.9.3. Deverá ser possível realizar o acompanhamento dos eventos de segurança e das ocorrências relevantes da solução, permitindo a identificação de incidentes, falhas, indisponibilidades e demais situações que possam comprometer a infraestrutura protegida.

6.18.9.4. A solução deverá permitir, quando aplicável, a geração de relatórios operacionais e de segurança, contendo informações relevantes sobre eventos, funcionamento, utilização e ocorrências identificadas.

6.18.9.5. As alterações de configuração realizadas nos componentes gerenciados deverão ser registradas em mecanismo de auditoria da própria solução, quando essa funcionalidade estiver disponível.

6.18.10. Dos Recursos Necessários à Operação

6.18.10.1. A CONTRATADA deverá disponibilizar, em regime de comodato, 2 (duas) TVs de, no mínimo, 43 (quarenta e três) polegadas, para utilização pela CONTRATANTE, destinadas à visualização de logs e eventos das soluções ofertadas.

6.18.10.2. Os equipamentos disponibilizados em comodato deverão permanecer em condições adequadas de funcionamento durante a vigência da contratação, cabendo à CONTRATADA sua manutenção ou substituição em caso de defeito que impeça sua utilização.

6.18.10.3. Ao término da contratação, os equipamentos disponibilizados em regime de comodato deverão ser retirados pela CONTRATADA, sem ônus para a CONTRATANTE.

6.18.11. Suporte Técnico

6.18.11.1. Toda a solução deverá ser fornecida contemplando suporte técnico do fabricante, em regime 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana – 24x7, durante todo o período de vigência da contratação.

6.18.11.2. Deverá ser contemplado e declarado na proposta o serviço de suporte técnico do fabricante, observando, no mínimo, os seguintes níveis de serviço (SLA):

6.18.11.2.1. Tempo de resposta para o atendimento inicial, em casos emergenciais que impliquem indisponibilidade dos serviços, de até 15 (quinze) minutos;

6.18.11.2.2. Tempo de resposta para o atendimento inicial, em casos de criticidade



alta, caracterizados por situações de perda de funcionalidades ou instabilidades, de até 15 (quinze) minutos;

6.18.11.2.3. Tempo para atualização das requisições, em casos emergenciais que impliquem indisponibilidade dos serviços, de até 3 (três) horas;

6.18.11.2.4. Tempo para atualização das requisições, em casos de criticidade alta, de até 2 (duas) vezes por dia;

6.18.11.2.5. Tempo para provimento de solução de contorno, em casos emergenciais que impliquem indisponibilidade dos serviços, de até 4 (quatro) horas;

6.18.11.2.6. Tempo para provimento de solução de contorno, em casos de criticidade alta, de até 24 (vinte e quatro) horas;

6.18.11.2.7. Deverão ser fornecidas, em regime de comodato, 2 (duas) TVs de, no mínimo, 43 (quarenta e três) polegadas, para utilização pela CONTRATANTE, destinadas à visualização de logs e eventos das soluções ofertadas.

7. CONTROLE E FISCALIZAÇÃO DA ATA/CONTRATO

7.1. Nos termos do Art. 117, da Lei nº 14.133/2021, a execução do contrato deverá ser acompanhada e fiscalizada por 1 (um) ou mais fiscais do contrato, representantes da Administração especialmente designados conforme requisitos estabelecidos no art. 7º desta Lei, ou pelos respectivos substitutos, permitida a contratação de terceiros para assisti-los e subsidiá-los com informações pertinentes a essa atribuição.

§ 1º O fiscal do contrato anotarà em registro próprio todas as ocorrências relacionadas à execução do contrato, determinando o que for necessário para a regularização das faltas ou dos defeitos observados.

§ 2º O fiscal do contrato informará a seus superiores, em tempo hábil para a adoção das medidas convenientes, a situação que demandar decisão ou providência que ultrapasse sua competência.

§ 3º O fiscal do contrato será auxiliado pelos órgãos de assessoramento jurídico e de controle interno da Administração, que deverão dirimir dúvidas e subsidiá-lo com informações relevantes para prevenir riscos na execução contratual.

7.2. A gestão e o acompanhamento da execução dos serviços serão realizados pela Secretaria Municipal de Administração e Modernização, por meio dos servidores responsáveis pela fiscalização e gestão do ajuste, competindo-lhes acompanhar a execução, verificar a conformidade dos serviços prestados, realizar os respectivos registros e proceder ao atesto das notas fiscais e/ou documentos necessários ao pagamento.



7.3. A Contratante deverá monitorar constantemente o nível de qualidade dos serviços para evitar problemas, devendo intervir para corrigir ou aplicar sanções quando verificar desconformidades da prestação do serviço com a qualidade exigida.

DO FISCAL DA ATA DE REGISTRO DE PREÇO/ CONTRATO

SECRETARIA	FISCAL DA ATA/ CONTRATO	SUPLENTE
SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO	Fiscal: FABIO DOS SANTOS CRUZ Cargo: COORDENADOR Matrícula: 968-1	Suplente: SAMUEL JESUS DE ALMEIDA Cargo: GESTOR DE PROJETOS Matricula: 13972-1-1

7.4. O Contrato ou instrumento equivalente deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei Federal n.º 14.133/2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

7.5. O Contrato ou instrumento equivalente será acompanhado por um gestor cujas atribuições são relativas aos aspectos administrativos contratuais, como: instruir o processo da contratação com toda a documentação relativa à sua execução e fiscalização, acompanhar a manutenção das condições habilitatórias, conferir a importância a ser paga, notificar sobre as irregularidades encontradas, adotar as medidas preparatórias para aplicação de sanção administrativa, promover a gestão documental etc, conforme estabelecido no Decreto Municipal n.º 359/2023.

7.6. O Contrato ou instrumento equivalente será fiscalizado por um fiscal cujas atribuições são relativas à execução do objeto contratual ou instrumento equivalente, conforme estabelecido no Decreto Municipal n.º 359/2023.

7.7. Após a assinatura do contrato ou instrumento equivalente, poderá ser elaborado o plano de fiscalização que terá como referência o Termo de Referência, Edital e instrumento contratual ou instrumento equivalente e constará as estratégias de execução e fiscalização, conforme estabelecido no Decreto Municipal n.º 359/2023.

7.8. A execução do contrato ou instrumento equivalente deverá ser acompanhada e fiscalizada por meio de instrumentos de controle, que compreendam, quando for o caso, a mensuração dos seguintes aspectos:

a) os resultados alcançados em relação ao contrato ou instrumento equivalente, com a verificação dos prazos de execução e da qualidade demandada;

b) os recursos humanos empregados, em função da quantidade e da formação



profissional exigida, quando se tratar de contrato com dedicação exclusiva de mão de obra;

c) a qualidade e adequação dos recursos materiais, equipamentos, licenças, sistemas e demais recursos empregados na execução dos serviços, quando aplicável;

d) a adequação dos serviços prestados à rotina de execução estabelecida;

e) o cumprimento das demais obrigações decorrentes do contrato ou instrumento equivalente; e

f) a satisfação do público usuário, quando cabível.

7.9. O fiscal do contrato ou instrumento equivalente deverá verificar ainda os impactos sobre o pagamento, nas situações em que a contratada:

I - Não produzir os resultados, deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas;

II - Deixar de utilizar materiais e recursos humanos exigidos para o fornecimento dos produtos ou da execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

7.10. O descumprimento total ou parcial das responsabilidades assumidas pelo fornecedor, sobretudo quanto às obrigações e encargos sociais e trabalhistas, ensejará a aplicação de sanções administrativas, previstas neste Edital e na legislação vigente, podendo culminar em rescisão contratual.

7.11. O recebimento provisório e definitivo dos serviços observará os critérios, procedimentos e prazos estabelecidos no item **6.2. CRITÉRIOS DE RECEBIMENTO PROVISÓRIO E DEFINITIVO DO OBJETO DA CONTRATAÇÃO** e seus subitens **6.2.1. Recebimento Provisório** e **6.2.2. Recebimento Definitivo** deste Termo de Referência, sem prejuízo das atribuições de acompanhamento e fiscalização previstas neste tópico.

7.12. O fiscal deverá anotar em registro próprio todas as ocorrências relacionadas à execução do contrato ou instrumento equivalente, determinando o que for necessário para a regularização das faltas ou dos defeitos observados.

7.13. Os produtos/serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e Edital, devendo ser substituídos de imediato, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

7.14. Os produtos/serviços serão recebidos definitivamente no prazo de 05 (cinco) dias úteis, contados do recebimento provisório, após a verificação da qualidade e



quantidade do material, conferência da autenticidade da Nota Fiscal e suas certidões negativas fiscais e consequente aceitação mediante termo circunstanciado.

7.15. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade do Fornecedor pelos prejuízos resultantes da incorreta execução do contrato.

7.16. A fiscalização de que trata este item não exclui nem reduz a responsabilidade do Fornecedor, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 120 e 140 da Lei Federal n.º 14.133/2021.

7.17. As notificações serão comunicadas preferencialmente por meio de endereço eletrônico do fornecedor, devendo a contratada informar em seus documentos as informações necessárias para tanto, e eventualmente mediante ofício de forma presencial.

8. MEDIÇÃO E PAGAMENTO

8.1. O pagamento das despesas orçamentárias será efetuado conforme prazos e cronograma previstos no art. 7º do Decreto municipal nº 129/2024 e será efetuado mediante a apresentação da(s) respectiva(s) nota(s) fiscais/fatura devidamente acompanhada das certidões demonstrando sua regularidade fiscal e trabalhista, que serão liberadas para pagamento somente quando aferido seu recebimento por meio de fiscal designado.

Art. 7º Os prazos que trata do artigo 06 serão limitados a: [...]

8.2. As notas fiscais não poderão ter rasuras e deverão descrever corretamente o item, e número de empenho, o número do processo de compras, dados bancários para depósito, devendo ainda, destacar e discriminar a retenção a que está sujeita, informando de forma clara e inequívoca todos os impostos e alíquotas incidentes, cabendo a ela toda a responsabilidade pela eventual ausência dessa informação ou pela informação incorreta.

8.3. Os prestadores de serviço e fornecedores de bens deverão observar às regras de retenção dispostas na Instrução Normativa RFB nº 1.234, de 2012.

8.4. Caso a documentação não esteja de acordo com o solicitado, será devolvida para a correção, sendo válida a data de protocolo corrigida, para fins de prazo de pagamento.



8.5. O Recebimento dos equipamentos/ materiais não exclui a responsabilidade da contratada por vícios de qualidade ou disparidade com as especificações técnicas verificadas posteriormente;

8.6. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência (**7. CONTROLE E FISCALIZAÇÃO DA ATA/CONTRATO em seu subitem 7.13.**) e na proposta, devendo ser substituídos *imediatamente*, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

7.13. Os produtos/serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e Edital, devendo ser substituídos de imediato, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

9. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

9.1. A referida licitação trata-se de bens e serviços comuns e será realizado de forma eletrônica no critério por menor preço, de acordo com a Lei nº 14.133/2021, Art. 6. no Inciso XIII, XLI.

9.2. E será realizada preferencialmente sob a forma eletrônica conforme Art. 17 do § 2º da Lei nº 14.133/2021.

9.3. A modalidade de licitação está regida no Art. 28, Inciso I, e trata-se da modalidade de pregão.

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

9.4.1. Habilitação Jurídica:

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

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

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

**Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br**



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

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

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

9.4.1.7. No caso do item **9.4.1.3.**, caso a empresa for identificada como EIRELI em seus atos constitutivos, ela deverá ser considerada como convertida em SLU, automaticamente pelo agente de contratação, devendo os seus atos constitutivos serem considerados regulares como EIRELI, mas a empresa deverá se comportar na contratação como uma SLU.

9.4.1.8. Quaisquer atos constitutivos elencados acima deverão ser apresentados juntamente com a Consulta ao Quadro de Sócios e Administradores – QSA;

9.4.1.9. Tratando-se de procurador, apresentar procuração por instrumento público ou particular, que comprove os poderes do mandante para a outorga, com firma reconhecida, da qual constem poderes específicos para formular lances, negociar preço, interpor recursos, desistir de sua interposição e praticar todos os demais atos pertinentes ao certame.

9.4.2. Regularidade fiscal, social e trabalhista:

9.4.2.1. Inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ);

9.4.2.2. Inscrição no cadastro de contribuintes estadual ou municipal, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

9.4.2.3. Regularidade perante a Fazenda Federal (incluindo Seguridade Social), Estadual e Municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da lei;

9.4.2.4. Regularidade relativa ao Fundo de Garantia por Tempo de Serviço (FGTS), que demonstre cumprimento dos encargos sociais instituídos por lei;



9.4.2.5. Regularidade perante a Justiça do Trabalho, mediante a apresentação de Certidão Negativa de Débitos Trabalhistas (CNDT);

9.4.2.6. Cumprimento do disposto no art. 7º, XXXIII, da Constituição Federal, declarando que não emprega menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 (dezesesseis) anos em qualquer trabalho, salvo na condição de aprendiz, a partir dos 14 (quatorze) anos, conforme Modelo de Declaração do Anexo VIII.

9.4.3. Qualificação Econômico-Financeira:

9.4.3.1. Balanço patrimonial, demonstrativo de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, exigidos na forma da lei:

a) O atendimento dos índices econômicos deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor, comprovando: Índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), maiores ou iguais a um ($\geq 1,0$), resultantes da aplicação das seguintes fórmulas:

$$\text{Liquidez Geral (LG)} = \frac{\text{Ativo Circulante} + \text{Realizável a Longo Prazo}}{\text{Passivo Circulante} + \text{Exigível a Longo Prazo}}$$

$$\text{Solvência Geral (SG)} = \frac{\text{Ativo Total}}{\text{Passivo Circulante} + \text{Exigível a Longo Prazo}}$$

$$\text{Liquidez Corrente (LC)} = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

b) Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação capital mínimo de 1,0% (um por cento) do valor total estimado para o item da contratação. (Lei nº 14.133, de 2021, art. 69, §4º).

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

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



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

f) O Balanço Patrimonial físico na forma da lei deve conter os seguintes elementos:

- Balanço Patrimonial;
- Demonstração de Resultado do Exercício;
- Assinado pelo contador e representante legal da empresa;
- Termo de Abertura e Termo de Encerramento do Livro Diário;
- Registrado na Junta Comercial, no Cartório De Registros De Pessoa

Jurídica ou OAB.

g). O Balanço Patrimonial digital na forma da lei deve conter os seguintes elementos:

- Balanço Patrimonial;
- Demonstração de Resultado do Exercício;
- Assinado digitalmente pelo contador e representante legal da empresa;
- Termo de Abertura e Termo de Encerramento do Livro Diário;
- Recibo emitido pelo sistema público.

9.4.3.2. Certidão negativa de feitos sobre falência expedida pelo distribuidor da sede do licitante.

9.4.3.3. A iniciativa de exigir qualificação econômico-financeira, sobretudo, no caso concreto, que se trata de entregas futuras, embasa-se, outrossim, no artigo 69 da Lei 14.133/2021, que no seu caput já descreve:

A habilitação econômico-financeira visa demonstrar a aptidão econômica do licitante para cumprir as obrigações decorrentes do futuro contrato, devendo ser comprovada de forma objetiva, por coeficientes e índices econômicos previstos no edital.

Justifica-se, portanto a exigência de qualificação econômico-financeira, considerando que o intuito é que seja demonstrada a saúde financeira, ou seja, que a empresa se mostre apta que possui disponibilidade de recursos para executar o objeto contratado com base na necessidade concreta do produto contratado e o seu valor estimado para a contratação.

9.5. TRATAMENTO DIFERENCIADO PARA MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE.



9.5.1. Nos termos da Lei Municipal nº 3.503/2025, que regulamenta, no âmbito do Município de Sinop-MT, o tratamento favorecido, diferenciado e simplificado previsto nos arts. 42 a 49 da Lei Complementar Federal nº 123/2006, com as alterações da LC nº 147/2014, este processo licitatório adotará, sempre que tecnicamente viável e vantajoso à Administração Pública, as medidas que promovam o desenvolvimento econômico local e regional, ampliem a eficiência das políticas públicas e incentivem a competitividade e a inovação.

9.5.2. Para os fins da aplicação das preferências legais, observa-se que:

- Será considerada empresa local aquela com sede ou filial efetivamente estabelecida no Município de Sinop-MT;
- Será considerada empresa regional: a pessoa jurídica de direito privado estabelecida em qualquer cidade localizada na Microrregião do Alto Teles Pires, a qual compreende, nos termos da Lei Municipal nº 3.503/2025, os seguintes municípios: Cláudia, Feliz Natal, Ipiranga do Norte, Itanhangá, Lucas do Rio Verde, Nova Mutum, Nova Ubiratã, Santa Carmem, Sinop, Sorriso, Tapurah, União do Sul, Santa Rita do Trivelato e São José do Rio Claro.

9.5.3. As empresas licitantes interessadas em usufruir do tratamento diferenciado deverão apresentar declaração expressa de enquadramento como Microempresa (ME) ou Empresa de Pequeno Porte (EPP), sob as penas da lei, bem como comprovação de sua condição mediante consulta à Receita Federal quanto à opção pelo Simples Nacional. O fornecimento de informações falsas ensejará responsabilização nas esferas administrativa, civil e penal, conforme legislação vigente.

9.5.4. Diante da análise técnica da natureza do objeto deste Termo de Referência, verificou-se a viabilidade e vantajosidade da aplicação dos dispositivos legais referentes ao tratamento diferenciado, sendo adotadas as seguintes medidas conforme Lei Municipal nº 3.503/2025:

- I. Nos critérios de julgamento, aplicar-se-á desempate em favor de ME/EPP, conforme previsto nos arts. 5º e 6º, respeitando os limites legais de 10% (regra geral) ou 5% (no pregão);
- II. Haverá preferência de contratação para empresas sediadas em Sinop-MT e, subsidiariamente, na microrregião Alto do Teles Pires (arts. 2º e 7º);

9.6. JUSTIFICATIVA PARA A EXIGÊNCIA DO BALANÇO PATRIMONIAL: As contratações relativas a obras, serviços de engenharia e serviços contínuos possuem natureza complexa, execução diferida no tempo e demandam mobilização constante de estrutura operacional, recursos humanos e investimentos financeiros por parte da
Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



contratada. Nessas hipóteses, a análise da qualificação econômico-financeira revela-se medida indispensável para mitigar o risco de descontinuidade contratual, paralisação de serviços essenciais ou inadimplemento de obrigações trabalhistas e operacionais que trariam graves prejuízos ao interesse público.

Dessa forma, em observância ao disposto no art. 69, I, da Lei Federal nº 14.133/2021, justifica-se motivadamente a exigência da apresentação do balanço patrimonial, da demonstração do resultado do exercício (DRE) e demais demonstrações contábeis dos últimos dois exercícios sociais.

Art. 69. A habilitação econômico-financeira visa a demonstrar a aptidão econômica do licitante para cumprir as obrigações decorrentes do futuro contrato, devendo ser comprovada de forma objetiva, por coeficientes e índices econômicos previstos no edital, devidamente justificados no processo licitatório, e será restrita à apresentação da seguinte documentação:

I - balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais;

A exigência encontra amparo na necessidade objetiva de comprovar a higidez e a saúde financeira da licitante, inclusive mediante coeficientes e índices econômicos devidamente fundamentados neste instrumento contratual, assegurando que a empresa dispõe de capital e liquidez suficientes para suportar os custos e a escala de execução do futuro contrato.

9.7. COM RELAÇÃO À POSSIBILIDADE DE OFERTAR PROPOSTA EM QUANTITATIVOS INFERIORES

9.7.1. No presente certame não é possível o licitante oferecer proposta de preços em quantitativo inferior ao máximo previsto no Termo de Referência, obrigando-se aos limites lá informados, bem como não poderá apresentar proposta de preços com descrição do item diferente da registrada no Termo de Referência, seja com descrição com menos ou mais informações do que lá estabelecidas.

9.8. COM RELAÇÃO À POSSIBILIDADE DE PREVER PREÇOS DIFERENTES

9.8.1. Em consonância com os princípios da eficiência, da economicidade e da padronização administrativa, esta Administração opta pela não aplicação da faculdade de prever preços diferentes prevista no art. 82, III, da Lei Federal nº 14.133/2021 e no art. 471, VIII, do Decreto Municipal 359/2023.

10. CUSTO ESTIMADO DA CONTRATAÇÃO/PREÇO DE REFERÊNCIA



10.1. Metodologia Aplicável para a Estimativa de Preços ou Preço de Referência: A estimativa de preços da presente contratação foi elaborada mediante pesquisa de mercado, observando os critérios estabelecidos na legislação aplicável às contratações públicas, com o objetivo de identificar valores compatíveis com a realidade do mercado e assegurar a obtenção da proposta mais vantajosa para a Administração.

Para a composição da estimativa, foram utilizadas múltiplas fontes de pesquisa, dentre elas: orçamentos obtidos junto a fornecedores especializados, abrangendo empresas locais, regionais e de atuação nacional; consultas ao Banco de Preços e demais plataformas especializadas de pesquisa de contratações públicas; Atas de Registro de Preços e contratos firmados por outros órgãos e entidades da Administração Pública; pesquisas em sítios eletrônicos especializados, quando admitidas pela legislação e compatíveis com o objeto da contratação.

Como parte da fase de planejamento, foram promovidas reuniões técnicas e mantido contato com fornecedores especializados, tanto para esclarecer aspectos relacionados ao objeto da futura contratação quanto para estimular a participação no certame, possibilitando maior conhecimento das soluções disponíveis no mercado e contribuindo para a elaboração de especificações compatíveis com a realidade tecnológica atualmente existente.

Após a consolidação das informações obtidas, será adotada a mediana dos preços considerados válidos e compatíveis com o objeto da contratação, a qual servirá como base para definição do valor estimado da contratação e do preço de referência a ser utilizado no procedimento licitatório.

Ressalta-se que a utilização de múltiplas fontes de pesquisa busca mitigar distorções decorrentes da adoção de uma única referência de mercado, proporcionando maior confiabilidade à estimativa de preços e refletindo de forma mais fidedigna os valores atualmente praticados para soluções de segurança da informação.

10.2. Valor Estimado para a Contratação:

O valor estimado da contratação será apurado após a conclusão da pesquisa de preços, mediante a consolidação das informações obtidas nas fontes de pesquisa definidas neste Estudo Técnico Preliminar, observada a metodologia descrita no item anterior.

Concluída a pesquisa de mercado, o valor estimado para a contratação corresponderá a R\$ 3.168.167,64 (três milhões cento e sessenta e oito mil cento e sessenta e sete reais e sessenta e quatro centavos), montante que servirá como referência para a elaboração do Termo de Referência e para a condução do

**Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br**



procedimento licitatório, observados os critérios de vantajosidade, economicidade e compatibilidade com os preços praticados no mercado.

O valor estimado contempla todos os custos necessários à execução integral do objeto, incluindo, quando aplicáveis, tributos, impostos, taxas, contribuições, encargos trabalhistas, previdenciários, fiscais e comerciais, transporte, frete, seguro, deslocamentos, mão de obra especializada, equipamentos, licenças, subscrições, materiais, acessórios, instalação, configuração, implantação, integração, manutenção, suporte técnico, atualizações, treinamento e demais despesas diretas e indiretas necessárias ao pleno funcionamento da solução e ao cumprimento das obrigações previstas na contratação, não cabendo à Administração o pagamento de valores adicionais decorrentes de custos que sejam de responsabilidade da contratada.

11. DOTAÇÃO ORÇAMENTÁRIA

11.1. Em regra, o Registro de Preços não gera compromisso efetivo de aquisição. Após declarado o vencedor, os preços são registrados e as necessidades posteriores de aquisição do órgão público serão adquiridas com o vencedor, respeitando o preço registrado.

11.2. Por se tratar de um procedimento auxiliar de Sistema de Registro de Preços, previsto na Lei 14.133/2021 no artigo 78, e que, conforme art. 17 do Decreto 11462 de 31 de março de 2023 *“a indicação da Declaração de disponibilidade de saldo (impacto financeiro) e Anexo VIII - Geração de despesas de caráter continuado somente será exigida para a formalização do contrato ou de outro instrumento hábil”*, portanto não sendo obrigatória a disponibilidade financeira no ato do registro, constam apenas as numerações orçamentárias das secretarias participantes, conforme segue: **SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO E MODERNIZAÇÃO DE SINOP-MT.**

DOTAÇÃO	RECURSO
2026.339040.0000.150000000000	REC.PRÓPRIO

11. DEMAIS INFORMAÇÕES ESPECÍFICAS DO TERMO DE REFERÊNCIA

11.1. (Não se aplica).

11.2. Não se identificam, para a presente contratação, outras informações específicas adicionais às já estabelecidas neste Termo de Referência, além
Av. das Embaúbas, nº 1386, Setor Comercial, Sinop-MT, CEP 78550-206, Caixa Postal 500;
Telefone(s): (66) 3520-7298;
E-mail: licitacao@sinop.mt.gov.br



daquelas necessárias à adequada caracterização, execução, fiscalização e recebimento dos serviços.

Sinop-MT, 31 de Agosto de 2026.

Gabriel Araújo

Matrícula: 18702-1

Responsável pela elaboração do Termo
de Referência
Portaria 571/2026

Daniel Jose Sepi de Lima

Matrícula 7230

Analista de Sistema

CIÊNCIA DA AUTORIDADE COMPETENTE

(X) Concordo com o Termo de Referência realizado e autorizo a contratação nos termos da Lei 14.133/2021.

Sinop-MT, 31 de Agosto de 2026.

Elizabete Cilião Guilherme

Portaria nº 1195/2025

Secretário Municipal de Administração e Modernização
Sinop/MT