De: Andressa C. - SMEAE - Compras

Para: Envolvidos internos acompanhando

Data: 26/05/2025 às 11:59:59

Prezados,

Segue conforme solicitado.

_

Atenciosamente,

Andressa Nair
Gerência de Compras

Anexos:

Minuta_edital_firewall_2_.docx

De: Andressa C. - SMEAE - Compras

Para: Envolvidos internos acompanhando

Data: 26/05/2025 às 15:27:52

Prezados,

Segue.

_

Atenciosamente,

Andressa Nair
Gerência de Compras

Anexos:

Minuta_edital_firewall_2_.docx
TR_FIREWALL_2025_FINAL_ALTERADO_2_.docx
TR_FIREWALL_2025_FINAL_ALTERADO_2_.pdf

Assinado digitalmente (anexos) por:

Assinante	Data	Assinatura	
Jeremias Pereira Leite	27/05/2025 10:48:58	ICP-Brasil	JEREMIAS PEREIRA LEITE CPF 045.XXX.XXX-72

Para verificar as assinaturas, acesse **https://caceres.1doc.com.br/verificacao/** e informe o código: **37F7-8C4F-BD72-1A02**

TERMO DE REFERÊNCIA 01/2025

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Registro de Preço para futura e eventual contratação de empresa especializada para prestação de serviços de segurança cibernética com Inteligência Artificial Preditiva, garantindo alta disponibilidade, segurança, eficiência e sustentabilidade no atendimento às demandas do Município de Cáceres, conforme condições e exigências estabelecidas neste instrumento.

1.1.1. O serviço a ser prestado engloba, fornecimento em regime de comodato, instalação e configuração de Next Generation Firewall (NGFW) e SD-WAN, redundância composta por links primário e secundário de ASN e rotas diferentes, manutenção contínua, suporte técnico, software de gerenciamento, conectividade segura para unidades externas e praças públicas, capacitação certificada da equipe e atendimento técnico especializado.

LOTE	ITEM	CÓDIGO TCE-MT	CÓDIGO CAT MAT	ESPECIFICAÇÃO	UNIDADE	QUANTIDADE	QUANTIDADE ANUAL
1 (ÚNICO)	1	257560-4	609340	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)	Serviço	173	2076
	2	152969	481647	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	Serviço	2	24
	3	00065206	26174	Serviço de Link dedicado de Acesso à internet, bloco /29 e Banda Mínima de Acesso Garantida de 500Mbps (Alta Disponibilidade) SEDE (Link de ASN e Rota Diferentes)	Serviço	2	24
	4	152970	26484	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 150Mbps Sites Remotos (Fibra Óptica)	Serviço	171	2052
	5	152972	26557	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G)	Serviço	171	2052
	6	339905-2	1988	Implantação da Solução	Serviço	1	1
	7	404876-8	16837	Capacitação especializada da equipe com emissão de certificação.	Treinamento	1	1
	8	332679-9	27340	Consultoria Política de Segurança	Serviço	1	1

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

1.2. As empresas interessadas deverão apresentar proposta para o **lote único** do certame, tendo em vista a natureza integrada da solução e a necessidade de contratação global sob responsabilidade de um único fornecedor.

1.3. A análise da documentação terá por finalidade verificar a habilitação da empresa, bem como sua capacidade de operar um projeto dessa complexidade.

1.3.1. Caso as exigências não sejam atendidas, será convocada a empresa subsequente que tenha apresentado o preço global imediatamente superior, observadas as regras de negociação.

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

1.5. O prazo de vigência da contratação será de 12 (doze) meses, contados a partir da assinatura do contrato, podendo ser prorrogado por períodos iguais e consecutivos, desde que, durante o planejamento e toda a execução do contrato, sejam observadas as seguintes condições:

a) seja emitido ateste da autoridade competente do órgão ou entidade contratante, confirmando que a contratação representa a alternativa mais vantajosa do ponto de vista econômico, em razão de sua natureza plurianual;

b) haja previsão e disponibilidade de créditos orçamentários vinculados à contratação e justificativa quanto à conveniência de sua manutenção; e

c) a Administração possa rescindir o contrato, sem ônus, caso não disponha dos recursos orçamentários necessários à sua continuidade ou caso entenda que a contratação deixou de atender ao interesse público.

Esse prazo poderá se estender até o limite de 15 (quinze) anos, conforme estabelecido no artigo 114 da Lei nº 14.133/2021, diante da natureza continuada da operação e da sua caracterização como sistema estruturante de tecnologia da informação, conforme demonstrado no Estudo Técnico Preliminar.

1.6. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico do Estudo Técnico Preliminar, apêndice deste Termo de Referência.

3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

3.1. A Fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada em tópico específico do Estudo Técnico Preliminar, apêndice deste Termo de Referência.

3.2. O objeto da contratação está previsto no Plano de Contratações Anual [2025], conforme detalhamento a seguir:

I) ID PCA no PNCP: 03214145000183-0-000001/2025;

II) Data de publicação no PNCP: 28/01/2025;

III) Id do item no PCA: 166;

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

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

4.1. A solução tem por objetivo proporcionar uma infraestrutura robusta, segura e eficiente para o ambiente de tecnologia da informação da Prefeitura Municipal de Cáceres, assegurando a continuidade dos serviços públicos e a proteção dos dados institucionais. O ciclo de vida da solução contempla todas as fases essenciais, desde a implantação até a operação contínua, manutenção e eventuais atualizações tecnológicas, garantindo um alto padrão de qualidade e desempenho ao longo da vigência do contrato.

4.2. A solução contempla segurança cibernética avançada, conectividade de alto desempenho e suporte especializado, alinhando-se às melhores práticas de governança digital e proteção de ativos públicos.

4.3. A implantação e execução do contrato seguem um modelo estruturado em duas fases principais:

4.3.1. **Fase de Implantação**, com prazo de até 60 dias após a assinatura do contrato, abrangendo a instalação dos equipamentos, ativação dos links, integração das unidades externas e capacitação da equipe técnica.

4.3.2. **Fase de Prestação de Serviço Mensal**, com duração de até 180 meses, garantindo manutenção contínua, suporte técnico especializado, atualizações tecnológicas e otimização da infraestrutura de segurança e comunicação de dados.

4.4. O ciclo de vida da solução envolve etapas bem definidas, assegurando que a infraestrutura implementada esteja sempre atualizada e alinhada com as necessidades da Prefeitura.

4.4.1. **Planejamento e Implantação**

4.4.1.1. Na fase inicial, serão executadas as atividades necessárias para a estruturação da solução contratada, garantindo que todos os componentes sejam devidamente configurados e operacionalizados. Essa etapa inclui:

4.4.1.1.1. Instalação e configuração dos equipamentos de segurança cibernética, incluindo Next Generation Firewall (NGFW) e SD-WAN, visando a proteção contra ameaças digitais e a otimização do tráfego de rede.

4.4.1.1.2. Implementação de serviços de segurança cibernética baseados em Inteligência Artificial Preditiva, permitindo a detecção e resposta antecipada a incidentes.

4.4.1.1.3. Ativação dos links dedicados de internet, garantindo 500 Mbps na sede, 150 Mbps nos sites remotos e 35 Mbps como link de contingência, assegurando conectividade estável para as operações administrativas e serviços públicos digitais.

4.4.1.1.4. Integração das unidades externas e praças públicas à infraestrutura de rede segura, possibilitando um acesso seguro e confiável aos sistemas municipais.

4.4.1.1.5. Capacitação certificada da equipe técnica da Prefeitura, garantindo a qualificação necessária para a gestão e monitoramento da solução implementada.

4.4.2. **Operação e Manutenção**

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.4.2.1. Após a implantação, a solução entrará em operação contínua, garantindo que os serviços contratados sejam entregues de forma eficiente e dentro dos padrões de qualidade exigidos. Esta fase inclui:

4.4.2.1.1. Monitoramento contínuo da infraestrutura, com análises preditivas para detecção de ameaças e otimização do desempenho dos sistemas.

4.4.2.1.2. Suporte técnico especializado, disponível para resolver quaisquer incidentes ou necessidades de ajustes na configuração da solução.

4.4.2.1.3. Gestão e atualização dos equipamentos e software, garantindo que os firewalls, SD-WAN e demais componentes tecnológicos operem sempre com as versões mais recentes e seguras.

4.4.2.1.4. Consultoria contínua para aprimoramento da política de segurança da informação, com foco na proteção de dados, conformidade regulatória e mitigação de riscos cibernéticos.

4.4.2.1.5. Garantia de alta disponibilidade, com suporte a redundância de links e contingência operacional para evitar interrupções nos serviços municipais.

4.4.3. **Evolução e Sustentabilidade da Solução**

4.4.3.1. Ao longo do ciclo de vida da solução, serão adotadas práticas que garantam sua evolução tecnológica e sustentabilidade, permitindo que o investimento realizado permaneça eficiente e alinhado às necessidades do município. Entre essas práticas, destacam-se:

4.4.3.1.1. Adoção de tecnologias emergentes para otimizar a performance e segurança da infraestrutura de TIC.

4.4.3.1.2. Revisão periódica da estratégia de segurança cibernética, considerando as tendências de ameaças digitais e as melhores práticas do setor.

4.4.3.1.3. Expansão escalável da solução, permitindo a incorporação de novas unidades e serviços de forma ágil e estruturada.

4.4.3.1.4. Otimização do consumo de recursos tecnológicos, garantindo um uso eficiente da infraestrutura contratada e contribuindo para a sustentabilidade financeira e operacional do município.

4.5. Especificação do Produto

4.5.1. Funcionamento Geral da Solução

4.5.1.1. A contratação deverá englobar além das soluções de defesa cibernética a prestação de serviços de rede de longa distância (WAN) para manter a interligação da Sede da Prefeitura de Cáceres aos Sites Remotos, localizados no interior do Município e fora dele.

4.5.1.2. A contratação também inclui a prestação de serviço de acesso à internet nos Sites Remotos e na sede da Prefeitura Municipal de Cáceres MT.

4.5.1.3. A contratação deverá englobar o fornecimento de um conjunto de equipamentos de redes, incluindo recursos de IP para trabalhar em alta disponibilidade na Sede e cada equipamento deverá permitir no mínimo 4(quatro) conexões à Internet.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.1.4. A nova solução de comunicação de dados entre os Sites Remotos e a Sede utilizará equipamentos com a tecnologia SD-WAN com o objetivo de balancear o tráfego de forma inteligente para otimizar o uso da rede. Para que o tráfego corporativo seja protegido quando trafegar pela internet, serão configurados túneis VPN IPSEC entre os equipamentos SD-WAN da Sede da Prefeitura e dos Sites Remotos.

4.5.1.5. Os equipamentos SD-WAN da Sede deverão trabalhar em alta disponibilidade.

4.5.1.6. A relação dos Sites Remotos e da Central nos quais os serviços serão prestados encontra-se descrita no item 7.2.1.3 deste Termo de Referência.

4.5.1.7. Em situações normais, os tráfegos de sistemas da prefeitura sobretudo os administrativos, além do tráfego de telefonia IP, devem ser encaminhados pela via IPSEC pelo melhor link. Por outro lado, os serviços de videoconferência das Plataformas Zoom, Google, Webex e Microsoft Teams devem ser acessados diretamente sem a necessidade de utilização deste túnel, além da navegação de Internet das redes dos assessores, colaboradores e cidadãos que acessam a rede social da Prefeitura.

4.5.1.8. Em situações de falha ou de uso intenso da rede, alternativamente os tráfegos corporativos devem ser encaminhados entre os Sites Central e remotos utilizando também túnel VPN IPSEC pelo link secundário estabelecidos pela Internet. Os túneis VPN devem utilizar a topologia hub-and-spoke, com centralização nos equipamentos SD-WAN na Sede.

4.5.1.9. Em situações de falha de um dos links de Internet dos Sites remotos, o tráfego deve ser encaminhado pela conexão de internet secundária até o Site Central da Prefeitura.

4.5.1.10. A configuração do encaminhamento do tráfego e da contingência em casos de falha deve ser feita utilizando tecnologia SD-WAN em que o encaminhamento de tráfego é feito com base no perfil de tráfego em vez da utilização de rotas.

4.5.1.11. A prestação dos serviços descritos em cada ITEM deverá ser considerada como entregue, a partir da assinatura do Termo de Recebimento Definitivo.

4.5.1.12. A prestação dos serviços será baseada no modelo de remuneração em função dos resultados apresentados, em que os pagamentos serão feitos após mensuração e verificação de métricas quantitativas e qualitativas, contendo indicadores de desempenho e metas, com Instrumento de Medição de Resultado (IMR) definido em contrato, de modo a resguardar a eficiência e a qualidade na prestação dos serviços.

4.5.1.13. Os serviços a serem prestados incluem, ainda, a elaboração prévia de um Projeto Executivo de rede, a ser analisado pela equipe técnica da Prefeitura para aprovação, conforme especificações incluídas neste documento. Esse documento deverá conter, no mínimo:

a) Definição de topologias físicas e lógicas;
b) Plano de Endereçamento;
c) Plano de balanceamento do tráfego;
d) Parâmetros de qualidade de serviço;

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

e) Dimensionamento de enlaces e interfaces de comunicação;

f) Documentação dos últimos 1000 metros de passagem das fibras ópticas.

4.5.1.14. Não haverá aquisição de equipamentos, incluindo roteadores, modens, appliances SD- WAN e demais ativos de rede. Contudo, deverão ser fornecidos equipamentos juntamente com a prestação dos serviços de tecnologia da informação e comunicações como parte integrante da solução contratada.

4.5.1.15. O CONTRATANTE poderá solicitar a desativação do serviço prestado a qualquer sítio, bem como mudança de local de prestação dos serviços. Entende-se por mudanças de local de prestação dos serviços a mudança de endereços de instalação dos equipamentos e acessos dentro da cidade.

4.5.1.16. Após a conclusão da etapa de instalação dos serviços, a CONTRATADA deverá apresentar documentação técnica da solução (As Built), contendo: topologia física e lógica da rede, descrição de equipamentos e circuitos de comunicação de dados, descrição dos níveis mínimos de serviços contratados, dados para acesso ao portal de monitoramento dos serviços e dados para abertura de chamados de suporte técnico.

4.5.1.17. A CONTRATADA deverá também realizar repasse de conhecimento na modalidade presencial para a equipe técnica do CONTRATANTE sobre a solução implantada, conforme descrito no item 5.2 deste Termo de Referência.

4.5.2. **Topologia Da Solução**

4.5.2.1. A solução foi estruturada com base nas necessidades específicas da Prefeitura Municipal de Cáceres, visando garantir conectividade segura, eficiente e de alta disponibilidade para todas as unidades envolvidas. A infraestrutura foi projetada para suportar um volume significativo de acessos simultâneos, assegurando a qualidade da comunicação de dados, a integridade das informações e a segurança cibernética dos sistemas institucionais.

4.5.2.1.1. Estruturação dos Sites e Capacidade dos Links

4.5.2.1.1.1. A topologia da solução foi desenhada considerando a divisão dos Sites Remotos e do Site Central em dois tipos distintos de tecnologia e capacidade de conexão, com base na demanda estimada de usuários simultâneos e nos requisitos operacionais de cada localidade.

4.5.2.1.1.1.1. **Sites Remotos:** A estrutura contempla unidades como Postos de Saúde, Centros de Saúde e espaços públicos, onde os serviços de tecnologia da informação serão utilizados para fins administrativos e sociais. A demanda estimada para os Postos de Saúde varia entre 7 e 10 usuários simultâneos, enquanto os Centros de Saúde podem atender de 15 a 30 usuários simultaneamente. O tráfego nesses locais incluirá tanto o acesso aos sistemas institucionais da Prefeitura

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

quanto a utilização de serviços públicos digitais pelos cidadãos.

4.5.2.1.1.1.2. **Site Central:** A Sede da Prefeitura concentra entre 400 e 500 usuários simultâneos, entre servidores e colaboradores, acessando tanto recursos internos quanto externos. Devido ao alto volume de tráfego e à criticidade dos serviços processados, a conexão do Site Central conta com dois links dedicados de alta capacidade (500 Mbps cada), providos por ASN distintos e rotas diferentes, garantindo redundância e continuidade operacional.

4.5.2.1.1.2. A configuração dos links de internet e a implementação da tecnologia SD-WAN asseguram balanceamento inteligente do tráfego, priorização de pacotes críticos e segurança reforçada para as comunicações entre as unidades.

4.5.2.1.2. **Topologia Lógica da Solução**

4.5.2.1.2.1. A topologia lógica da solução foi elaborada para representar a interconexão dos elementos envolvidos e demonstrar o produto final desta contratação. A arquitetura contempla os seguintes componentes essenciais:

4.5.2.1.2.1.1. Next Generation Firewalls (NGFW) instalados no Site Central, atuando como pontos de controle de segurança cibernética, prevenindo ataques e garantindo a integridade dos dados trafegados entre as unidades.

4.5.2.1.2.1.2. Solução de segurança cibernética com utilização de Inteligência Preditiva.

4.5.2.1.2.1.3. Dispositivos SD-WAN implementados na Sede e nos Sites Remotos, possibilitando gerenciamento eficiente do tráfego, redundância e otimização dos links de comunicação.

4.5.2.1.2.1.4. VPN IPSEC configurada em topologia hub-and-spoke, assegurando segurança na troca de informações entre os Sites Remotos e o Site Central.

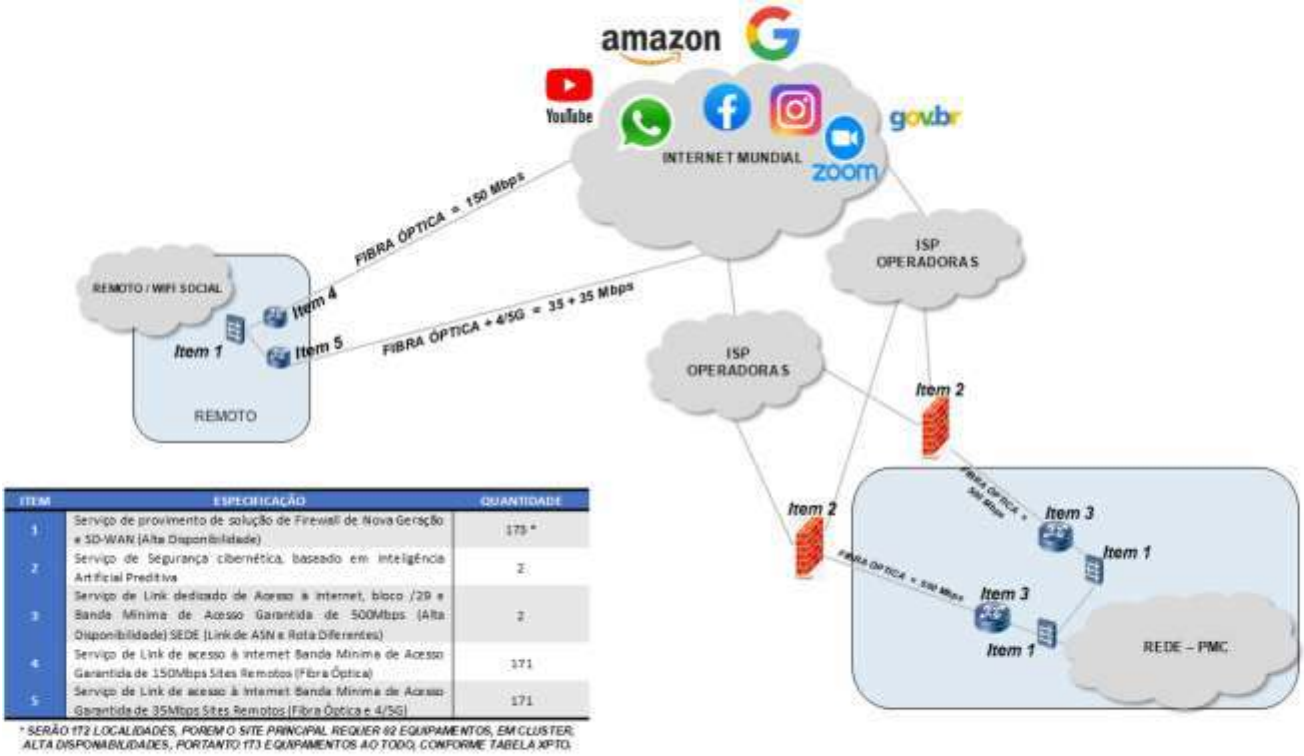
4.5.2.1.2.1.5. Monitoramento centralizado, por meio de um software de gestão e segurança, permitindo a visualização em tempo real do tráfego da rede, detecção de anomalias e gerenciamento proativo de incidentes.

4.5.2.1.2.1.6. Consultoria especializada e capacitação da equipe técnica da Prefeitura, garantindo conhecimento sobre a administração

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

da solução e autonomia na gestão da infraestrutura implantada.

4.5.2.1.2.2. Foi elaborada uma topologia lógica da solução demonstrando o produto final desta contratação:



ITEM	ESPECIFICAÇÃO	QUANTIDADE
1	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)	173 *
2	Serviço de Segurança cibernética, baseado em inteligência Artificial Preditiva	2
3	Serviço de Link dedicado de Acesso à internet, bloco /29 e Banda Mínima de Acesso Garantida de 500Mbps (Alta Disponibilidade) SEDE (Link de ASN e Rota Diferentes)	2
4	Serviço de Link de acesso à internet Banda Mínima de Acesso Garantida de 150Mbps Sites Remotos (Fibra Óptica)	171
5	Serviço de Link de acesso à internet Banda Mínima de Acesso Garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G)	171

* SERÃO 172 LOCALIDADES, POREM O SITE PRINCIPAL REQUER 02 EQUIPAMENTOS, EM CLUSTER, ALTA DISPONIBILIDADES, PORTANTO 173 EQUIPAMENTOS AO TODO, CONFORME TABELA XPTO.

4.5.3. **Equipamentos e Funcionalidades Chave**

4.5.3.1. **Os equipamentos do ITEM 1, do Lote Único, deverão ser entregues no formato e características técnicas bem como funcionalidades conforme especificações abaixo:**

4.5.3.1.1. **Appliance NGFW de 5 Gbps de Capacidade de Firewall**

4.5.3.1.1.1. **Características do Hardware**

4.5.3.1.1.1.1. O equipamento deve se instalar em mesa ocupando no máximo 1U (44,45mm) da referida mesa;

4.5.3.1.1.1.2. Dispor de fonte de alimentação com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;

4.5.3.1.1.1.3. Deverão ser fornecidos todos os cabos de energia, serial (RS-232/RJ45), para instalação e funcionamento do dispositivo;

4.5.3.1.1.1.4. Possuir led indicador on/off, disco e devices de rede;

4.5.3.1.1.1.5. Possuir throughput mínimo de 5 Gbps para tráfego UDP;

4.5.3.1.1.1.6. Suportar no mínimo 4.000.000 (quatro milhões) conexões simultâneas;

4.5.3.1.1.1.7. Suportar no mínimo 37.000 (trinta e sete mil) novas conexões por segundo;

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.1.1.1.8. Possuir throughput mínimo de 300 Mbps para tráfego IPS/IDS;

4.5.3.1.1.1.9. Possuir throughput mínimo de 280 Mbps para tráfego VPN IPSEC com criptografia (AES-256);

4.5.3.1.1.1.10. Possuir throughput mínimo de 140 Mbps para tráfego VPN SSL com criptografia (AES-256);

4.5.3.1.1.1.11. Possuir throughput mínimo de 150 Mbps para SSL Inspection;

4.5.3.1.1.1.12. Possuir throughput mínimo de 200 Mbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

4.5.3.1.1.1.13. Possuir no mínimo 4 (quatro) interfaces de rede Gigabit Ethernet 10/100/1000/2500 Mbps com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

4.5.3.1.1.1.14. Possuir dispositivo de armazenamento interno de no mínimo 64 GB padrão SSD e deve suportar expansão futura para, no mínimo, 120 GB;

4.5.3.1.1.1.15. Possuir no mínimo 1 (uma) porta console de conexão para acesso a interface de comando CLI específica para esta finalidade, utilizando cabo do tipo serial RS-232 ou RJ-45;

4.5.3.1.1.1.16. Possuir pelo menos 1 (uma) portas USB para conexão de dispositivos externos;

4.5.3.1.1.1.17. Deve possuir modem interno 3G/4G/LTE para conexão de link de Internet. O modulo deverá estar incluso no valor do equipamento;

4.5.3.1.2. **Appliance NGFW de 9.7 Gbps de Capacidade de Firewall**

4.5.3.1.2.1. **Características do Hardware**

4.5.3.1.2.1.1. O equipamento deve se instalar em mesa ocupando no máximo 1U (44,45mm) da referida mesa;

4.5.3.1.2.1.2. Dispor de fonte de alimentação com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;

4.5.3.1.2.1.3. Deverão ser fornecidos todos os cabos de energia, serial (RS-232/RJ45) ou similar, para instalação e funcionamento do dispositivo;

4.5.3.1.2.1.4. Possuir led indicador on/off, disco e devices de rede;

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.1.2.1.5. Possuir throughput mínimo de 9.7 Gbps para tráfego UDP;

4.5.3.1.2.1.6. Suportar no mínimo 6.000.000 (seis milhões) conexões simultâneas;

4.5.3.1.2.1.7. Suportar no mínimo 45.000 (quarenta e cinco mil) novas conexões por segundo;

4.5.3.1.2.1.8. Possuir throughput mínimo de 1.25 Gbps para tráfego IPS/IDS;

4.5.3.1.2.1.9. Possuir throughput mínimo de 2.0 Gbps para tráfego VPN IPSEC com criptografia (AES-256);

4.5.3.1.2.1.10. Possuir throughput mínimo de 1.2 Gbps para tráfego VPN SSL com criptografia (AES-256);

4.5.3.1.2.1.11. Possuir throughput mínimo de 700 Mbps para tráfego SSL Inspection;

4.5.3.1.2.1.12. Possuir throughput mínimo de 850 Mbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

4.5.3.1.2.1.13. Possuir no mínimo 4 (quatro) interfaces de rede Gigabit Ethernet 10/100/1000/2500 Mbps com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

4.5.3.1.2.1.14. Possuir dispositivo de armazenamento interno de no mínimo 64 GB padrão SSD e deve suportar expansão futura para, no mínimo, 120 GB;

4.5.3.1.2.1.15. Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento;

4.5.3.1.2.1.16. Possuir pelo menos 1 (uma) porta USB para conexão de dispositivos externos;

4.5.3.1.2.1.17. A interface USB deve suportar o uso de modem 3G/4G/LTE para conexão de link de Internet;

4.5.3.1.3. **Appliance NGFW de 11.8 Gbps de Capacidade de Firewall**

4.5.3.1.3.1. **Características do Hardware**

4.5.3.1.3.1.1. O equipamento deve se instalar em mesa ocupando no máximo 1U (44,45mm) da referida mesa;

4.5.3.1.3.1.2. Dispor de fonte de alimentação com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.1.3.1.3. Deverão ser fornecidos todos os cabos de energia, serial (RS-232/RJ45) ou similar, para instalação e funcionamento do dispositivo;

4.5.3.1.3.1.4. Possuir led indicador on/off, disco e devices de rede;

4.5.3.1.3.1.5. Possuir throughput mínimo de 11.8 Gbps para tráfego UDP;

4.5.3.1.3.1.6. Suportar no mínimo 7.000.000 (sete milhões) conexões simultâneas;

4.5.3.1.3.1.7. Suportar no mínimo 52.000 (cinquenta e duas mil) novas conexões por segundo;

4.5.3.1.3.1.8. Possuir throughput mínimo de 1.5 Gbps para tráfego IPS/IDS;

4.5.3.1.3.1.9. Possuir throughput mínimo de 2.5 Gbps para tráfego VPN IPSEC com criptografia (AES-256);

4.5.3.1.3.1.10. Possuir throughput mínimo de 1.5 Gbps para tráfego VPN SSL com criptografia (AES-256);

4.5.3.1.3.1.11. Possuir throughput mínimo de 900 Mbps para tráfego SSL Inspection;

4.5.3.1.3.1.12. Possuir throughput mínimo de 1.0 Gbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

4.5.3.1.3.1.13. Possuir no mínimo 6 (seis) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

4.5.3.1.3.1.14. Possuir dispositivo de armazenamento interno de no mínimo 120 GB padrão SSD;

4.5.3.1.3.1.15. Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento;

4.5.3.1.3.1.16. Possuir pelo menos 1 (uma) porta USB para conexão de dispositivos externos;

4.5.3.1.3.1.17. A interface USB deve suportar o uso de modem 3G/4G/LTE para conexão de link de Internet;

4.5.3.1.4. **Appliance NGFW de 19.4 Gbps de Capacidade de Firewall**

4.5.3.1.4.1. **Características do Hardware**

4.5.3.1.4.1.1. Deverá ser entregue dois equipamentos idênticos para atender a funcionalidade de cluster;

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.1.4.1.2. O equipamento deve se instalar em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 1U (44,45mm) do referido rack;

4.5.3.1.4.1.3. Dispor de fonte de alimentação interna com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;

4.5.3.1.4.1.4. Possuir painel/led indicador on/off, disco e devices de rede;

4.5.3.1.4.1.5. Possuir throughput de no mínimo 19.4 Gbps para tráfego UDP;

4.5.3.1.4.1.6. Suportar no mínimo 8.200.000 (oito milhões e duzentas mil) conexões simultâneas;

4.5.3.1.4.1.7. Suportar no mínimo 65.000 (sessenta e cinco mil) novas conexões por segundo;

4.5.3.1.4.1.8. Possuir throughput mínimo de 3.0 Gbps para tráfego IPS/IDS;

4.5.3.1.4.1.9. Possuir throughput mínimo de 3.0 Gbps para tráfego VPN IPSEC com criptografia (AES-256);

4.5.3.1.4.1.10. Possuir throughput mínimo de 1.8 Gbps para tráfego VPN SSL com criptografia (AES-256);

4.5.3.1.4.1.11. Possuir throughput mínimo de 1.3 Gbps para tráfego SSL Inspection;

4.5.3.1.4.1.12. Possuir throughput mínimo de 2.5 Gbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

4.5.3.1.4.1.13. Possuir pelo menos 6 (seis) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

4.5.3.1.4.1.14. Possuir dispositivo de armazenamento interno de no mínimo 120 GB padrão SSD;

4.5.3.1.4.1.15. Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento;

4.5.3.1.4.1.16. Possuir no mínimo 1 (uma) porta USB para conexão de dispositivos externos;

4.5.3.1.4.1.17. A interface USB deve suportar o uso de modem 3G/4G/LTE para conexão de link de Internet;

4.5.3.2. **Especificações Gerais de Software NGFW Para Todos os Itens**

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.2.1. Das Funcionalidades do Firewall, SD-Wan, VPN IPsec/SSL

4.5.3.2.1.1. Características Gerais

4.5.3.2.1.1.1. Quaisquer licenças que forem entregues para atender aos recursos da solução especificado no termo de referência, deverão ter seu vencimento de acordo com o período de contrato.

4.5.3.2.1.1.2. O desempenho e as interfaces solicitados deverão ser comprovados através de datasheet público na internet. Caso haja divergência entre métricas do mesmo datasheet, será aceito o valor de menor capacidade.

4.5.3.2.1.1.3. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

4.5.3.2.1.1.4. Todos os recursos listados neste termo de referência deverão ser suportado e estar disponíveis na versão mais atual do software fornecido;

4.5.3.2.1.1.5. Os desempenhos dos appliances ofertados devem ser mensurados através da metodologia baseada em proxy (Proxy Based), não serão aceitos appliances mensurados somente no método baseado em fluxo (Flow Based);

4.5.3.2.1.1.6. Interface em português, espanhol e inglês;

4.5.3.2.1.1.7. Suportar notificação de vencimento da licença na janela de alertas com os dias restantes da data vencimento;

4.5.3.2.1.1.8. Suportar acesso à Web por HTTP e CLI por TELNET;

4.5.3.2.1.1.9. Permitir alterar a porta padrão para os acessos a interface de administração via HTTP, HTTPs e CLI;

4.5.3.2.1.1.10. Atualização de modo “offline”, onde pode ser baixado na base do fabricante e posteriormente fazer o upload do arquivo na solução.

4.5.3.2.1.1.11. Restore de Snapshot sem executar o Wizard e sem licenciamento;

4.5.3.2.1.1.12. A solução deve oferecer suporte ao NAT444 (CGNAT) ou funcionalidade que implemente a persistência no NAT de saída independente da porta de destino, de forma que o endereço IP e porta traduzidos para um determinado usuário se mantenham os mesmos nas novas sessões que cheguem com o mesmo endereçamento IP e porta de origem;

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.2.1.1.13. Suportar segundo fator de autenticação (2FA/MFA) via token / OTP (One Time Password);

4.5.3.2.1.1.14. Deve suportar sistemas virtuais;

4.5.3.2.1.1.15. 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 diferentemente;

4.5.3.2.1.1.16. Qualquer interface de rede do equipamento deverá ser utilizada como gerenciamento, ou seja, não deve haver nenhuma interface exclusiva para a função de gerenciamento;

4.5.3.2.1.1.17. O sistema deve permitir o acesso à interface de gerenciamento WEB por qualquer interface de rede configurada;

4.5.3.2.1.1.18. O software deverá ser fornecido em sua versão mais atualizada, não sendo permitido qualquer tipo de comprovação futura.

4.5.3.2.1.1.19. Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução.

4.5.3.2.1.1.20. Todos os recursos detalhados no termo de referência deverão ser providos por um único software.

4.5.3.2.1.1.21. Tanto os Gateways de Segurança bem como a Gerência Centralizada deverão suportar monitoramento através de SNMP v1, v2 e v3.

4.5.3.2.1.1.22. Deverá possuir uma janela para monitoramento do tráfego de rede com informações do throughput e da quantidade de conexões simultâneas;

4.5.3.2.1.1.23. A Solução deverá prover inspeção SSL:

4.5.3.2.1.1.24. Deve suportar cluster do tipo Failover (HA) com replicação da tabela de estado;

4.5.3.2.1.1.25. Suportar a utilização de um proxy para atualização do software e licenciamento e deverá permitir as seguintes opções de configuração:

a) Endereço do servidor;
b) Porta do servidor;
c) Usuário;
d) Senha;

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.2.1.1.26. Deverá permitir o monitoramento SNMP, no mínimo, dos seguintes itens:

a) Desempenho total (throughput);
b) Conexões simultâneas;
c) Usuários autenticados;
d) Serviços habilitados ou desabilitados;
e) Quantidade de endereços distribuídos pelo DHCP.

4.5.3.2.1.1.27. Deverá implementar a funcionalidade de "zero-touch" para sua primeira implementação ou substituição. Dessa forma, deverá ser possível provisionar a configuração do equipamento via sistema de gerenciamento centralizado, transformando a atividade em uma simples conexão física de equipamento, sem a necessidade de configurações individuais nos equipamentos;

4.5.3.2.1.1.28. A Solução deve permitir ao administrador associar na solução de gerenciamento centralizado o número de série dos equipamentos ao site onde será instalado, de maneira que ao se ativar um equipamento no site remoto, esse equipamento se conecte com a Sistema Central e receba a configuração;

4.5.3.2.1.1.29. Ao instalar um equipamento no site remoto, cabeá-lo e energizá-lo, ele deverá tentar localizar Sistema Central para receber a sua configuração, sem que seja necessária qualquer configuração via console local do equipamento;

4.5.3.2.1.1.30. Deverá possuir um painel centralizado para exportação e agendamento de relatórios e deverá permitir exportá-los nos formatos: HTML, PDF, CSV;

4.5.3.2.1.1.31. Implementar protocolo de coleta de informações de fluxos que circulam pelo equipamento, como Netflow v5, v9 e v10 (IPFIX):

4.5.3.2.1.1.32. Os módulos de IPS, SD-WAN, Controle de aplicativos, Proxy WEB e Antimalware devem ser disponibilizados em perfis e estes devem ser inseridos em uma única política.

4.5.3.2.1.1.33. Deve implementar o protocolo ECMP;

4.5.3.2.1.1.34. O sistema deverá implementar otimização de fluxos TCP em conjunto com mecanismo para evitar retransmissão ou implementar métodos de correção de erros que permitam à

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

unidade receptora recuperar pacotes que venham a ser perdidos na transmissão.

4.5.3.2.1.1.35. Deve possuir suporte ao protocolo de encapsulamento de redes MPLS;

4.5.3.2.1.1.36. Esta condição deve permitir conectar links MPLS diretamente no equipamento sem a necessidade de estar plugado a um segundo roteador/dispositivo.

4.5.3.2.1.1.37. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;

4.5.3.2.1.1.38. 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;

4.5.3.2.1.2. **Recursos Gerais de Firewall**

4.5.3.2.1.2.1. Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas;

4.5.3.2.1.2.2. Possuir um sistema de armazenamento remoto para salvar backups da solução com suporte a conexões utilizando os protocolos Network File System (NFS), SSH e que permita salvar em dispositivo USB conectado localmente;

4.5.3.2.1.2.3. Possibilitar a visualização dos países de origem e destino nos logs de eventos, de acessos e ameaças.

4.5.3.2.1.2.4. Possuir mecanismo que permita a realização de cópias de segurança (backups) do sistema e restauração remota, através da interface gráfica, a solução deve permitir o agendamento diário ou semanal;

4.5.3.2.1.2.5. O sistema deve permitir configurar o período ou número de cópias que deseja manter no repositório remoto e executar a manutenção de período automaticamente.

4.5.3.2.1.2.6. As cópias de segurança devem ser salvas compactadas e criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;

4.5.3.2.1.2.7. O sistema ainda deve contemplar um recurso de cópia de segurança do tipo snapshot, que contemple a cópia completa das configurações dos serviços e recursos do sistema;

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.2.1.2.8. Deve possibilitar a restauração do snapshot através da interface web de qualquer ponto remoto, de modo a contribuir para uma restauração imediata sem a necessidade de reinicialização do sistema;

4.5.3.2.1.2.9. Deve permitir habilitar ou desabilitar o registro de log por política de firewall.

4.5.3.2.1.2.10. Possuir controle de acesso à internet por endereço IP de origem e destino;

4.5.3.2.1.2.11. Possuir controle de acesso à internet por sub-rede;

4.5.3.2.1.2.12. Possuir suporte a tags de VLAN (802.1q);

4.5.3.2.1.2.13. Suportar agregação de links, segundo padrão IEEE 802.3ad;

4.5.3.2.1.2.14. Possuir ferramenta de diagnóstico do tipo tcpdump;

4.5.3.2.1.2.15. Possuir integração com Servidores de Autenticação RADIUS, TACACS+, LDAP e Microsoft Active Directory;

4.5.3.2.1.2.16. Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

4.5.3.2.1.2.17. Possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um, vários para vários e vários para um.

4.5.3.2.1.2.18. Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;

4.5.3.2.1.2.19. Permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br;

4.5.3.2.1.2.20. Possuir suporte a roteamento dinâmico RIP V1, V2, OSPFv2, OSPFv3, BGP e suportar duplicação de pacotes;

4.5.3.2.1.2.21. Possuir funcionalidades de DHCP Cliente, Servidor e Relay;

4.5.3.2.1.2.22. Deve ser possível configurar um servidor RADIUS para a validação de usuários;

4.5.3.2.1.2.23. A solução deve consultar o Servidor Radius integrado, caso o Servidor Radius autorize, o NGFW deve entregar o endereço IP do range; caso contrário, não fornece endereço

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

IP e a máquina não recebe o endereço, ficando sem acesso à rede.

4.5.3.2.1.2.24. Deverá suportar aplicações multimídia como: H.323, SIP;

4.5.3.2.1.2.25. Possuir tecnologia de firewall do tipo Stateful;

4.5.3.2.1.2.26. Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo-passivo;

4.5.3.2.1.2.27. Permitir o funcionamento em modo transparente tipo “bridge”;

4.5.3.2.1.2.28. Permitir a criação de mínimo 4090 VLANS no padrão IEEE 802.1q por interface de rede;

4.5.3.2.1.2.29. Possuir conexão entre estação de gerência e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando);

4.5.3.2.1.2.30. Deverá suportar forwarding de multicast;

4.5.3.2.1.2.31. Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP;

4.5.3.2.1.2.32. Permitir o agrupamento de serviços;

4.5.3.2.1.2.33. Possuir mecanismo de anti-spoofing;

4.5.3.2.1.2.34. Possuir a funcionalidade de balanceamento e contingência de links;

4.5.3.2.1.2.35. Possibilitar a configuração dos timeouts de resposta dos protocolos de conexão, devendo suportar no mínimo a definição das opções do timeout padrão do ICMP, estabelecimento do TCP, envio do SYN em sessões TCP.

4.5.3.2.1.2.36. Permitir a configuração de regras de entrada baseado em zona de rede, possibilitando habilitar recursos de autenticação e restrição por origem baseado em IP.

4.5.3.2.1.2.37. Deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas, suportando ao menos: Yahoo! Messenger, MSN Messenger, ICQ, Telegram, Whatsapp, WeChat, Snapchat BitTorrent, UTorrent, Vuze, eDonkey, GNUTella, Skype e Microsoft Teams.

4.5.3.2.1.2.38. A solução deverá suportar nativamente o recurso SIMET (nic.br) medidor de Internet.

4.5.3.2.1.3. **Política de Segurança**

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.2.1.3.1. Permitir limitar a quantidade máxima de pacotes por segundo no Firewall, evitando ataques distribuídos ou anomalias de tráfego causadas por possíveis malwares na rede;

4.5.3.2.1.3.2. A configuração de proteção DOS deve estar disponível para habilitar em modo global e por política de segurança;

4.5.3.2.1.3.3. Possuir recurso de validação das políticas de segurança para identificar regras duplicadas ou que se ofusquem;

4.5.3.2.1.3.4. Possui uma única janela de configuração de política de segurança onde seja possível inserir os perfis de Proxy WEB, IPS, APP control, SD-WAN e ATP.

4.5.3.2.1.3.5. Deverá permitir implementar filtros de IPS, WEB Filter, Threat Protection, SSL Inpection, Application Control, assim como definir roteamento de aplicativos por SD-Wan, limitação de taxa de DOS por pacotes em uma única política.

4.5.3.2.1.3.6. Exibir na própria política a visualização de quais módulos estão habilitados, sem que seja necessário a edição da regra de proteção.

4.5.3.2.1.3.7. Possibilitar a edição de objetos vinculados, sem a necessidade de recriar a política.

4.5.3.2.1.3.8. Possibilitar a duplicação de uma política, otimizando tempo de configuração;

4.5.3.2.1.4. **Identificação de Usuário**

4.5.3.2.1.4.1. Deve possuir a capacidade de criação de políticas de acesso de Firewall, VPN, IPS e Controle de aplicação integradas ao repositório de usuários sendo: Active Directory, LDAP, TACAC´S e Radius;

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

4.5.3.2.1.4.3. Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador (Captive Portal), sem a necessidade de agente;

4.5.3.2.1.4.4. Deve possuir Captive Portal com suporte a Autenticação Social (Facebook, Twitter, Google);

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.2.1.4.5. A solução deverá ser capaz de identificar nome do usuário, login, máquina/computador registrados no Microsoft Active Directory;

4.5.3.2.1.4.6. Para o sistema de controles no serviço de autenticação o produto deve possuir, no mínimo, as seguintes condições para o Controle de Autenticação:

a) Usuários e Grupos de Usuários;
b) Datas (Objetos de Datas)
c) Horários (Objetos de Horário)
d) Lista de palavras chave ou conjunto de combinações de expressões regulares, (Objetos de Dicionários)
e) Endereços Remotos (Objetos de IPv4 e IPv6)
f) Zona de Rede (Múltiplas Zonas)

4.5.3.2.1.4.7. A solução deve suportar autenticação por SSO utilizando WMI (Windows Management Instrument), ou seja, não deve ser necessário instalar nenhum agente no servidor de autenticação.

4.5.3.2.1.4.8. A solução deve suportar o sincronismo entre vários NGFW em relação a replicação das sessões autenticadas da filial (Branch) na matriz (Head Office) e vice-versa, sem a necessidade de agentes externos.

4.5.3.2.1.4.9. A solução deverá suportar múltiplos Servidores de Autenticação (MS AD e/ou Ldap) atuando no modo failover;

4.5.3.2.1.5. **Das Funcionalidades Da Vpn:**

4.5.3.2.1.5.1. VPN baseada em appliance;

4.5.3.2.1.5.2. Possuir algoritmos de criptografia para túneis VPN: AES, 3DES;

4.5.3.2.1.5.3. Suporte a certificados PKI X.509 para construção de VPNs;

4.5.3.2.1.5.4. Possuir suporte a VPNs IPSec site-to-site:

4.5.3.2.1.5.5. Criptografia, 3DES, AES128, AES256, AES-GCM-128

4.5.3.2.1.5.6. Integridade MD5, SHA-1, SHA-256, SHA384 e AES-XCBC;

4.5.3.2.1.5.7. Algoritmo Internet Key Exchange (IKE) versões I e II;

4.5.3.2.1.5.8. AES 128 e 256 (Advanced Encryption Standard);

4.5.3.2.1.5.9. Suporte a Diffie-Hellman Grupo 1, Grupo 2, Grupo 5, Grupo 14; Grupo 15, Grupo 16, Grupo 17, Grupo 18, Grupo 19, Grupo 20, Grupo 21, Grupo 22, Grupo 23, Grupo 24, Grupo

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

25, Grupo 26, Grupo 27, Grupo 28, Grupo 29, Grupo 30, Grupo 31, Grupo 32;

4.5.3.2.1.5.10. Possuir suporte a VPN SSL;

4.5.3.2.1.5.11. Possuir capacidade de realizar SSL VPNs utilizando certificados digitais;

4.5.3.2.1.5.12. Suportar VPN SSL Clientless, sem a necessidade de utilização de Java, no mínimo, para os serviços abaixo:

a) RDP;
b) VNC;
c) SSH;
d) WEB;
e) SMB.

4.5.3.2.1.5.13. Deve permitir a arquitetura de vpn hub and spoke;

4.5.3.2.1.5.14. Suporte a VPNs IPSec client-to-site;

4.5.3.2.1.5.15. Deverá possuir cliente próprio para Windows para o estabelecimento da VPN client-to-site.

4.5.3.2.1.5.16. Suporte à inclusão em autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol);

4.5.3.2.1.5.17. Possuir funcionalidades de Auto-Discovery VPN capaz de permitir criar tuneis de VPN dinâmicos entre múltiplos dispositivos (spokes) com um gateway centralizador (hub).;

4.5.3.2.1.5.18. A funcionalidade de AD-VPN deve suportar criar os seguintes tipos de tuneis:

a) Site-to-Site;
b) Full-Mesh;
c) Star.

4.5.3.2.1.5.19. Suportar configuração VTI (virtual interface) na configuração de túneis VPN site-to-site com BGP (Border Gateway Protocol). Os túneis são utilizados para prover uma comunicação criptografada e encapsulada, por rotas, entre o peer (NGFW local) e o host;

4.5.3.2.1.5.20. A solução poderá atuar como cliente de tuneis VPN IPSec com suporte à autenticação XAuth/PSK e/ou XAuth/RSA.

4.5.3.2.1.5.21. A VPN client-to-site deve suportar o estabelecimento automático da VPN nos protocolos ICMP ou DNS.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

(53/UDP), caso o cliente remoto identifique que a porta padrão está sendo bloqueada;

4.5.3.2.1.5.22. Possuir recurso para configurar vários túneis simultâneos da VPN cliente-to-site, com o objetivo de aumentar o desempenho do tráfego;

4.5.3.2.1.5.23. Suportar segundo fator de autenticação (2FA/MFA) via token / OTP (One Time Password);

4.5.3.2.1.6. **SD-WAN:**

4.5.3.2.1.6.1. Entende-se como tecnologia SD-WAN (Software-Defined WAN) a rede de área ampla definida por software que centraliza a gerência da rede WAN em uma console única, eliminando a necessidade de intervenções manuais em roteadores em localidades remotas, proporcionando visibilidade do tráfego, seleção de caminho dinâmico baseado em políticas de QoS, aplicação ou performance e utilização de túneis VPN para comunicação entre os sites remotos;

4.5.3.2.1.6.2. Possuir o balanceamento automático para conexões externas à internet através das interfaces físicas;

4.5.3.2.1.6.3. Suportar modo de duplicação de pacotes de dados pelo links WAN, para que em caso de queda do link principal, possa ser enviado ao link secundário uma cópia do pacote de dados perdido permitindo assim a maior integridade e disponibilidade do tráfego;

4.5.3.2.1.6.4. Permitir utilizar VPN IPsec para interligar unidades remotas;

4.5.3.2.1.6.5. Possuir recurso de “persistência de link” para impedir a queda de conexões em aplicações que não suportam o load balance de link;

4.5.3.2.1.6.6. O balanceamento deverá ser baseado em critérios de desempenho, devendo no mínimo, permitir verificar o monitoramento do consumo de banda, perda de pacotes, jitter e latência;

4.5.3.2.1.6.7. Deve possuir uma janela web ou dashboard capaz de fornecer informações dos eventos e com informações do monitoramento de desempenho relacionado ao recurso SD-WAN;

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.2.1.6.8. O recurso de SD-WAN deverá suportar o roteamento de tráfego por política baseado em aplicação;

4.5.3.2.1.6.9. O appliance SD-WAN deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link monitorado recuperado seja avaliado. Deve suportar especificar um valor variando de 1 a 100.

4.5.3.2.1.6.10. O recurso de SD-WAN deverá permitir o monitoramento de, no mínimo 03 (três) endereços alvos para verificar a disponibilidade e desempenho do link;

4.5.3.2.1.6.11. A solução de SD-WAN NGFW deve permitir a configuração da funcionalidade de SD-WAN em qualquer interface WAN de forma agnóstica, independente se é internet, 3G/4G/LTE, entre outras;

4.5.3.2.1.6.12. A solução deverá suportar os seguintes métodos de seleção de link:

a) Failover;
b) Load Balance;
c) Spillover;
d) Dynamic Selection;

4.5.3.2.1.6.13. Deverá oferecer um monitor capaz de prover em tempo real as seguintes informações em uma única janela:

a) Consumo de banda;
b) Perda de pacotes;
c) Jitter;
d) Latência.

4.5.3.2.1.6.14. A Solução de SD-WAN deve desempenhar a função de Packet Duplication (PD) permitindo encaminhar o pacote por mais de um circuito para em casos de falhas não haver retransmissão;

4.5.3.2.1.7. **Das Funcionalidades de QoS**

4.5.3.2.1.7.1. Adotar solução de Qualidade de Serviço baseada em appliance;

4.5.3.2.1.7.2. Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;

4.5.3.2.1.7.3. Permitir modificação de valores DSCP;

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.2.1.7.4. Limitar individualmente a banda utilizada por programas de compartilhamento de arquivos do tipo peer-to-peer;

4.5.3.2.1.7.5. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

4.5.3.2.1.7.6. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;

4.5.3.2.1.7.7. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;

4.5.3.2.1.7.8. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino;

4.5.3.2.1.7.9. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

4.5.3.2.1.8. **Alta Disponibilidade**

4.5.3.2.1.8.1. Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Standby, com as implementações de Fail Over.

4.5.3.2.1.8.2. O Sincronismo dos servidores deve ser por interface exclusiva de Heartbeat;

4.5.3.2.1.8.3. No caso de falha do H.A. Ativo Primário, o H.A. Ativo secundário deve assumir de uma forma transparente sem impacto ao usuário ou perda de serviço;

4.5.3.2.1.8.4. Deverá suportar a persistências de sessão de usuarios e conexões estabelecidas, entre os membros da Alta Disponibilidade;

4.5.3.2.2. **Das Funcionalidades de Controle de Aplicação e Web Proxy**

4.5.3.2.2.1. **Controle de Aplicações**

4.5.3.2.2.1.1. As funcionalidades abaixo devem ser baseadas em appliance:

4.5.3.2.2.1.2. Deverá reconhecer no mínimo 4000 aplicações;

4.5.3.2.2.1.3. Deverá possuir, no mínimo, 19 categorias para classificação de aplicações;

4.5.3.2.2.1.4. Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações como:

a) P2P;

b) Web;

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

c) Transferência de arquivos;

d) Social;

4.5.3.2.2.1.5. Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;

4.5.3.2.2.1.6. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

4.5.3.2.2.1.7. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

4.5.3.2.2.1.8. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;

4.5.3.2.2.1.9. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;

4.5.3.2.2.1.10. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

4.5.3.2.2.1.11. Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino;

4.5.3.2.2.1.12. Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.

4.5.3.2.2.2. **Filtro de Conteúdo Web**

4.5.3.2.2.2.1. Possuir solução de filtro de conteúdo web integrado a solução de segurança

4.5.3.2.2.2.2. Possuir pelo menos 80 categorias para classificação de sites web

4.5.3.2.2.2.3. Possuir base mínima contendo, 48 milhões de sites internet web já registrados e classificados;

4.5.3.2.2.2.4. Possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites web como:

a) Webmail;

b) Instituições de Saúde;

c) Notícias;

d) Pornografia;

e) Restaurante;

f) Mídias Sociais;

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

g) Esporte;
h) Educação;
i) Games;
j) Compras;

4.5.3.2.2.2.5. Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

4.5.3.2.2.2.6. Possuir sistema de cache interno, armazenando requisições WEB em disco local e memória;

4.5.3.2.2.2.7. Deve permitir a definição do tamanho mínimo dos objetos salvos em cache no disco;

4.5.3.2.2.2.8. Deve permitir a definição do tamanho máximo dos objetos salvos em cache em memória;

4.5.3.2.2.2.9. Deve atender a estrutura de navegação através de hierarquia de proxy com e sem autenticação;

4.5.3.2.2.2.10. Possibilitar a integração com servidores de cache WEB externos;

4.5.3.2.2.2.11. Deve ser capaz de armazenar cache dinâmicos para as atualizações Microsoft Windows Update, Youtube, Sourceforge Downloads, Facebook, Google Maps;

4.5.3.2.2.2.12. Deve possuir a capacidade de excluir URL’s específicas do cache web, configurável por listas de palavras chaves com suporte inclusive a expressões regulares;

4.5.3.2.2.2.13. Integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;

4.5.3.2.2.2.14. Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory, LDAP , TACACS+ e Radius;

4.5.3.2.2.2.15. Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança da contratante;

4.5.3.2.2.2.16. Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;

4.5.3.2.2.2.17. Deverá permitir o bloqueio de URLs inválidas cujo campo CN do certificado SSL não contém um domínio válido;

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.2.2.2.18. Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web;

4.5.3.2.2.2.19. Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;

4.5.3.2.2.2.20. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

4.5.3.2.2.2.21. Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem;

4.5.3.2.2.2.22. Possuir Logs e Relatórios de tempo de navegação de sites web - Domínios Web;

4.5.3.2.2.2.23. Possuir recurso capaz de controlar e restringir o acesso a sites com base em seus nomes de domínio, conhecido como DNS Content Filter;

4.5.3.2.2.3. **Recursos do Proxy**

4.5.3.2.2.3.1. Deverá funcionar em modo Proxy Explícito para HTTP, HTTPS, FTP, POP3 e SMTP e em Proxy Transparente;

4.5.3.2.2.3.2. A solução deve ser capaz de identificar o comportamento do protocolo SSH onde pode ser feito através da inspeção do protocolo;

4.5.3.2.2.3.3. Deverá permitir configurar a porta do Proxy Explícito;

4.5.3.2.2.3.4. O equipamento deverá poder suportar funcionalidades de antispam sem a necessidade de equipamento dedicado.

4.5.3.2.3. **Das Funcionalidades da Detecção de Intrusão e ATP**

4.5.3.2.3.1. **Das Funcionalidades da Detecção de Intrusão**

4.5.3.2.3.1.1. A Detecção de Intrusão deverá ser baseada em appliance:

4.5.3.2.3.1.2. Possuir no mínimo 82.000 (oitenta e duas mil) assinaturas ou regras de IPS/IDS;

4.5.3.2.3.1.3. Permitir a criação de assinaturas customizadas pelo administrador do NGFW;

4.5.3.2.3.1.4. O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;

4.5.3.2.3.1.5. Possuir tecnologia de detecção baseada em assinatura;

4.5.3.2.3.1.6. Deverá suportar a implantação em modo Gateway, inline e em modo sniffer;

4.5.3.2.3.1.7. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.

4.5.3.2.3.1.8. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação.

4.5.3.2.3.1.9. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos.

4.5.3.2.3.1.10. Possuir opção para administrador as listas de Blacklist, Whitelist e Quarentena com suporte a endereços IPv6.

4.5.3.2.3.1.11. Possuir capacidade de remontagem de pacotes para identificação de ataques;

4.5.3.2.3.1.12. Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque; Exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de Servidores Web;

4.5.3.2.3.1.13. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;

4.5.3.2.3.1.14. Mecanismos de detecção/proteção de ataques;

4.5.3.2.3.1.15. Reconhecimento de padrões;

4.5.3.2.3.1.16. Análise de protocolos;

4.5.3.2.3.1.17. Detecção de anomalias;

4.5.3.2.3.1.18. Detecção de ataques de RPC (Remote procedure call);

4.5.3.2.3.1.19. Proteção contra-ataques de Windows ou NetBios;

4.5.3.2.3.1.20. Proteção contra-ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);

4.5.3.2.3.1.21. Proteção contra-ataques DNS (Domain Name System);

4.5.3.2.3.1.22. Proteção contra-ataques a FTP, SSH , Telnet e rlogin;

4.5.3.2.3.1.23. Proteção contra-ataques de ICMP (Internet Control Message Protocol);

4.5.3.2.3.1.24. Alarmes na console de administração;

4.5.3.2.3.1.25. Alertas via correio eletrônico;

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.2.3.1.26. Monitoração do comportamento do appliance através de SNMP, o dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;

4.5.3.2.3.1.27. Capacidade de resposta/logs ativa a ataques;

4.5.3.2.3.1.28. Terminação de sessões via TCP resets;

4.5.3.2.3.1.29. Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;

4.5.3.2.3.1.30. O Sistema de detecção de Intrusos deverá atenuar os efeitos dos ataques de negação de serviços;

4.5.3.2.3.1.31. Possuir filtros de ataques por anomalias;

4.5.3.2.3.1.32. Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;

4.5.3.2.3.1.33. Permitir filtros de anomalias de protocolos;

4.5.3.2.3.1.34. Suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;

4.5.3.2.3.1.35. Suportar verificação de ataque nas camadas de aplicação;

4.5.3.2.3.2. **Das Funcionalidades Do Threat Protection**

4.5.3.2.3.2.1. Possuir funções de Antivírus, Anti-spyware;

4.5.3.2.3.2.2. Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, POP3, SMB/CIFS e FTP;

4.5.3.2.3.2.3. Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.)

4.5.3.2.3.2.4. Permitir o bloqueio de download de arquivos por extensão e tipo de arquivo;

4.5.3.2.4. **Solução de Gerenciamento Centralizado de Firewall**

4.5.3.2.4.1. **Funcionalidades de Gerenciamento**

4.5.3.2.4.1.1. Como boa prática de segurança e de mercado, a solução de gerência deverá ser separada do gateway de segurança, onde irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste projeto;

4.5.3.2.4.1.2. A solução de gerenciamento centralizado deve possibilitar o gerenciamento de todos os Firewall contratados.

4.5.3.2.4.1.3. A solução de gerenciamento centralizado deverá ser do mesmo fabricante da solução de segurança.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.2.4.1.4. O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance físico deve ser compatível com rack 19 polegadas e possuir todos os acessórios necessários para sua instalação. Caso seja entregue em appliance virtual, deverá ser compatível com VMware ESXi e todo custo da infraestrutura necessária para suportar o appliance virtual é responsabilidade da CONTRATANTE;

4.5.3.2.4.1.5. Centralizar a administração de regras e políticas do(s) cluster(s), usando uma única interface de gerenciamento;

4.5.3.2.4.1.6. A solução deverá permitir seu gerenciamento por: CLI (Command Line Interface) via SSH, Web GUI utilizando protocolo HTTPS ou console gráfica;

4.5.3.2.4.1.7. Deve manter um canal de comunicação segura, com encriptação baseada em certificados, entre todos os componentes que fazem parte da solução de firewall, gerência, armazenamento de logs e emissão de relatórios;

4.5.3.2.4.1.8. A solução deve incluir a opção de segmentar a base de regra utilizando rótulos ou títulos de seção para organizar melhor a política facilitando a localização e gestão do administrador;

4.5.3.2.4.1.9. A solução de gerência deverá prover fácil administração na aplicação das políticas para os gateways, sendo capaz de realizar o processo de alteração de regras e configuração de todas as soluções de segurança, que pode ser aplicada nos gateways remotos em uma única sessão, evitando qualquer tipo de retrabalho.

4.5.3.2.4.1.10. Deve possibilitar a realização de "backup" e restauração de dados.

4.5.3.2.4.1.11. Deve possibilitar a gerência de "logs", realizando as configurações de relatórios de todos os "firewalls" integrados.

4.5.3.2.4.1.12. Deve permitir buscas e realizar análise de usuários e grupos, rastreando toda a sua atividade e uso da internet.

4.5.3.2.4.1.13. O gerenciamento deve permitir/possuir:

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.2.4.1.14. Criação e administração de políticas de Firewall, Controle de aplicação e IPS, Antivírus e Anti-Malware, Filtro de URL e prevenção contra ameaças avançadas;

4.5.3.2.4.1.15. Monitoração de logs;

4.5.3.2.4.1.16. Debugging;

4.5.3.2.4.1.17. Deve permitir usar palavras chaves para facilitar identificação de regras;

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

4.5.3.2.4.1.19. Autenticação integrada à base de dados local;

4.5.3.2.4.1.20. Deve possuir ferramenta para localização de objetos (por exemplo: endereço IP, Range de IP, subrede) na base de regras;

4.5.3.2.4.1.21. Criação de regras que fiquem ativas em horário definido;

4.5.3.2.4.1.22. Habilidade de upgrade via interface de gerenciamento;

4.5.3.2.4.1.23. Deverá ter a capacidade de gerar um relatório gráfico, que permita visualizar as mudanças na utilização de aplicações na rede, no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações, no tempo presente com relação ao passado;

4.5.3.2.4.1.24. Controle sobre todos os equipamentos da plataforma de proteção em uma única console, com administração de privilégios e funções;

4.5.3.2.4.1.25. Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de proteção;

4.5.3.2.4.1.26. Deve permitir a criação de objetos e políticas compartilhadas;

4.5.3.2.4.1.27. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

4.5.3.2.4.1.28. Solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

4.5.3.2.4.1.29. A solução deve permitir gerenciar templates de customização visual e marca do produto pelo sistema de gerenciamento centralizado e permitir aplicar nos NGFW's;

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

gerenciados. Portanto, deve ser possível customizar a interface gráfica nos seguintes itens:

a) Título da Página;
b) Ícone (favicon);
c) Logotipo;
d) Imagem de fundo;
e) Cores do menu (primária e secundária);

4.5.3.2.4.1.30. O sistema deve ser capaz de gerenciar de modo central as políticas de backup do equipamento remotos;

4.5.3.2.4.1.31. O sistema deve permitir habilitar uma mensagem de Disclaimer na página de login da Interface de Administração. Ou seja, a página de login deverá apresentar um banner com uma mensagem customizada pelo administrador. Essa mensagem poderá ser utilizada para avisos de políticas de uso e compliance do sistema.

4.5.3.2.4.1.32. Deve suportar sistema de cluster do tipo Alta Disponibilidade para a solução ofertada;

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

4.5.3.2.4.1.34. Deve permitir inserir uma notificação do tipo “Login Disclaimer” que deve ser exibida na página de login da Interface de Administração da solução de gerenciamento centralizado.

4.5.3.2.4.1.35. Suportar API para integração com sistemas de terceiros;

4.5.3.2.4.2. **Alta Disponibilidade**

4.5.3.2.4.2.1. Deve suportar recurso de Alta-Disponibilidade (HA), sendo um primário e outros em modo secundário com sincronização e replicação das configurações;

4.5.3.2.4.2.2. O sistema de cluster deve suportar utilizar 02 (duas) interfaces como heatbeat;

4.5.3.2.4.2.3. Deve suportar definir o intervalo do sincronismo em minutos;

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.2.4.2.4. Permitir definir o número máximo de falhas dos testes do heartbeat e a solução somente irá convergir para o segundo equipamento após atingir o valor definido;

4.5.3.2.4.2.5. Suportar inserir um endereço de email para receber notificações relacionadas ao cluster.

4.5.3.2.4.3. **Armazenamento e Gerenciamento de Logs e Eventos**

4.5.3.2.4.3.1. A solução de armazenamento e gerenciamento de logs e eventos, deverá suportar, no mínimo, e estar licenciada para receber no mínimo 50GB de logs por dia;

4.5.3.2.4.3.2. A solução de armazenamento e gerenciamento de logs e eventos poderá ser entrega na mesma solução de gerenciamento centralizado, desde que atenda aos requisitos solicitados.

4.5.3.2.4.3.3. A solução de armazenamento e gerenciamento de logs e eventos deverá ser do mesmo fabricante da solução de segurança e compatível com a ferramenta de gerenciamento centralizado.

4.5.3.2.4.3.4. Deverá prover análise de tráfego de rede de modo centralizado;

4.5.3.2.4.3.5. Deve possuir análise de tráfego de rede e ameaças por geolocalização;

4.5.3.2.4.3.6. Deverá ser capaz de receber os logs e eventos com o objetivo de prover os seguintes tipos de análises:

4.5.3.2.4.3.7. Análise de ameaças e incidentes de segurança;

4.5.3.2.4.3.8. Análise de tráfego e uso de categorias Web;

4.5.3.2.4.3.9. Análise de tráfego e uso de aplicativos;

4.5.3.2.4.3.10. Análise de tráfego e ameaças por usuário;

4.5.3.2.4.3.11. Análise de desempenho de políticas de segurança;

4.5.3.2.4.3.12. A solução ofertada deve ser capaz de fazer o gerenciamento centralizado de logs, consolidação de logs, arquivamento de logs, busca avançada de logs;

4.5.3.2.4.3.13. Deverá possuir ferramenta para salvar consultas avançadas;

4.5.3.2.4.3.14. Deve possuir relatórios personalizados;

4.5.3.2.4.3.15. Deverá ser capaz de efetuar o arquivamento de relatórios;

4.5.3.2.4.3.16. Deve possuir agendamento de relatórios;

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.2.4.3.17. Os Relatórios deverão, no mínimo, serem exportados em formatos flexíveis (PDF, CSV);

4.5.3.2.4.3.18. Logs e Relatórios de tempo de navegação de sites web - Domínios Web;

4.5.3.2.4.3.19. Permitir o envio de relatórios por e-mail;

4.5.3.2.4.3.20. Relatório por Dispositivo/Consolidado;

4.5.3.2.5. **Tabela de Distribuição do Item 1, do Lote Único**

SUBITEM DO TR Nº	DESCRIÇÃO	QTDE
4.5.3.1.1	APPLIANCE NGFW DE 5 GBPS DE CAPACIDADE DE FIREWALL	157
4.5.3.1.2	APPLIANCE NGFW DE 9.7 GBPS DE CAPACIDADE DE FIREWALL	11
4.5.3.1.3	APPLIANCE NGFW DE 11.8 GBPS DE CAPACIDADE DE FIREWALL	3
4.5.3.1.4	APPLIANCE NGFW DE 19.4 GBPS DE CAPACIDADE DE FIREWALL	2
4.5.3.2.4	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE FIREWALL	1

4.5.3.3. **A solução de segurança cibernética de bloqueio de ameaças, conforme ITEM 2, do Lote Único, deve possuir as seguintes características:**

4.5.3.3.1. **Interface e Gestão:**

4.5.3.3.1.1. Deve ser instalado em equipamento com S.O. Linux, Unix ou BSD.

4.5.3.3.1.2. Deve ter uma interface amigável para configuração e gestão.

4.5.3.3.1.3. Não deve possuir endereçamento IP nas interfaces pelas quais passam o tráfego internet.

4.5.3.3.1.4. Não deve permitir a identificação da existência da solução.

4.5.3.3.1.5. Não ser suscetível à exploração externa de possíveis vulnerabilidades no software.

4.5.3.3.1.6. Deve permitir instalação de forma transparente, sem necessidade de alterações nas configurações lógicas de rede, IP ou do roteamento do ambiente atual.

4.5.3.3.1.7. Deve atuar diretamente no tráfego de entrada da internet.

4.5.3.3.1.8. Deve proporcionar proteção abrangente para toda a infraestrutura, desde o firewall podendo incluir os roteadores à internet.

4.5.3.3.1.9. O aumento de latência no tráfego de rede não deve ser superior a 5 milésimos de segundo.

4.5.3.3.1.10. Deve permitir comunicação com a internet através de proxy.

4.5.3.3.1.11. Deve possuir painel para configuração de mecanismo para detecção de acesso indesejado.

4.5.3.3.1.12. Deve possuir painel para configuração de origens confiáveis.

4.5.3.3.1.13. Deve possuir mecanismo de autoproteção.

4.5.3.3.1.14. Deve possuir log de auditoria de tudo que foi feito na solução, devendo no mínimo identificar user, data-hora e atividade realizada.

4.5.3.3.1.15. Deve armazenar no mínimo os últimos 8.000 registros de log de auditoria.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.3.2. **Inteligência Artificial Avançada:**

4.5.3.3.2.1. Deve ser uma solução baseada em Inteligência Artificial Preditiva.

4.5.3.3.2.2. Deve ser capaz de analisar padrões de comportamento no tráfego de internet.

4.5.3.3.2.3. Deve identificar origens maliciosas e neutralizá-las imediatamente e automaticamente, sem intervenção humana.

4.5.3.3.2.4. A solução não deve depender de assinaturas para reconhecer tráfegos indesejados.

4.5.3.3.2.5. Deve criar uma blacklist local com as origens maliciosas.

4.5.3.3.2.6. Deve possuir mecanismo de gestão do tempo de guarda dos dados da blacklist.

4.5.3.3.2.7. Deve possuir capacidade de aprendizado de acessos indesejados.

4.5.3.3.3. **Taxa de Falso Positivo:**

4.5.3.3.3.1. Deve apresentar uma taxa de falso positivo inferior a 0,0001% (uma identificação errada a cada um milhão de identificações), garantindo precisão nas identificações e bloqueios.

4.5.3.3.4. **Proteção Contra Ataques de "Zero Day":**

4.5.3.3.4.1. Deve oferecer proteção eficaz contra ataques de "Zero Day", mesmo aqueles que ainda não tenham sido identificados e que ainda não possuam "assinatura de identificação" ou "patch de correção" dos fabricantes das outras soluções informáticas que o órgão disponibiliza na internet.

4.5.3.3.5. **Visibilidade:**

4.5.3.3.5.1. Deve fornecer visibilidade das origens maliciosas dos ataques.

4.5.3.3.5.2. Deve fornecer visibilidade das tentativas de acessos bloqueadas.

4.5.3.3.5.3. Deve fornecer visibilidade dos serviços de rede alvos de ataques.

4.5.3.3.5.4. Deve possuir funcionalidade que permita identificar de forma fácil e ágil o motivo do bloqueio do ataque.

4.5.3.3.5.5. Deve apresentar um dashboard para a equipe de monitoramento (SOC) com mapa dos países dos IPS atacantes.

4.5.3.3.5.6. Deve apresentar um dashboard para a equipe de monitoramento (SOC) com mapa dos países de onde foram gerados os ataques.

4.5.3.3.5.7. Deve permitir a consulta através de vários tipos de indicadores como por exemplo, IP de origem, IP de Destino, Porta de origem, Porta de destino entre outros.

4.5.3.3.5.8. Deve possuir funcionalidade de geolocalização de IP identificado como malicioso.

4.5.3.3.5.9. Deve possuir busca de CVEs na base do MITRE.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.3.5.10. Deve possuir mecanismo de autogestão do armazenamento dos logs de ataque.

4.5.3.3.6. **Relatórios e Integrações:**

4.5.3.3.6.1. Deve permitir integração, através de API, com outros equipamentos/soluções de segurança como por exemplo firewall ou soluções de observabilidade.

4.5.3.3.6.2. Deve permitir envio dos logs de ataques para servidor externo.

4.5.3.3.6.3. Deve possuir integração com rede externa de Inteligência de Ameaças Global, com capacidade de aprendizado sobre novas ameaças identificadas exercendo atividade hacker recente pelo mundo e, de forma automática e pró-ativa, ativar proteção contra essas origens.

4.5.3.3.6.4. Deve gerar relatório gerencial mensal com pelo menos as seguintes informações: quantidade de ataques, bloqueios, origens mais frequentes, países de origem e serviços mais atacados.

4.5.3.3.6.5. Deve possuir capacidade suficiente para armazenar e disponibilizar consultas aos relatórios gerenciais mensais de pelo menos 5 anos.

4.5.3.3.6.6. Deve permitir exportar os relatórios para PDF.

4.5.3.3.7. **Especificações Técnicas do Equipamento**

4.5.3.3.7.1. **O equipamento físico deve atender aos seguintes requisitos:**

4.5.3.3.7.1.1. **Dimensões e Montagem:**

4.5.3.3.7.1.1.1. Deve ser compatível com rack de 19 polegadas, com tamanho de 1U ou 2U.

4.5.3.3.7.1.2. **Conectividade:**

4.5.3.3.7.1.2.1. Deve possuir no mínimo 8 interfaces de rede Gigabit Ethernet com conexão do tipo RJ45.

4.5.3.3.7.1.2.2. Deve ter porta console para configuração local.

4.5.3.3.7.1.2.3. Deve possuir interface de rede exclusiva para acesso e gerenciamento interno do equipamento.

4.5.3.3.7.1.3. **Alimentação elétrica:**

4.5.3.3.7.1.3.1. Deve ter fonte de alimentação elétrica VAC automática nos padrões brasileiros conforme a continuidade operacional.

4.5.3.4. **Os serviços e equipamentos do ITEM 3, do Lote Único, deverão ser entregues no formato e características técnicas bem como funcionalidades conforme especificações abaixo:**

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.4.1. O serviço de acesso à Internet compreenderá a instalação, operação, manutenção e gerenciamento da infraestrutura de acesso à Internet através de roteador PE, integrado imediatamente ao roteamento BGP da Operadora. Entende-se operadora, Provedor de Internet Autônomo, ou seja, que possua ASN (Autonomous System Number) vinculado a um CNPJ de um ISP distinto, ou seja, a CONTRATADA deverá suportar a operação através de dois link dedicado distintos, oriundo de 02(dois) ASN diferentes, através de infraestrutura de chegada ao prédio da Prefeitura percorrida por caminhos diferentes, visando a eventual queda de um dos link não haver impacto na operação como um todo.

4.5.3.4.2. Cada link deverá ser entregue com blocos blocos IPV4 /29 e IPV6 /64, públicos, os quais serão cadastrados no portal numeração.br, compreendendo inicialmente banda de 500 Mbps mas a porta de rede não pode haver limite rate, devendo suportar os serviço em wire speed, pois eventual queda de um dos link, a operadora redundante deverá suportar o tráfego na integralidade.

4.5.3.4.3. Conforme topologia da rede, a CONTRATADA deverá entregar o link em duas portas distintas, uma porta conectada no equipamento de cibersegurança A e outra porta a ser conectada no equipamento de cibersegurança B. Tal feito se repetirá em cada ASN, conforme topologia apresentada.

4.5.3.4.4. Em caso de falha no equipamento A, o serviço deverá realizar a migração automática para o equipamento redundante em regime de failover, sem necessidade de configurações adicionais ou intervenções técnicas. O mesmo procedimento deverá ocorrer em situação inversa. Caso este Termo de Referência não detalhe alguma instrução específica, caberá à CONTRATADA assegurar a entrega da solução em pleno funcionamento, incluindo todos os custos inerentes à implantação, sem qualquer cobrança adicional.

4.5.3.4.5. A CONTRATADA deverá fornecer todos os equipamentos, acessórios e demais componentes indispensáveis à disponibilização do serviço no local designado, ainda que não estejam expressamente mencionados neste Termo de Referência, desde que sejam essenciais à operação da solução ou ao cumprimento das funcionalidades e configurações exigidas, sem gerar ônus adicionais à CONTRATANTE.

4.5.3.4.6. O acesso entre a operadora e o ambiente de TI da CONTRATANTE deverá ser feito exclusivamente por meio de fibra óptica da CONTRATADA.

4.5.3.4.7. Devem transportar pacotes IPv4 e IPv6 com no mínimo 1500 bytes sem exigir a fragmentação dos mesmos na camada 3 do modelo OSI.

4.5.3.4.8. Os links devem suportar IPv6, sendo necessário o fornecimento de endereçamento para as redes internas do CONTRATANTE.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.4.9. Deverão ser fornecidos 1 (roteador) por link dedicado que irá compor o ambiente de alta disponibilidade.

4.5.3.4.10. Deverá suportar todos os protocolos de roteamento necessários para suportar as conexões WANs em ambiente de alta disponibilidade (OSPF, BGP, RIP etc).

4.5.3.4.11. Cada equipamento deve possuir no mínimo 2 (duas) interfaces WAN de 1 Gbps e 2 (duas) ou mais interfaces LAN de 1 Gbps.

4.5.3.4.12. Possuir LEDs de diagnóstico sobre alimentação, atividade e diagnóstico das portas.

4.5.3.4.13. Deve possuir funcionalidades necessárias para monitoramento, diagnóstico e features como QoS, permitir a atualização remota do SO e arquivos de configuração via ethernet ou serial, FTP e TFTP; Permitir a gravação de log externo via syslog; Suportar o recurso port mirroring para um endereço IP; e suportar protocolo de coleta de tráfego Netflow ou IPFIX para a realização de coleta de informações de fluxo, tráfego que circulam no equipamento.

4.5.3.5. **Os serviços e equipamentos dos ITENS 4 e 5 deverão ser entregues no formato e características técnicas bem como funcionalidades conforme especificações abaixo:**

4.5.3.5.1. As velocidades de acesso à internet contratadas serão classificadas da seguinte maneira:

4.5.3.5.1.1. Link principal (item 4, do Lote Único): 150Mbps

4.5.3.5.1.2. Link redundante (item 5, do Lote Único): 75Mbps

4.5.3.5.1.2.1. A CONTRATADA deverá comprovar que possui capacidade de operar com dois circuitos distintos, em fibra óptica.

4.5.3.5.1.2.2. A CONTRATADA deverá comprovar que possui capacidade operacional através de redes espectrais.

4.5.3.5.2. A CONTRATADA deverá garantir largura de banda simétrica (download/upload) de 100% da velocidade contratada, em link único para o link principal (Item 4, do Lote Único), não sendo aceita a agregação de múltiplos links para atingir a velocidade contratada.

4.5.3.5.3. A CONTRATADA deverá garantir largura de banda simétrica (download/upload) de pelo menos 70% da velocidade contratada, podendo ser em 02(dois) link (Item 4, do Lote Único), um link performando em fibra óptica e outro através de chip especial para suportar esta operação estruturante, não sendo possível chip de dados convencionais, com limite de dados. Neste caso específico será aceito a agregação desses 2 link em comento, para atingir a velocidade contratada.

4.5.3.5.4. A localização e classificação de cada unidade está relacionada nos itens 7.2.1.3.1, 7.2.1.3.2 e 7.2.1.3.3.

4.5.3.5.5. O acesso de fibra óptica até o ambiente de TI da CONTRATANTE deverá ser feito exclusivamente por meio de fibra óptica da CONTRATADA, exceto chip 4/5Gbps.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.5.6. Cada acesso de fibra óptica ao ambiente de TI deve ser percorrido por caminhos distintos; não serão aceitos acessos de redes convergindo para um mesmo ISP, sendo necessária a validação de comprovação deste quesito no momento do certame.

4.5.3.6. **Requisitos Tecnológicos Mínimos Para Suportar a Conectividade das Praças**

4.5.3.6.1. **Ponto de Acesso Outdoor Wi-Fi 6 2x2**

4.5.3.6.1.1. **Conectividade:**

4.5.3.6.1.1.1. Deve possuir, no mínimo, 1 porta uplink ethernet 100/1000/2.5G Base-T em conector RJ45 com suporte a alimentação PoE compatível com o padrão IEEE 802.3at e com reconhecimento automático de crossover MDI/MDIX;

4.5.3.6.1.1.2. Deve possuir 1 porta LAN ethernet 100/1000Base-T em conector RJ45 e com reconhecimento automático de crossover MDI/MDIX;

4.5.3.6.1.1.3. Possuir porta de console para gerenciamento e configuração via linha de comando (CLI – command line interface) com conector RJ-45 diferente da porta de rede solicitada anteriormente;

4.5.3.6.1.1.4. Deve possuir 2 rádios operando nas frequências de 2,4GHz e 5GHz simultaneamente;

4.5.3.6.1.1.5. Deve possuir rádio Bluetooth Low-Energy (BLE) integrado ao equipamento;

4.5.3.6.1.1.6. Deve possuir antenas omnidirecionais internas ao equipamento com ganho mínimo de 5 dBi na frequência de 2,4GHz, 6 dBi na frequência de 5GHz;

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

4.5.3.6.1.1.8. Deve possuir LEDs indicadores de conectividade;

4.5.3.6.1.2. **Funcionalidades WLAN Deve Atender aos Seguintes Padrões:**

4.5.3.6.1.2.1. IEEE 802.11a/b/g/n/ac/ax;

4.5.3.6.1.2.2. Dupla banda 2,4 e 5GHz simultâneas;

4.5.3.6.1.2.3. Deve operar em MIMO 2x2 com suporte a 2 spatial streams e suporte a MU-MIMO;

4.5.3.6.1.2.4. Deve suportar as seguintes taxas de dados:

a) IEEE 802.11b: 1, 2, 5.5, 11 Mbps;

b) IEEE 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps;

c) IEEE 802.11n: 6.5 – 300 Mbps (20 / 40 MHz);

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

d) IEEE 802.11ac: 6.5 – 866 Mbps (20 / 40 / 80 MHz);

e) IEEE 802.11ax: 3.6 - 574 Mbps (2.4GHz, 20 / 40 MHZ)

f) IEEE 802.11ax: 3.6 - 2400 Mbps (5GHz, 20 / 40 / 80 / 160MHz)

4.5.3.6.1.2.5. Deve oferecer potência mínima de transmissão RF de 26dBm em 2,4GHz e 25dBm em 5GHz;

4.5.3.6.1.2.6. Deve suportar no mínimo 16 SSIDs simultaneamente por rádio totalizando até 32 SSIDs no sistema;

4.5.3.6.1.2.7. Deve suportar a configuração de no mínimo 16 VLANs ativas simultaneamente por rádio totalizando até 32 VLANs ativas simultaneamente no sistema;

4.5.3.6.1.2.8. O equipamento proposto deverá poder operar nos seguintes modos:

a) Access Point;

b) Wireless Mesh;

4.5.3.6.1.2.9. Deverá permitir o controle de tráfego para cada SSID;

4.5.3.6.1.2.10. Deverá selecionar dinamicamente os canais de operação;

4.5.3.6.1.2.11. Deverá selecionar automaticamente a melhor opção de conexão dos clientes (Band Steering);

4.5.3.6.1.3. **Gerenciamento**

4.5.3.6.1.3.1. Deve suportar gerenciamento SNMP v2c;

4.5.3.6.1.3.2. Deve permitir configuração dos parâmetros IP através de serviço DHCP Cliente;

4.5.3.6.1.3.3. Deve permitir acesso remoto a console via HTTP e HTTPs;

4.5.3.6.1.3.4. Deve permitir a atualização de firmware via TFTP ou HTTP;

4.5.3.6.1.3.5. Deve suportar sincronização de relógio através de SNTP ou NTP;

4.5.3.6.1.3.6. Deve suportar atualização automática do firmware quando estiver operando em modo gerenciado;

4.5.3.6.1.3.7. Deve suportar plataforma em nuvem que permite o gerenciamento de pontos de acesso de diferentes fabricantes;

4.5.3.6.1.4. **Segurança**

4.5.3.6.1.4.1. Deve suportar autenticação através de servidor RADIUS;

4.5.3.6.1.4.2. Deve suportar WiFi Protected Access (WPA/WPA2);

4.5.3.6.1.4.3. Deve suportar WPA/WPA2 (PSK);

4.5.3.6.1.4.4. Deve suportar WPA3;

4.5.3.6.1.4.5. Deve permitir bloqueio da divulgação do SSID;

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.6.1.5. **Gerais**

4.5.3.6.1.5.1. Deve suportar fonte de alimentação DC externa operando em tensões de 100 a 240 V e em frequências de 50 a 60 Hz automaticamente;

4.5.3.6.1.5.2. Deve possuir a classificação IP68 de resistência a intempéries;

4.5.3.6.1.5.3. Deve permitir montagem em parede ou poste;

4.5.3.6.1.5.4. Deve suportar temperatura de operação entre - 40°C a 60°C;

4.5.3.6.1.5.5. Deve suportar sistema operacional em conformidade com o OpenWiFi da Telecom Infra Project;

4.5.3.6.1.5.6. Deverá suportar o padrão OpenRoaming para garantir a facilidade e segurança de conexão dos clientes à rede sem fio, permitindo a ampla utilização da rede pelos usuários finais;

4.5.3.6.1.5.7. A controladora deve permitir que o access point seja controlado simultaneamente com access points de diferentes fabricantes

4.5.3.6.1.5.8. A empresa fornecedora da solução deverá apresentar uma prova de conceito (PoC) comprovando o funcionamento da controladora gerenciando no mínimo 2 access points de fabricantes diferentes

4.5.3.6.1.5.9. A empresa fornecedora deverá possuir atestado de capacidade de implementação de solução equivalente com ecossistema OpenWiFi

4.5.3.6.2. **Ponto de Acesso Indoor Wi-Fi 6 2x2**

4.5.3.6.2.1. **Conectividade**

4.5.3.6.2.1.1. Deve possuir, no mínimo, 1 porta uplink ethernet 100/1000/2.5G Base-T em conector RJ45 com suporte a alimentação PoE compatível com o padrão IEEE 802.3at e com reconhecimento automático de crossover MDI/MDIX;

4.5.3.6.2.1.2. Deve possuir 1 porta LAN ethernet 100/1000Base-T em conector RJ45 e com reconhecimento automático de crossover MDI/MDIX;

4.5.3.6.2.1.3. Possuir porta de console para gerenciamento e configuração via linha de comando (CLI – command line interface) com conector RJ-45 diferente da porta de rede solicitada anteriormente;

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.6.2.1.4. Deve possuir 1 porta USB;

4.5.3.6.2.1.5. Deve possuir 2 rádios operando nas frequências de 2,4GHz e 5GHz simultáneamente;

4.5.3.6.2.1.6. Deve possuir rádio Bluetooth Low-Energy (BLE) integrado ao equipamento;

4.5.3.6.2.1.7. Deve possuir antenas omnidirecionais internas ao equipamento com ganho mínimo de 4 dBi na frequência de 2,4GHz, 6 dBi na frequência de 5GHz e 4 dBi para BLE;

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

4.5.3.6.2.1.9. Deve possuir LEDs indicadores de conectividade WLAN e Power/Diag;

4.5.3.6.2.2. **Funcionalidades WLAN Deve Atender aos Seguintes Padrões:**

4.5.3.6.2.2.1. IEEE 802.11a/b/g/n/ac/ax;

4.5.3.6.2.2.2. Dupla banda 2,4 e 5GHz simultâneas;

4.5.3.6.2.2.3. Deve operar em MIMO 2x2 com suporte a 2 spatial streams e suporte a MU-MIMO;

4.5.3.6.2.2.4. Deve suportar as seguintes taxas de dados:

a) IEEE 802.11b: 1, 2, 5.5, 11 Mbps;
b) IEEE 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps;
c) IEEE 802.11n: 6.5 – 300 Mbps (20 / 40 MHz);
d) IEEE 802.11ac: 6.5 – 866 Mbps (20 / 40 / 80 MHz);
e) IEEE 802.11ax: 3.6 - 574 Mbps (2.4GHz, 20 / 40 MHZ)
f) IEEE 802.11ax: 3.6 - 1200 Mbps (5GHz, 20 / 40 / 80 MHz)

4.5.3.6.2.2.5. Deve oferecer potência mínima de transmissão RF de 23dBm em 2,4GHz e 23dBm em 5GHz;

4.5.3.6.2.2.6. Deve suportar Wi-Fi Multimedia (WMM);

4.5.3.6.2.2.7. Deve suportar no mínimo 16 SSIDs simultaneamente por rádio totalizando até 32 SSIDs no sistema;

4.5.3.6.2.2.8. Deve suportar a configuração de no mínimo 16 VLANs ativas simultaneamente por rádio totalizando até 32 VLANs ativas simultaneamente no sistema;

4.5.3.6.2.2.9. O equipamento proposto deverá poder operar nos seguintes modos:

a) Access Point;

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

b) Wireless Mesh;

4.5.3.6.2.2.10. Deverá permitir o controle de tráfego para cada SSID;

4.5.3.6.2.2.11. Deverá selecionar dinamicamente os canais de operação;

4.5.3.6.2.2.12. Deverá selecionar automaticamente a melhor opção de conexão dos clientes (Band Steering);

4.5.3.6.2.3. **Gerenciamento**

4.5.3.6.2.3.1. Deve suportar gerenciamento SNMP v2c;

4.5.3.6.2.3.2. Deve permitir configuração dos parâmetros IP através de serviço DHCP Cliente;

4.5.3.6.2.3.3. Deve permitir acesso remoto a console via HTTP e HTTPs;

4.5.3.6.2.3.4. Deve permitir a atualização de firmware via TFTP ou HTTP;

4.5.3.6.2.3.5. Deve suportar sincronização de relógio através de SNTP ou NTP;

4.5.3.6.2.3.6. Deve suportar atualização automática do firmware quando estiver operando em modo gerenciado;

4.5.3.6.2.3.7. Deve suportar plataforma em nuvem que permite o gerenciamento de pontos de acesso de diferentes fabricantes;

4.5.3.6.2.4. **Segurança**

4.5.3.6.2.4.1. Deve suportar autenticação através de servidor RADIUS;

4.5.3.6.2.4.2. Deve suportar WiFi Protected Access (WPA/WPA2);

4.5.3.6.2.4.3. Deve suportar WPA/WPA2 (PSK);

4.5.3.6.2.4.4. Deve suportar WPA3;

4.5.3.6.2.4.5. Deve permitir bloqueio da divulgação do SSID;

4.5.3.6.2.4.6. Desempenho

4.5.3.6.2.4.7. Deve possibilitar a conexão de até 250 clientes concorrentes por rádio totalizando 500 simultaneamente;

4.5.3.6.2.5. **Gerais**

4.5.3.6.2.5.1. Deve suportar fonte de alimentação DC externa operando em tensões de 100 a 240 V e em frequências de 50 a 60 Hz automaticamente;

4.5.3.6.2.5.2. Deve permitir montagem em parede ou teto e vir acompanhado dos devidos kits de instalação;

4.5.3.6.2.5.3. Deve permitir a instalação de trava tipo Kensington;

4.5.3.6.2.5.4. Deve suportar temperatura de operação entre 0°C a 50°C;

4.5.3.6.2.5.5. Possuir certificado válido de homologação emitido pela Anatel.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.6.2.5.6. Deverá ser apresentado certificado válido de interoperabilidade fornecido pela Wi-Fi Alliance na categoria de Enterprise Access Point;

4.5.3.6.2.5.7. Deve suportar sistema operacional em conformidade com o OpenWiFi da Telecom Infra Project;

4.5.3.6.2.5.8. Deverá suportar o padrão OpenRoaming para garantir a facilidade e segurança de conexão dos clientes à rede sem fio, permitindo a ampla utilização da rede pelos usuários finais;

4.5.3.6.2.5.9. A controladora deve permitir que o access point seja controlado simultaneamente com access points de diferentes fabricantes

4.5.3.6.2.5.10. A empresa fornecedora da solução deverá apresentar uma prova de conceito (PoC) comprovando o funcionamento da controladora gerenciando no mínimo 2 access points de fabricantes diferentes

4.5.3.6.2.5.11. A empresa fornecedora deverá possuir atestado de capacidade de implementação de solução equivalente com ecossistema OpenWiFi

4.5.3.6.3. **Switch de Acesso POE 8 Portas 2.5base-T e 2 Portas 10G SFP+**

4.5.3.6.3.1. **Conectividade**

4.5.3.6.3.1.1. Deve possuir 8 portas padrão 2.5G/1000 Base-T em conector RJ45 compatível com o padrão IEEE 802.3az de eficiência energética;

4.5.3.6.3.1.2. Deve possuir no mínimo 2 portas 10G Base-X padrão SFP+ para a instalação de módulos padrão SFP+ ou cabos DAC;

4.5.3.6.3.1.3. As portas Base-T deverão suportar autonegociação de velocidade, modo de operação e detecção MDI-MDIX;

4.5.3.6.3.1.4. Deve possuir porta console serial padrão RS-232 em conector DB-9 ou RJ45 acompanhado do respectivo cabo para conexão ao PC;

4.5.3.6.3.2. **PoE**

4.5.3.6.3.2.1. Deve suportar alimentação PoE conforme o padrão IEEE 802.3af/802.3at nas 8 portas RJ45 dentro da disponibilidade de potência destinada a esse fim;

4.5.3.6.3.2.2. Deve suportar alimentação PoE++ conforme o padrão IEEE 802.3bt em, no mínimo, 4 portas RJ45 de forma simultânea;

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.6.3.2.3. Deve possibilitar visualização da alimentação através de LED exclusivo ou de múltipla funcionalidade;

4.5.3.6.3.2.4. Deve disponibilizar no mínimo 240W para utilização exclusiva no PoE sem utilização de fonte adicional para esse fim;

4.5.3.6.3.3. **Controle**

4.5.3.6.3.3.1. Deve suportar Jumbo Frames de 12K;

4.5.3.6.3.3.2. Deve suportar até 4K VLANs segundo o protocolo IEEE 802.1Q, por porta e por protocolo;

4.5.3.6.3.3.3. Deve suportar implementação de VLANs Privativas;

4.5.3.6.3.3.4. Deve suportar implementação de Voice VLANs;

4.5.3.6.3.3.5. Deve implementar suporte a QinQ;

4.5.3.6.3.3.6. Possuir no mínimo oito filas em hardware para priorização de tráfego por porta;

4.5.3.6.3.3.7. Implementar QoS com base no protocolo 802.1p e DSCP;

4.5.3.6.3.3.8. Deve implementar controle de fluxo com o protocolo 802.3X e Back Pressure;

4.5.3.6.3.3.9. Deve implementar IGMP Snooping v1, v2 e v3;

4.5.3.6.3.3.10. Deve implementar IGMP Filtering, Immediate Leave e Querier;

4.5.3.6.3.3.11. Deve implementar MLD Snooping;

4.5.3.6.3.3.12. Deve possibilitar a limitação de Broadcast, Multicast e Unicast;

4.5.3.6.3.3.13. Deve implementar o gerenciamento de banda com valores distintos para entrada e saída;

4.5.3.6.3.3.14. Deve implementar os mecanismos de controle de fila: SP (Strict Priority) e WRR (Weighted Round Robin);

4.5.3.6.3.4. **Disponibilidade**

4.5.3.6.3.4.1. Implementar o protocolo Spanning Tree (802.1D);

4.5.3.6.3.4.2. Implementar o protocolo Rapid Spanning Tree (802.1w);

4.5.3.6.3.4.3. Deve implementar o protocolo Multiple Spanning Tree (802.1s);

4.5.3.6.3.4.4. Deve suportar detecção de laço (loopback detection);

4.5.3.6.3.4.5. Deve implementar BPDU Guard/Filter e ROOT Guard;

4.5.3.6.3.4.6. Deve suportar até 8 grupos de agregação dinâmicos no padrão LACP ou estático de até 8 portas GbE;

4.5.3.6.3.5. **Gerenciamento**

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.6.3.5.1. Deve possuir suporte a pilha dupla de protocolo IPv4/IPv6;

4.5.3.6.3.5.2. Deve suportar gerenciamento SNMP v1, v2c e v3;

4.5.3.6.3.5.3. Deve permitir configuração dos parâmetros IP através de serviço DHCP Cliente;

4.5.3.6.3.5.4. Deve permitir acesso remoto a console via Telnet, SSHv2, HTTP e HTTPs;

4.5.3.6.3.5.5. Deve permitir configuração através de plataforma de gerenciamento em nuvem com suporte a OpenLan Switching (OLS) e OpenWiFi em conformidade com as especificações da Telecom Infra Project (TIP);

4.5.3.6.3.5.6. Deve permitir acesso local a console CLI;

4.5.3.6.3.5.7. Deve permitir atualização e provisionamento automáticos, podendo este ser executado por sistema de gestão externo sendo, neste caso, necessário proporcionar a solução completa;

4.5.3.6.3.5.8. Deve suportar os grupos 1, 2, 3 e 9 de RMON;

4.5.3.6.3.5.9. Deve suportar o protocolo LLDP (IEEE 802.1ab);

4.5.3.6.3.5.10. Deve permitir armazenar no mínimo duas imagens de firmware em memória flash interna;

4.5.3.6.3.5.11. Deve permitir a atualização de firmware via HTTP, TFTP ou FTP em memória tipo flash;

4.5.3.6.3.5.12. Deve permitir armazenar no mínimo duas configurações distintas em memória flash interna;

4.5.3.6.3.5.13. Deve permitir salvar as configurações em um computador local (backup) via HTTP, TFTP ou FTP;

4.5.3.6.3.5.14. Deve suportar espelhamento de tráfego;

4.5.3.6.3.5.15. Deve suportar SNMP over IPv6;

4.5.3.6.3.5.16. Deve suportar HTTP over IPv6;

4.5.3.6.3.5.17. Deve suportar IPv6 remote ping;

4.5.3.6.3.5.18. Deve suportar NTP ou SNTP;

4.5.3.6.3.5.19. Deve implementar log de eventos em memória flash e permitir a gravação em servidor externo padrão Syslog;

4.5.3.6.3.6. **Segurança**

4.5.3.6.3.6.1. Deve possuir proteção a ataques Denial of Service;

4.5.3.6.3.6.2. Deve suportar autenticação local e através de servidor RADIUS e TACACS+;

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.6.3.6.3. Deve implementar segurança de acesso através do protocolo IEEE 802.1X e autenticação por MAC;

4.5.3.6.3.6.4. Deve suportar assinalamento automático de VLAN e política de QoS;

4.5.3.6.3.6.5. Deve possuir suporte à AAA (Authentication, Authorization and Account) em servidores RADIUS ou TACACS+;

4.5.3.6.3.6.6. Deve suportar implementação de VLANs para visitantes;

4.5.3.6.3.6.7. Deve permitir filtragem de pacotes identificados por cabeçalho ethernet ou IP;

4.5.3.6.3.6.8. Deve suportar DHCP snooping;

4.5.3.6.3.6.9. Deve suportar IP Source Guard;

4.5.3.6.3.6.10. Deve possuir Port Security ou funcionalidade similar;

4.5.3.6.3.6.11. Deve possuir Dynamic ARP Inspection ou funcionalidade similar;

4.5.3.6.3.6.12. Deve implementar MAC based ACL;

4.5.3.6.3.7. **Desempenho**

4.5.3.6.3.7.1. Deve possuir capacidade de vazão de ao menos 80 Gbps;

4.5.3.6.3.7.2. Deve chavear no mínimo 59 Mpps;

4.5.3.6.3.7.3. Tabela de endereços MAC com capacidade para no mínimo 16.000 endereços;

4.5.3.6.3.7.4. Funções camada 3

4.5.3.6.3.7.5. Deve implementar rotas estáticas;

4.5.3.6.3.7.6. Deve implementar o protocolo RIP;

4.5.3.6.3.8. **Padronização**

4.5.3.6.3.8.1. Deve ser compatível com os seguintes padrões:

a) IEEE 802.1D (STP)
b) IEEE 802.1p (COS)
c) IEEE 802.1Q (VLAN)
d) IEEE 802.1s (MSTP)
e) IEEE 802.1v (VLAN)
f) IEEE 802.1w (RSTP)
g) IEEE 802.1X (Security)
h) IEEE 802.3ad (Link aggregation)
i) IEEE 802.3x (Flow control)
j) IEEE 802.3z (Gigabit)
k) IEEE 802.1AB (Link Layer Discovery Protocol)
l) IEEE 802.3az (Energy Efficiency)

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.5.3.6.3.9. **Gerais**

4.5.3.6.3.9.1. Deve possuir fonte de alimentação interna operando em tensões de 100 a 240 V e em frequências de 50 a 60 Hz automaticamente;

4.5.3.6.3.9.2. Deve vir acompanhado do kit de suporte específico para montagem em Rack de 19;

4.5.3.6.3.9.3. O equipamento deverá ocupar uma unidade de rack;

4.5.3.6.3.9.4. Deve possuir temperatura de operação de 0° C a 50° C;

4.5.3.6.3.9.5. Deve possuir sistema operacional OpenLan Switching (OLS) em conformidade com as especificações da Telecom Infra Project (TIP);

4.6. O sistema de gerenciamento de acesso das praças deverá ser de responsabilidade da Contratada, seguindo todas as normas da lei 13.709/2018 (LEI GERAL DE PROTEÇÃO DE DADOS - LGPD) e Lei Federal nº 12.965/2014, Decreto Federal nº 8.771/2016 que regulamenta o Marco Civil da Internet e demais legislações Federais ou Municipais relativas à matéria.

4.7. O caráter confidencial das informações dos usuários será garantido, não podendo ser compartilhado, em nenhuma hipótese, inclusive para uso comercial, publicitário ou estatístico.

4.8. A contratada deverá fornecer acesso ao sistema de gerenciamento das Praças, quantidade de acesso, acesso para inserção de informações e ações da Prefeitura e demais secretarias, não sendo aceito propagandas da contratada.

4.9. O SSID da rede não poderá associar o nome do eventual contratante privado.

4.10. O formato do SSID será definido pela Prefeitura Municipal de Cáceres / Coordenação de Tecnologia da Informação (CTI).

4.11. A Contratada deverá fornecer o sistema de gerenciamento hotspot de fácil acesso para os visitantes, que seja feito a coleta do nome, telefone e e-mail dos visitantes.

4.12. Será obrigação contratual a armazenagem, por todo o período de vigência, do registro de conexão, de medições básicas da rede e de todas as informações de cadastro de usuários, incluindo as informações de preenchimento voluntário.

4.13. Ao pressionar o botão destinado à conexão com a internet pela primeira vez, ele será transferido para a página de cadastro definido pela Contratante;

4.14. Que os usuários não tenham acesso a equipamentos de outros usuários conectados à rede WI-FI.

4.15. A contratada deverá fornecer sistema ou API de gerenciamento de funcionamento dos Wi-Fi das praças para auxiliar a fiscalização e acompanhamento do funcionamento das conexões, além de identificar cada Wi-Fi com o nome das respectivas Praças.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

4.16. A Contratada deverá apresentar junto à emissão de Nota Fiscal, os respectivos relatórios de funcionamento, login acessos dos visitantes e consumo de banda por aparelho de rádio, identificando cada praça conforme mês referência da Nota Fiscal.

4.17. A contratada, se achar necessário, poderá fazer uma visita técnica aos pontos das possíveis praças que receberão a internet, para mensurar o custo de cada praça, para a montagem da proposta do preço médio total.

4.18. A contratada deverá fornecer os aparelhos que sejam capazes de abranger geograficamente toda a área da praça ofertada, podendo ser de 1(um) ou mais aparelhos para cada praça.

4.19. Deverão ser previstos todos os equipamentos ativos e passivos de rede, infraestrutura e insumos necessários ao bom funcionamento do sistema, tais como, mas não exclusivamente: postes, fios, cabos, conectores, amplificadores, racks, pontos de conexão (access points), no- breaks, wireless controllers, watch dogs, software e suprimentos complementares de energia elétrica, conforme o caso.

4.20. Cada aparelho de acesso das Praças deverá aceitar até 500 conexões simultâneas, dividindo assim a banda de internet 100mbs igualmente para os visitantes.

4.21. Internets Wi-Fi instaladas deverão ser capazes de garantir a qualidade e estabilidade do sinal aos usuários, evitando jitters e latências, sendo compatíveis com notebooks, celulares, smartphones, netbooks, tablets e outros dispositivos comumente utilizados para acesso à internet, dentro dos padrões mínimos: 802.11b, 802.11g, 802.11n e 802.11ac.

4.22. A contratada deverá garantir o nível de sinal de pelo menos -65 dBm na área de cobertura em todas as localidades e em ambas as faixas de frequência (2,4 GHz e 5 GHz).

4.23. CONTRATADA deverá dispor de ferramentas e recursos de monitoramento e controles de hardware e/ou software que possam ser operados por seus técnicos, e que possibilitem a imediata identificação de anormalidades na operação da infraestrutura de comunicação da rede Wi-Fi

4.24. A Contratada deverá fornecer uma banda de internet de 150 Mbs dedicada para cada ponto instalado.

4.25. O funcionamento de cada praça ofertada será por 24 (vinte e quatro) horas por dia, durante 7 (sete) dias da semana.

4.26. A combinação dessas tecnologias resulta em uma infraestrutura altamente disponível, segura e escalável, proporcionando continuidade operacional, proteção avançada contra ameaças cibernéticas e eficiência na comunicação entre as unidades municipais.

4.27. A solução foi desenhada para assegurar a proteção e a disponibilidade dos serviços municipais ao longo de todo o ciclo de vida do contrato, abrangendo desde a implantação inicial até a gestão contínua da infraestrutura de segurança e conectividade. A abordagem adotada permite que o município de Cáceres modernize sua infraestrutura digital, proteja seus ativos de TI e garanta a prestação eficiente de serviços à população, sempre com segurança, confiabilidade e alta performance.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

5. REQUISITOS DA CONTRATAÇÃO

5.1. Requisitos De Negócio

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

5.1.1.1. Implementação de tecnologia Next Generation Firewall (NGFW) para garantir proteção robusta contra ameaças cibernéticas e manutenção da integridade das operações de rede.

5.1.1.2. Implementação de sistema baseado em Inteligência Artificial Preditiva capaz de analisar padrões de comportamento na rede, identificar e neutralizar automaticamente ameaças sem necessidade de intervenção humana.

5.1.1.3. Disponibilização de equipamentos de hardware necessários à proteção da rede, sem a necessidade de aquisição direta, com manutenção e suporte garantidos pelo fornecedor, promovendo economicidade e flexibilidade.

5.1.1.4. Proteção eficaz contra ataques de “Zero Day”.

5.1.1.5. Atuação direta no tráfego de entrada da internet, identificando e neutralizando instantaneamente origens maliciosas.

5.1.1.6. Proteção abrangente para toda a infraestrutura, incluindo firewalls e roteadores.

5.1.1.7. Proteção abrangente para toda a infraestrutura, incluindo firewalls e roteadores.

5.1.1.8. Inclusão de software para configuração, monitoramento e gestão centralizada das políticas de segurança da rede de forma integrada e eficiente, permitindo maior controle e visibilidade.

5.1.1.9. Garantia de licenças válidas durante todo o período contratual, permitindo o pleno uso das funcionalidades da solução contratada.

5.1.1.10. Provisão de link dedicado de acesso à internet, bloco /29 e banda mínima de acesso garantida de 500Mbps para a solução NGFW SEDE (Dois Link de ASN e Rota Diferentes), essa configuração garante alta disponibilidade, resiliência a falhas e suporte eficiente às operações críticas.

5.1.1.11. Configuração e integração dos links diretamente com a solução NGFW, permitindo a gestão eficiente do tráfego e a aplicação das políticas de segurança.

5.1.1.12. Implementação de soluções SD-WAN integradas ao NGFW para conectar unidades externas vinculadas às secretarias municipais, promovendo segurança, desempenho e centralização na gestão de tráfego entre os locais.

5.1.1.13. Provisão de link primário de acesso à internet banda mínima de acesso garantida de 150Mbps Sites Remotos (Fibra Óptica), e link secundário de acesso à internet banda mínima de acesso garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G), link de ASN e rota diferentes, específicos para cada unidade externa e praças municipais, assegurando a continuidade das operações e a resiliência da rede em caso de falhas.

5.1.1.14. Realização de serviços especializados para instalação, configuração inicial e adequação às necessidades específicas do contratante e das unidades externas.

5.1.1.15. Implantação nas unidades externas de redes Wi-Fi seguras e segregadas para uso exclusivo dos servidores municipais, otimizando a conectividade e produtividade.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

5.1.1.16. Garantia de autenticação por usuário e integração com políticas de segurança baseadas no NGFW.

5.1.1.17. Oferta de internet Wi-Fi gratuita nas unidades externas e nas praças municipais, com políticas de acesso baseadas no NGFW, assegurando privacidade e controle de navegação.

5.1.1.18. Implementação de mecanismos de limitação de banda e monitoramento para manter a qualidade do serviço e evitar o uso inadequado.

5.1.1.19. Atualizações regulares de firmware e assinaturas de segurança e patches, assegurando proteção contra ameaças emergentes e melhorias contínuas no desempenho da solução.

5.1.1.20. Capacitação especializada para a equipe do contratante, com emissão de certificação que ateste o domínio das funcionalidades e a capacidade de operação e manutenção da solução.

5.1.1.21. Oferta de suporte técnico com níveis de serviço bem definidos (SLA), cobrindo atendimento remoto e presencial, para resolução de incidentes e dúvidas operacionais.

5.1.1.22. Expansibilidade da solução para atender a demandas futuras de crescimento em tráfego, usuários e funcionalidades.

5.1.1.23. Ferramentas para supervisão em tempo real e geração de relatórios detalhados para análise de desempenho, auditorias e conformidade.

5.1.1.24. Garantia de aderência às regulamentações aplicáveis à proteção de dados e segurança da informação, incluindo requisitos legais e normativos vigentes.

5.1.1.25. Solução projetada para assegurar operação ininterrupta, com mecanismos de failover, redundância e backup que minimizem o impacto de falhas ou interrupções.

5.1.1.26. Redução da complexidade operacional, proporcionando maior eficiência no gerenciamento da segurança da rede e otimização de recursos técnicos e financeiros.

5.1.1.27. Configuração de políticas de tráfego e priorização de dados para garantir a performance ideal em aplicações críticas.

5.2. **Requisitos De Capacitação**

5.2.1. Deverá ser incluído na contratação capacitação técnica para a operação da solução, a serem conduzidos diretamente pelo fabricante ou por parceiro nacional devidamente capacitado, certificado e autorizado pelo fabricante para ministrar capacitações oficiais.

5.2.2. Deverá ser ministrado em Língua Portuguesa/Brasil.

5.2.3. Realização de capacitação básica com duração de 40 horas, abrangendo os conhecimentos essenciais para operar e gerenciar a solução implantada.

5.2.4. Deverá ser realizada uma reunião prévia entre o contratante e a empresa contratada para definição do calendário da capacitação básica que trata o item 5.2.3.

5.2.4.1. O cronograma deverá ser ajustado às necessidades da equipe da Coordenação de TI e compatível com a disponibilidade operacional, garantindo a participação integral dos envolvidos e a eficácia do processo de aprendizado.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

5.2.5. Capacitação destinada a uma equipe de até 10 participantes da Coordenação de TI, garantindo maior interação com os instrutores e personalização do aprendizado.

5.2.6. Emissão de certificação oficial reconhecida pelo fabricante da solução ou por entidades de referência na área de segurança de rede, atestando a qualificação da equipe.

5.2.7. Capacitação presencial, realizado na sede da Prefeitura Municipal de Cáceres, para otimizar o tempo e garantir a participação efetiva da equipe.

5.2.8. Divisão do conteúdo em módulos, facilitando o aprendizado progressivo:

- Módulo 1: Introdução ao NGFW, IA Preditiva e princípios de segurança de rede.
- Módulo 2: Configuração inicial e operação básica dos equipamentos e software.
- Módulo 3: Gerenciamento de políticas de segurança e monitoramento da rede.
- Módulo 4: Configuração de links dedicados (redundância e backup).
- Módulo 5: Resolução de problemas e resposta a incidentes.

5.2.9. A divisão de conteúdo que trata o item 5.2.8 poderá ser alterado mediante reunião prévia entre o contratante e a empresa contratada.

5.2.10. Inclusão de laboratórios práticos para simulação de cenários reais, como aplicação de políticas de segurança, monitoramento de tráfego e configuração de redundância e backup.

5.2.11. Disponibilização de apostilas, guias de configuração, tutoriais e acesso a uma base de conhecimento técnico para consulta pós-capacitação.

5.2.12. Instruções específicas sobre a configuração, gerenciamento e monitoramento dos links de redundância e backup, incluindo a utilização de IPs fixos.

5.2.13. Aplicação de avaliação ao final da capacitação para validação do conhecimento adquirido, seguido da entrega de certificados aos aprovados.

5.2.14. Abordagem de procedimentos para garantir a continuidade operacional da solução, como atualizações, backup de configurações e gerenciamento de logs.

5.2.15. Disponibilização de suporte técnico após a capacitação, para auxiliar na aplicação prática dos conhecimentos adquiridos.

5.2.16. Orientação sobre as melhores práticas para gestão segura da rede, incluindo conformidade com normas e regulamentações aplicáveis, como a LGPD.

5.2.17. Previsão de um workshop complementar, podendo este ser por vídeo conferencia, a ser realizado após a conclusão da capacitação, para reforçar conteúdos e sanar dúvidas remanescentes.

5.2.18. Elaboração de relatórios detalhados com informações sobre a participação, desempenho e certificação da equipe, para acompanhamento da gestão de competências.

5.3. **Requisitos Legais**

5.3.1. **Conformidade Legal e Normativa:**

5.3.1.1. A contratação deve obedecer à Constituição Federal, garantindo os princípios da legalidade, moralidade, publicidade, eficiência e economicidade.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

5.3.1.2. Estar em conformidade com a Lei nº 14.133/2021, que regula as normas gerais de licitação e contratação pública.

5.3.1.3. Atender à Instrução Normativa SGD/ME nº 94, de 2022, que disciplina contratações de TIC no setor público.

5.3.1.4. Respeitar a Instrução Normativa SEGES/ME nº 65, de 2021, que trata da governança em aquisições de TIC.

5.3.1.5. Observar a Lei nº 13.709, de 2018 (LGPD), garantindo a proteção de dados pessoais.

5.3.1.6. Aplicar as disposições da Lei nº 10.520, de 2001, e do Decreto nº 10.024, de 2019, referentes ao pregão eletrônico.

5.3.1.7. Cumprir o Decreto Municipal nº 665, de 09 de outubro de 2024, que regulamenta contratações de TIC no âmbito municipal.

5.3.2. **Proteção de Dados e Privacidade:**

5.3.2.1. Garantir conformidade integral com a LGPD, implementando medidas para prevenir acessos não autorizados e vazamentos de dados pessoais.

5.3.2.2. O contratado deve demonstrar, quando solicitado, os mecanismos e políticas utilizados para assegurar a proteção de dados, sujeitos à auditoria da contratante.

5.3.3. **Transparência e Publicidade:**

5.3.3.1. Todos os atos do processo licitatório e de execução contratual deverão ser registrados e divulgados nos meios oficiais, conforme exigido por lei.

5.3.3.2. Relatórios e informações sobre a execução do contrato deverão ser disponibilizados periodicamente para consulta pública, garantindo transparência no uso dos recursos.

5.3.4. **Responsabilidade do Contratado:**

5.3.4.1. O contratado é responsável por cumprir integralmente as obrigações legais aplicáveis, incluindo as previstas na Lei nº 14.133/2021 e no Decreto Municipal nº 665/2024, respondendo por eventuais descumprimentos com as penalidades previstas em contrato e em lei.

5.4. **Requisitos De Manutenção**

5.4.1. **Manutenção Preventiva (Não Emergencial):**

5.4.1.1. Realização de manutenções programadas para garantir o funcionamento ideal da solução NGFW, incluindo inspeções, limpeza, análise de logs, e aplicação de atualizações de firmware.

5.4.1.2. Frequência mínima semestral ou conforme cronograma estabelecido entre as partes.

5.4.2. **Manutenção Corretiva (Emergencial):**

5.4.2.1. Atendimento imediato para corrigir falhas ou defeitos nos equipamentos ou no software, visando a restauração do funcionamento normal da solução NGFW.

5.4.2.2. Inclui diagnóstico remoto e, quando necessário, deslocamento técnico para reparos ou substituição de componentes.

5.4.3. **Manutenção Adaptativa (Não Emergencial):**

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

5.4.3.1. Adequação da solução NGFW às mudanças no ambiente operacional ou aos requisitos específicos do contratante, como ajustes de configuração ou implementação de novas políticas de segurança.

5.4.4. **Manutenção Evolutiva (Não Emergencial):**

5.4.4.1. Implementação de melhorias na solução, incluindo a integração de novas funcionalidades, suporte a tecnologias emergentes e expansão da capacidade para atender a demandas crescentes.

5.4.5. **Monitoramento Proativo (Não Emergencial):**

5.4.5.1. Serviço contínuo de monitoramento da solução, com análise de logs e detecção antecipada de falhas ou ameaças que exijam intervenção.

5.4.6. **Substituição de Equipamentos (Emergencial):**

5.4.6.1. Garantia de substituição rápida e sem custos adicionais de equipamentos defeituosos durante a vigência contratual, minimizando interrupções.

5.4.7. **Relatórios Periódicos (Não Emergencial):**

5.4.7.1. Emissão de relatórios detalhados sobre intervenções realizadas, estado dos equipamentos, atualizações aplicadas e resultados das manutenções.

5.4.8. **Classificação de Ocorrências:**

5.4.8.1. Critérios claros para categorizar os atendimentos em emergenciais e não emergenciais, com tratamento prioritário para problemas críticos.

5.4.9. **Tabela de atendimento:**

TIPO DE ATENDIMENTO	DESCRIÇÃO	EMERGENCIAL/NÃO EMERGENCIAL	TEMPO DE RESPOSTA	TEMPO DE SOLUÇÃO	MEIO DE ATENDIMENTO
Emergencial	Ocorrências críticas que impactem diretamente a operação da rede, como falhas graves nos equipamentos NGFW, links de redundância ou brechas de segurança.	Emergencial	Até 1 hora	Até 4 horas	Suporte remoto e, se necessário, presencial.
Corretiva	Problemas pontuais ou defeitos que não sejam de natureza crítica, mas que exijam reparo técnico para evitar impactos futuros.	Emergencial	Até 4 horas	Até 8 horas	Suporte remoto ou presencial agendado.
Preventiva	Ações periódicas de inspeção e manutenção para prevenir falhas e garantir o desempenho ideal da solução.	Não Emergencial	Agendamento prévio	Conforme cronograma	Suporte presencial planejado.
Adaptativa	Ajustes para adequação da solução a novas necessidades operacionais ou mudanças no ambiente do contratante.	Não Emergencial	Até 2 dias úteis	Até 7 dias úteis	Suporte remoto ou presencial agendado.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

Evolutiva	Melhorias e implementações que ampliem as funcionalidades ou capacidades da solução NGFW.	Não Emergencial	Até 5 dias úteis	Conforme projeto	Suporte remoto ou presencial planejado.
Substituição de Equipamentos	Substituição de equipamentos defeituosos ou que apresentem falhas que afetem a continuidade do serviço.	Emergencial	Até 1 hora	Até 4 horas	Suporte remoto e, se necessário, presencial.
Monitoramento Proativo	Monitoramento contínuo da solução para antecipar problemas, como detecção de falhas ou anomalias.	Não Emergencial	Até 4 horas	Contínuo	Suporte remoto.
Relatórios Periódicos	Emissão de relatórios detalhados sobre o status da solução NGFW, ações realizadas e estado dos equipamentos.	Não Emergencial	Até 24 horas	Conforme cronograma	Suporte remoto ou presencial agendado.

5.5. **Requisitos Temporais**

5.5.1. **Prazos de Entrega dos Equipamentos e Solução:**

5.5.1.1. O fornecimento dos equipamentos necessários para a implementação da solução, incluindo hardware, licenças e software de gerenciamento, deverá ser realizado no prazo máximo de 30 dias corridos a partir da assinatura do contrato.

5.5.1.2. A instalação, configuração e ativação completa da solução, incluindo os links de internet e redundância, deverá ser concluída no prazo máximo de 45 dias corridos após a entrega dos equipamentos.

5.5.1.3. O treinamento básico com carga horária de 40 horas para a equipe técnica da Prefeitura Municipal de Cáceres deverá ser realizada uma reunião prévia entre o contratante e a empresa contratada para definição do calendário da capacitação básica.

5.5.2. **Prazos de Atendimento para Suporte Técnico:**

5.5.2.1. **Atendimento Emergencial:**

5.5.2.1.1. Chamados emergenciais, que incluem falhas críticas que afetam diretamente a operação da rede ou a disponibilidade de serviços essenciais, deverão ser atendidos no prazo máximo de 4 horas após a abertura do chamado.

5.5.2.1.2. A solução completa para o problema deverá ser implementada no prazo máximo de 8 horas, salvo situações excepcionais que exijam medidas corretivas complexas.

5.5.2.2. **Atendimento Não Emergencial:**

5.5.2.2.1. Chamados de manutenção corretiva, preventiva, adaptativa ou evolutiva que não impactem diretamente a operação da rede deverão ser atendidos no prazo máximo de 24 horas úteis após a abertura do chamado.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

5.5.2.2.2. A resolução deverá ocorrer no prazo de até 5 dias úteis, salvo a necessidade de ajustes ou implementações que exijam maior prazo, o qual será acordado previamente.

5.5.3. **Forma de Atendimento do Suporte Técnico:**

5.5.3.1. **Atendimento Remoto:**

5.5.3.1.1. O suporte técnico deverá ser disponibilizado remotamente como primeira opção para resolução de problemas, utilizando ferramentas seguras para acesso remoto e diagnóstico.

5.5.3.1.2. O suporte remoto deverá estar disponível 24x7 (24 horas por dia, 7 dias por semana) para incidentes emergenciais.

5.5.3.2. **Atendimento Presencial:**

5.5.3.2.1. Quando a resolução do problema não for possível de forma remota, será realizado atendimento presencial por técnicos especializados.

5.5.3.2.2. O prazo para deslocamento e início do atendimento no local para casos emergenciais será de até 4 horas úteis a partir da solicitação.

5.5.3.2.3. Para casos não emergenciais, o atendimento presencial será agendado com a equipe de TI da Prefeitura, respeitando o prazo máximo de 2 dias úteis.

5.5.4. **Monitoramento e Relatórios de SLA:**

5.5.4.1. A empresa contratada deverá monitorar e registrar os tempos de atendimento e resolução de chamados, emitindo relatórios mensais que comprovem o cumprimento dos SLAs estabelecidos.

5.5.4.2. O descumprimento dos prazos estabelecidos implicará penalidades contratuais conforme especificado nos termos do contrato.

5.5.5. **Atendimento de Manutenção Preventiva e Evolutiva:**

5.5.5.1. Manutenções preventivas deverão ser realizadas trimestralmente, com agendamento prévio com a equipe de TI da Prefeitura Municipal de Cáceres.

5.5.5.2. Manutenções evolutivas, que envolvam atualizações ou melhorias significativas na solução, deverão ser realizadas mediante planejamento e acordo prévio, com prazo máximo de implementação em 30 dias úteis após a aprovação.

5.6. **Requisitos de Segurança e Privacidade**

5.6.1. **Políticas de Segurança Baseadas no NGFW**

5.6.1.1. Permitir a configuração de políticas robustas de segurança para controle e monitoramento do tráfego de rede, assegurando proteção contra ataques cibernéticos, intrusões, malwares e acessos não autorizados.

5.6.1.2. Definir regras personalizadas para bloquear tráfego malicioso e permitir apenas conexões seguras e autorizadas.

5.6.1.3. Configuração de proteção contra ataques de negação de serviço (DoS), com a opção de habilitação global ou por política específica.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

5.6.1.4. Disponibilizar uma interface única para configuração de políticas, integrando perfis de segurança como Proxy Web, IPS, Controle de Aplicações, SD-WAN e Proteção contra Ameaças Avançadas (ATP).

5.6.1.5. Implementar validação automatizada das políticas de segurança para identificar e resolver regras duplicadas ou conflitantes.

5.6.2. **Segmentação e Isolamento de Redes**

5.6.2.1. Segmentação lógica da rede principal e das redes das unidades externas, garantindo o isolamento entre setores e usuários, reduzindo os riscos de propagação de ataques.

5.6.2.2. Configuração de SD-WAN para roteamento dinâmico de tráfego entre diferentes unidades e praças municipais, assegurando desempenho e segurança.

5.6.3. **Proteção Avançada Contra Ameaças**

5.6.3.1. Ativação de funcionalidades como inspeção profunda de pacotes (DPI), prevenção contra intrusões (IPS) e detecção de anomalias baseadas em inteligência artificial.

5.6.3.2. Integração com serviços de inteligência de ameaças para identificação e mitigação de ataques emergentes.

5.6.4. **Criptografia de Dados e Segurança em Trânsito**

5.6.4.1. Garantir que todas as comunicações de dados entre firewall principal, unidades externas e dispositivos sejam protegidas por protocolos de criptografia avançados, como TLS/SSL.

5.6.4.2. Implementação de inspeção de tráfego criptografado (SSL Inspection) para detecção de ameaças em comunicações seguras.

5.6.5. **Controle de Acessos e Gerenciamento Centralizado**

5.6.5.1. Adotar autenticação multifator (MFA) para acesso ao sistema de gerenciamento do NGFW e a serviços críticos.

5.6.5.2. Realizar o gerenciamento centralizado de permissões, com auditoria detalhada de acessos e atividades realizadas na rede.

5.6.6. **Monitoramento, Logs e Alertas de Segurança**

5.6.6.1. Configuração de logs detalhados de eventos e atividades, com centralização das informações em uma solução de SIEM (Gestão de Informações e Eventos de Segurança).

5.6.6.2. Geração de alertas em tempo real para eventos críticos, como tentativas de intrusão ou anomalias de tráfego.

5.6.6.3. Emissão de relatórios periódicos sobre segurança da rede, destacando vulnerabilidades detectadas e ações tomadas.

5.6.7. **Conformidade com Normas de Segurança e Privacidade**

5.6.7.1. Garantir que a solução NGFW esteja em conformidade com a LGPD e outras legislações aplicáveis, assegurando a proteção e privacidade dos dados pessoais.

5.6.7.2. Disponibilizar recursos para anonimização ou pseudonimização de dados, conforme exigido pelas normas.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

5.6.8. **Testes e Avaliações Periódicas de Segurança**

5.6.8.1. Realização de testes de penetração (pentests) regulares para avaliar a eficácia das medidas de segurança.

5.6.8.2. Simulações de incidentes de segurança para treinar equipes e validar os planos de resposta a incidentes.

5.6.9. **Backup e Recuperação Segura**

5.6.9.1. Implementar backups automáticos e criptografados das configurações do NGFW e de dados críticos, com armazenamento em locais seguros.

5.6.9.2. Garantir processos rápidos de recuperação em caso de falha ou desastre, assegurando a continuidade operacional.

5.6.10. **Conscientização e Educação de Usuários**

5.6.10.1. Desenvolver programas regulares de conscientização sobre segurança da informação para servidores municipais, abordando práticas seguras de uso da internet.

5.6.10.2. Orientar os cidadãos sobre o uso responsável das redes Wi-Fi públicas disponibilizadas nas praças e unidades municipais.

5.7. **Requisitos de Metodologia de Trabalho**

5.7.1. Emissão de Ordem de Serviço (OS):

5.7.1.1. A execução de qualquer serviço contratado está condicionada ao recebimento pelo contratado de uma Ordem de Serviço (OS) emitida pela contratante.

5.7.1.2. A Ordem de Serviço deverá especificar, de forma clara:

- O serviço a ser executado.
- A quantidade de serviços.
- A localidade onde o serviço deverá ser prestado.

5.7.2. **Meios de Contato e Registro de Ocorrências:**

5.7.2.1. O contratado deve fornecer canais de comunicação para contato e registro de ocorrências, conforme as seguintes especificações:

- Atendimento eletrônico (e-mail, sistema de chamados ou aplicativo): 24 horas por dia, 7 dias por semana.
- Atendimento telefônico: 12 horas por dia, 5 dias por semana, garantindo resposta ágil a chamados emergenciais.

5.7.3. **Acompanhamento e Comunicação Durante a Execução:**

5.7.3.1. A execução de todos os serviços deverá ser acompanhada diretamente pelo contratado, assegurando o cumprimento das especificações definidas na Ordem de Serviço.

5.7.3.2. Eventuais ocorrências ou desvios identificados durante a execução deverão ser imediatamente comunicados à contratante, com descrição detalhada da situação e das medidas corretivas adotadas.

5.7.4. **Prazos de Atendimento e Execução:**

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

5.7.4.1. O prazo para início da execução dos serviços será contado a partir do recebimento da Ordem de Serviço, respeitando os prazos definidos nos Requisitos Temporais.

5.7.4.2. Os serviços deverão ser finalizados dentro dos prazos estabelecidos, salvo justificativas formalmente apresentadas e aceitas pela contratante.

5.7.5. **Registro e Relatório de Serviços Executados:**

5.7.5.1. Ao término de cada serviço, o contratado deverá entregar à contratante um relatório detalhado contendo:

- Descrição do serviço realizado.
- Data e horário de início e conclusão do serviço.
- Identificação dos profissionais envolvidos.
- Observações sobre eventuais dificuldades ou necessidades futuras.

5.7.5.2. O relatório deverá ser aprovado pela contratante para formalizar a conclusão do serviço.

5.7.6. **Garantia de Qualidade e Conformidade:**

5.7.6.1. O contratado deverá assegurar que todos os serviços sejam executados em conformidade com as especificações técnicas, normativas e de segurança previamente acordadas.

5.7.6.2. Qualquer serviço executado em desacordo com o estabelecido será considerado não conforme, cabendo ao contratado refazê-lo sem custos adicionais para a contratante.

5.7.7. **Reuniões de Alinhamento e Planejamento:**

5.7.7.1. O contratado deverá participar de reuniões periódicas com a contratante para alinhar prioridades, revisar o cronograma e discutir ajustes necessários nos serviços prestados.

5.7.7.2. Essas reuniões ocorrerão em frequência mínima trimestral ou conforme solicitado pela contratante.

5.7.8. **Garantia de Resposta a Ocorrências:**

5.7.8.1. O contratado deverá manter equipe disponível para atender a chamados dentro dos prazos especificados nos Requisitos de Manutenção, priorizando serviços emergenciais.

5.7.8.2. As ocorrências serão classificadas conforme sua criticidade, e o atendimento será realizado de acordo com a priorização estabelecida na Ordem de Serviço.

5.8. Requisitos de Experiência Profissional

5.8.1. **Experiência Comprovada no Fornecimento de Soluções NGFW:**

5.8.1.1. O contratado deverá comprovar experiência na implementação e gerenciamento de soluções de Next Generation Firewall (NGFW) em instituições públicas ou privadas de grande porte, preferencialmente na administração municipal.

5.8.1.2. Será exigida a apresentação de no mínimo 3 (três) atestados de capacidade técnica, emitidos por clientes anteriores, que confirmem a execução de serviços similares ao escopo deste contrato, incluindo fornecimento de hardware, software, implantação, configuração e suporte técnico.

5.8.2. **Qualificação da Equipe Técnica:**

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

5.8.2.1. A equipe técnica alocada deve possuir profissionais certificados pelo fabricante da solução NGFW a ser implementada, garantindo competência técnica para execução dos serviços contratados.

5.8.2.2. Os profissionais responsáveis pela execução dos serviços devem ter experiência mínima de 2 (dois) anos em funções relacionadas à implantação, manutenção e suporte de soluções de segurança da informação.

5.8.3. **Experiência em Projetos de TIC para o Setor Público:**

5.8.3.1. O contratado deverá demonstrar experiência específica em projetos de Tecnologia da Informação e Comunicação (TIC) realizados para órgãos da administração pública, especialmente em contextos municipais.

5.8.3.2. A comprovação poderá incluir contratos anteriores, declarações ou relatórios técnicos que atestem a capacidade do contratado em atender às exigências específicas de órgãos públicos.

5.8.4. **Atendimento a Requisitos de Escalabilidade e Complexidade:**

5.8.4.1. A empresa deverá comprovar ter executado projetos que envolvam ambientes complexos, com integração de múltiplas unidades ou localidades, utilizando tecnologias como SD-WAN e links redundantes.

5.8.4.2. Será considerado diferencial a experiência em projetos que incluíram a disponibilização de internet Wi-Fi para servidores e cidadãos.

5.8.5. **Experiência em Treinamento e Capacitação:**

5.8.5.1. A empresa deve demonstrar ter conduzido treinamentos técnicos relacionados à operação de soluções NGFW, com fornecimento de certificações reconhecidas.

5.8.5.2. O contratado deverá apresentar registro de treinamentos realizados, com informações sobre a carga horária, conteúdo programático e feedback dos participantes.

5.8.6. **Critérios de Avaliação da Experiência:**

5.8.6.1. A experiência profissional será avaliada com base nos documentos apresentados, como contratos, atestados, certificados de conclusão de projetos e outros registros comprobatórios.

5.8.6.2. A ausência de comprovação adequada poderá resultar na desclassificação da proposta, conforme previsto na legislação vigente.

5.9. **Requisitos de Segurança da Informação e Privacidade**

5.9.1. **Conformidade com Normas e Padrões de Segurança:**

5.9.1.1. O contratado deve aderir às diretrizes da ISO/IEC 27001, garantindo a gestão eficiente da segurança da informação durante toda a execução do contrato.

5.9.1.2. Implementar controles técnicos e organizacionais para mitigar riscos de acessos não autorizados, vazamentos de dados e interrupções nos serviços.

5.9.2. **Proteção de Dados Sensíveis:**

5.9.2.1. A CONTRATADA deverá assegurar a proteção de todos os dados sensíveis e confidenciais trafegados, processados ou armazenados nos equipamentos fornecidos, utilizando criptografia

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

adequada e outros mecanismos de segurança, em estrita conformidade com a Lei Geral de Proteção de Dados (LGPD).

5.9.2.2. É vedado à CONTRATADA compartilhar, divulgar ou permitir o acesso de terceiros a quaisquer dados sensíveis ou confidenciais, salvo mediante autorização expressa e formal da CONTRATANTE, observadas as disposições legais aplicáveis.

5.9.3. **Gestão de Políticas de Segurança:**

5.9.3.1. A solução fornecida deverá possibilitar a criação, gerenciamento e auditoria de políticas de segurança de forma centralizada, assegurando a rastreabilidade de todas as alterações e acessos.

5.9.3.2. As políticas deverão integrar funcionalidades de IPS (Prevenção contra Intrusões), SD-WAN, controle de aplicações, filtros de conteúdo web e inspeção de tráfego criptografado (SSL/TLS).

5.9.4. **Monitoramento e Resposta a Incidentes:**

5.9.4.1. O sistema deve realizar monitoramento contínuo para identificar e mitigar incidentes de segurança em tempo real.

5.9.4.2. Eventos críticos deverão gerar alertas automáticos e relatórios detalhados, a serem compartilhados com a CONTRATANTE conforme prazos previamente estabelecidos.

5.9.5. **Controle de Acesso:**

5.9.5.1. O acesso ao sistema de gerenciamento do NGFW e demais serviços críticos deverá ser protegido por mecanismos robustos de autenticação, incluindo autenticação multifator (MFA).

5.9.5.2. Os acessos deverão ser controlados por perfis de usuário, com registros completos (logs) de todas as atividades realizadas.

5.9.6. **Tratamento de Dados de Redes Wi-Fi:**

5.9.6.1. A solução deverá garantir a segregação lógica entre os dados trafegados por servidores municipais e cidadãos nas redes Wi-Fi disponibilizadas.

5.9.6.2. É vedada a utilização dos dados coletados ou trafegados na rede Wi-Fi para qualquer finalidade sem autorização formal da CONTRATANTE e em conformidade com a LGPD.

5.9.7. **Backup e Recuperação de Dados:**

5.9.7.1. O sistema deverá realizar backups automáticos e criptografados de todas as configurações, incluindo logs de segurança e políticas implementadas.

5.9.7.2. Deve-se garantir a recuperação rápida e segura dos dados em caso de falhas ou incidentes.

5.9.8. **Educação e Conscientização de Segurança:**

5.9.8.1. A CONTRATADA deverá fornecer materiais educativos ou treinamentos para conscientização dos servidores municipais sobre práticas seguras de navegação, uso de redes Wi-Fi e proteção contra ameaças cibernéticas.

5.9.9. **Auditorias e Testes de Segurança:**

5.9.9.1. Realizar auditorias periódicas no ambiente de segurança implementado, identificando vulnerabilidades e propondo medidas corretivas.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

5.9.9.2. Realizar testes de vulnerabilidade e simulações de incidentes para avaliar a eficácia das medidas de proteção e identificar oportunidades de aprimoramento.

5.10. **Requisitos de Sustentabilidade**

5.10.1. **Uso Eficiente de Recursos Energéticos:**

5.10.1.1. Os equipamentos fornecidos, incluindo os dispositivos NGFW, deverão possuir características de eficiência energética, certificadas por padrões internacionais reconhecidos, como Energy Star ou equivalentes.

5.10.1.2. A empresa contratada deverá garantir que os equipamentos operem com consumo energético reduzido, promovendo a sustentabilidade ambiental e diminuindo os custos operacionais.

5.10.2. **Descarte Adequado de Equipamentos Obsoletos:**

5.10.2.1. Todos os equipamentos substituídos durante a vigência do contrato deverão ser descartados de forma responsável e conforme as normas ambientais vigentes, incluindo a Política Nacional de Resíduos Sólidos (PNRS).

5.10.2.2. A contratada deverá apresentar comprovantes de descarte adequado ou reciclagem dos componentes eletrônicos substituídos.

5.10.3. **Redução de Impacto Ambiental no Transporte:**

5.10.3.1. Sempre que possível, as atividades de instalação, manutenção e suporte deverão ser realizadas de forma remota, minimizando deslocamentos físicos e reduzindo a emissão de gases de efeito estufa.

5.10.3.2. Quando o atendimento presencial for indispensável, a empresa contratada deverá priorizar o uso de veículos elétricos ou de baixo consumo energético.

5.10.4. **Promoção de Práticas Digitais Sustentáveis:**

5.10.4.1. O contratado deverá implementar soluções digitais que reduzam o uso de papel, como relatórios, registros de manutenção e documentação de configuração disponibilizados exclusivamente em formato eletrônico.

5.10.4.2. Os sistemas e ferramentas utilizados deverão ser otimizados para minimizar o consumo de banda de rede, evitando desperdícios e sobrecargas desnecessárias.

5.10.5. **Gestão Responsável dos Links de Internet:**

5.10.5.1. A configuração dos links de internet deverá priorizar o uso eficiente dos recursos disponíveis, evitando sobrecargas e consumo desnecessário.

5.10.5.2. O contratado deverá implementar práticas de monitoramento contínuo para garantir que os links estejam sendo utilizados de forma sustentável e equilibrada.

5.10.6. **Capacitação com Enfoque Sustentável:**

5.10.6.1. Os treinamentos oferecidos para a equipe da Prefeitura deverão incluir orientações sobre práticas sustentáveis no uso e gerenciamento dos sistemas e dispositivos de rede.

5.10.6.2. A capacitação deverá enfatizar a importância da economia de recursos, como energia e banda, no contexto de TI sustentável.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

5.10.7. **Relatórios de Sustentabilidade:**

5.10.7.1. A contratada deverá apresentar relatórios periódicos sobre ações e práticas sustentáveis implementadas, incluindo:

- Consumo energético dos equipamentos fornecidos.
- Impacto ambiental reduzido pelas operações remotas.
- Quantidade de materiais reciclados ou descartados adequadamente.

5.10.7.2. Esses relatórios deverão ser analisados em conjunto com a contratante para identificar oportunidades adicionais de sustentabilidade.

5.11. Da Exigência de Carta de Solidariedade

5.11.1. Será exigida a apresentação de Carta de Solidariedade, emitida pelo fabricante, como garantia da execução contratual.

5.11.2. A referida carta deverá ser apresentada juntamente com a qualificação técnica da licitante e abranger os seguintes itens da solução ofertada:

- Item 1, do Lote Único;
- Item 2, do Lote Único;
- Item 3, do Lote Único;
- Item 4, do Lote Único.

5.11.3. A exigência visa assegurar que as licitantes contratadas possuam plenas condições de fornecimento e manutenção dos equipamentos mencionados, garantindo seu pleno funcionamento durante a vigência do contrato.

5.11.4. A exigência busca resguardar a Administração contra eventuais prejuízos decorrentes da indisponibilidade de peças de reposição ou da ausência de suporte técnico necessário para ajustes e aprimoramentos dos equipamentos fornecidos.

5.12. Subcontratação

5.12.1. **Critérios para Subcontratação:**

5.12.1.1. A subcontratação de serviços pela empresa contratada será permitida apenas mediante autorização prévia e formal da Prefeitura Municipal de Cáceres.

5.12.1.2. A empresa contratada deverá garantir que a subcontratada possua capacidade técnica comprovada, com experiência e certificações relevantes ao escopo dos serviços a serem executados.

5.12.2. **Responsabilidades da Contratada em Caso de Subcontratação:**

5.12.2.1. A empresa contratada será responsável integralmente pelos serviços executados pela subcontratada, respondendo pelos mesmos padrões de qualidade, prazos e resultados exigidos no contrato.

5.12.2.2. A contratada deverá assegurar que os serviços realizados pela subcontratada estejam em conformidade com todos os requisitos técnicos, normativos e de segurança estabelecidos no contrato.

Assinado por 1 pessoa: JUREMAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

5.12.2.3. Qualquer prejuízo ou falha decorrente de serviços executados pela subcontratada será de total responsabilidade da empresa contratada, que deverá arcar com os custos e medidas corretivas necessárias.

5.12.3. **Obrigações Adicionais da Subcontratada:**

5.12.3.1. A subcontratada deverá seguir rigorosamente as normas de segurança e privacidade, especialmente aquelas relacionadas à Lei Geral de Proteção de Dados (LGPD).

5.12.3.2. A subcontratada deverá assinar um Termo de Confidencialidade, comprometendo-se a proteger todas as informações relacionadas ao projeto e à infraestrutura da Prefeitura Municipal de Cáceres.

5.12.4. **Limitações e Proibições:**

5.12.4.1. Não será permitido subcontratar o fornecimento de equipamentos essenciais, como os dispositivos NGFW, IA preditiva e softwares de gerenciamento, que deverão ser fornecidos diretamente pela contratada ou pelo fabricante autorizado.

5.12.4.2. Não será permitido subcontratar serviços que envolvam suporte emergencial ou atividades críticas que demandem resposta imediata.

5.12.4.3. A subcontratação de serviços especializados (ex.: treinamento oficial, suporte técnico avançado) somente será permitida se o subcontratado for certificado pelo fabricante da solução NGFW, IA preditiva e softwares de gerenciamento.

5.12.5. **Comunicação e Relatórios:**

5.12.5.1. A empresa contratada deverá notificar previamente a Prefeitura Municipal de Cáceres sobre qualquer intenção de subcontratar serviços, fornecendo informações detalhadas sobre a empresa subcontratada e os serviços a serem realizados.

5.12.5.2. Relatórios detalhados sobre a execução de serviços pela subcontratada deverão ser incluídos nos relatórios periódicos enviados pela empresa contratada.

5.12.6. **Penalidades em Caso de Irregularidades na Subcontratação:**

5.12.6.1. O não cumprimento das condições estabelecidas para subcontratação poderá implicar penalidades contratuais, incluindo advertências, multas ou até rescisão contratual.

5.12.6.2. A Prefeitura Municipal de Cáceres poderá solicitar a substituição imediata da subcontratada caso se identifiquem falhas graves ou descumprimento dos requisitos contratuais.

5.13. **Garantia Da Contratação**

5.13.1. Não se aplica ao objeto deste Termo de Referência.

5.14. **Da Alteração Subjetiva**

5.14.1. Não se aplica no presente processo licitatório.

6. PAPÉIS E RESPONSABILIDADES

6.1. Durante o período de vigência do contrato sem prejuízo para as obrigações mencionadas em outros dispositivos deste instrumento ou de qualquer outra obrigação imposta por lei, **serão obrigações da CONTRATANTE**:

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

6.1.1. Proporcionar à CONTRATADA todas as condições necessárias para a execução dos serviços e entrega dos produtos, incluindo infraestrutura, suporte técnico e informações adicionais de responsabilidade da CONTRATANTE.

6.1.2. Prestar à CONTRATADA todas as informações, esclarecimentos, elementos e dados técnicos necessários ao cumprimento do contrato.

6.1.3. Encaminhar à CONTRATADA todas as solicitações relativas à execução dos serviços e ao fornecimento de produtos, detalhando requisitos, prazos e especificações.

6.1.4. Permitir o acesso de empregados, prepostos ou representantes da CONTRATADA às dependências da Prefeitura Municipal de Cáceres, desde que previamente autorizado e em conformidade com as normas de segurança do local.

6.1.5. Acompanhar e fiscalizar a execução do contrato, designando servidor ou comissão responsável para monitoramento das atividades da CONTRATADA, conforme previsto na Lei nº 14.133/2021.

6.1.6. Garantir que os fiscais designados documentem ocorrências, elaborem relatórios e comuniquem irregularidades à CONTRATADA de forma tempestiva.

6.1.7. Verificar, no prazo fixado, a conformidade dos serviços prestados e produtos entregues, garantindo sua adequação às especificações contratuais.

6.1.8. Rejeitar, total ou parcialmente, serviços ou produtos que não atendam aos requisitos contratuais, comunicando a necessidade de correção ou substituição.

6.1.9. Aplicar as penalidades cabíveis, garantindo a prévia e ampla defesa da CONTRATADA.

6.1.10. Informar imediatamente à CONTRATADA qualquer problema ou irregularidade detectada nos serviços ou produtos fornecidos.

6.1.11. Solicitar, por escrito, a substituição dos serviços que apresentarem desconformidade com o contrato.

6.1.12. Emitir o Termo de Aceite Definitivo após a devida implantação dos serviços contratados.

6.1.13. Atestar as faturas de serviço apresentadas mensalmente pela CONTRATADA.

6.1.14. Manifestar-se, no prazo de 3 dias úteis, sobre as informações contidas na planilha de memória de cálculo fornecida pela CONTRATADA.

6.1.15. Efetuar o pagamento à CONTRATADA no prazo estipulado, desde que todas as obrigações contratuais tenham sido devidamente cumpridas e homologadas.

6.1.16. Promover reuniões periódicas com a CONTRATADA para avaliação do andamento dos serviços, apresentação de relatórios técnicos e resolução de eventuais problemas.

6.1.17. Registrar todas as interações e ocorrências relacionadas ao contrato, garantindo rastreabilidade e acompanhamento das obrigações de ambas as partes.

6.2. Durante o período de vigência do contrato, sem prejuízo para as obrigações mencionadas em outros dispositivos deste instrumento ou de qualquer outra obrigação imposta por lei, **serão obrigações da CONTRATADA**:

6.2.1. Cumprir todas as obrigações previstas no Edital, seus anexos e na proposta apresentada, assumindo integralmente os riscos e as despesas decorrentes da execução do contrato.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

6.2.2. Executar o objeto do contrato em sua totalidade, em conformidade com as especificações estabelecidas no Termo de Referência e no contrato firmado.

6.2.3. Efetuar a entrega dos serviços e produtos dentro dos prazos estabelecidos, garantindo que estejam em perfeitas condições e em conformidade com as especificações contratuais.

6.2.4. Acompanhar a entrega dos produtos com a devida nota fiscal, contendo marca, fabricante, modelo, procedência, prazo de garantia ou validade e demais informações exigidas.

6.2.5. Garantir que os serviços e produtos fornecidos sejam de boa qualidade, atendendo integralmente às condições, quantidades e padrões estipulados no contrato.

6.2.6. Resolver prontamente quaisquer falhas ou não conformidades apontadas pela CONTRATANTE, incluindo a substituição ou correção dos serviços e produtos rejeitados.

6.2.7. Manter, durante toda a execução do contrato, as condições de habilitação exigidas, incluindo requisitos técnicos, fiscais, trabalhistas e sociais.

6.2.8. Assumir integralmente as despesas relacionadas à execução do contrato, incluindo tributos, encargos trabalhistas e previdenciários de seus empregados.

6.2.9. Disponibilizar equipe técnica qualificada e apta a atender às demandas durante toda a vigência do contrato.

6.2.10. Implementar práticas de sustentabilidade ambiental, social e econômica na execução dos serviços, conforme princípios legais e normativos aplicáveis.

6.2.11. Permitir à CONTRATANTE a fiscalização da execução dos serviços e fornecimento dos produtos, prestando todos os esclarecimentos solicitados.

6.2.12. Registrar todas as interações e ocorrências relacionadas ao contrato, garantindo rastreabilidade e acompanhamento das obrigações contratuais.

6.2.13. Fornecer canais de atendimento eficientes para comunicação com a CONTRATANTE, garantindo solução ágil para eventuais problemas.

6.2.14. Tomar todas as providências necessárias para implantar e manter os serviços contratados em níveis satisfatórios, de acordo com o IMR e demais disposições contratuais.

6.2.15. Fornecer, sem custo adicional, todos os equipamentos e acessórios necessários à prestação dos serviços nas condições estabelecidas no contrato.

6.2.16. Diagnosticar falhas nos serviços relatadas pela CONTRATANTE e eliminar defeitos nos componentes sob sua responsabilidade.

6.2.17. Sanar quaisquer falhas, degradações ou indisponibilidades do serviço, independentemente de notificação da CONTRATANTE ou detecção via monitoramento proativo.

6.2.18. Executar serviços que acarretem riscos aos sistemas em produção ou requeiram parada de servidores, equipamentos ou rede elétrica somente fora do expediente, incluindo finais de semana e feriados, mediante prévia autorização do Setor de Tecnologia da Informação e Comunicação.

6.2.19. Comunicar à CONTRATANTE, via e-mail e com antecedência mínima de três horas, a presença de seus colaboradores no ambiente da CONTRATANTE, informando nome completo e CPF do técnico para prestação de serviços de instalação ou manutenção.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

6.2.20. Fornecer crachá de identificação a seus prepostos durante a realização das atividades no ambiente da CONTRATANTE.

6.2.21. Apresentar mensalmente relatório contendo a planilha de memória de cálculo do faturamento, detalhando:

I) Período de faturamento;
II) Discriminação dos serviços prestados e seus valores;
III) Relação dos eventos, incluindo numeração de chamado, horários de início e término;
IV) Eventos que ensejam descontos contratuais e seus respectivos valores;
V) Totais e subtotais.

6.2.22. Informar, nos relatórios fornecidos, detalhes sobre indisponibilidades ocorridas, incluindo data, período, causas, total de minutos e percentual de disponibilidade do período faturado.

6.2.23. Aplicar os devidos descontos em fatura por descumprimento do IMR, conforme previsto no contrato.

6.2.24. Apresentar mensalmente as faturas dos serviços prestados, acompanhadas da planilha de memória de cálculo definitiva validada pela CONTRATANTE.

6.2.25. Atender a reclamações ou pedidos de esclarecimento relacionados ao faturamento dos serviços contratados.

7. MODELO DE EXECUÇÃO DO OBJETO

7.1. A execução do objeto será conduzida de forma estratégica, visando garantir a plena implementação da solução contratada, conforme os requisitos previamente estabelecidos. A prestação dos serviços envolverá a implantação de um ambiente de segurança cibernética robusto, integrando tecnologias de Firewall de Nova Geração (NGFW), SD-WAN e IA Preditiva, conectividade segura e suporte técnico especializado, de modo a proporcionar alta disponibilidade, eficiência operacional e proteção integral dos ativos digitais da Prefeitura Municipal de Cáceres.

7.2. A prestação do serviço se dará em duas fases, garantindo uma implementação estruturada e um suporte contínuo para a operação da solução contratada, respeitando os prazos estipulados:

7.2.1. **Fase de Implantação** (até 60 dias após a assinatura do contrato):

7.2.1.1. Essa etapa compreende todas as atividades relacionadas à implementação física e lógica da solução. Inclui a instalação e configuração dos equipamentos, ativação dos links dedicados de internet, integração das unidades externas e praças municipais à infraestrutura de comunicação, além da capacitação técnica da equipe da Prefeitura. A fase será concluída com a entrega da documentação técnica detalhada (As Built) e a validação operacional dos serviços prestados.

7.2.1.2. A solução será implantada na sede da Prefeitura e em todas as unidades externas e praças municipais, garantindo conectividade segura e redundante para os serviços essenciais. Para viabilizar a execução adequada, serão instalados e configurados equipamentos de última geração, com capacidade para gerenciar múltiplas conexões simultâneas e otimizar o fluxo de dados.

7.2.1.3. A distribuição dos serviços seguirá a estrutura administrativa do município, contemplando unidades estratégicas vinculadas a diversas secretarias. O quantitativo necessário foi

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

dimensionado considerando a demanda operacional de cada local, garantindo que todos os pontos críticos estejam devidamente atendidos. Entre as unidades contempladas, incluem-se:

7.2.1.3.1. **Unidades Centralizadas**

SECRETARIA	UNIDADE	LOCALIZAÇÃO	QUANTIDADE
SMEAE	SMEAE - PREFEITURA SEDE (COC)	https://maps.app.goo.gl/qTzbhDM8NCAEBxBf7	1
	UNIDADE CENTRALIZADA 1		1
	UNIDADE CENTRALIZADA 2		1
SMA	SMA - ALMOXARIFADO	https://maps.app.goo.gl/NiAhRcuDi3oF6Qvn9	1
	SMA - GUARDA MUNICIPAL	https://maps.app.goo.gl/hoMkt4EuyDL3BrFKA	1
SMAGRI	SMAGRI	https://maps.app.goo.gl/J1rDH3pp4oPSEfsj7	1
SMASC	SMASC - CCI	https://maps.app.goo.gl/j8UjTvfKLx4ypbPs5	1
SME	SME - CMEC	https://maps.app.goo.gl/ZUD6oU9HeMvLqXe89	1
SMIL	SMIL - GUARITA OBRAS	https://maps.app.goo.gl/PTWC8Lr3aGwXPxnP9	1
	SMIL - GUARITA PORTICO	https://maps.app.goo.gl/u39WX2UzVeVQQWS28	1
	SMIL - OFICINA	https://maps.app.goo.gl/wQmT4CxnPbdKZUYC9	1
TOTAL			**11**

7.2.1.3.2. **Unidades Descentralizadas**

SECRETARIA	UNIDADE	LOCALIZAÇÃO	QUANTIDADE
SMEAE	SMEAE - DEFESA CIVIL	https://maps.app.goo.gl/zYaMoX5jtfJ1VQ2h8	1
	UNIDADE DESCENTRALIZADA 1	-	1
SMA	SMA - ARQUIVO	https://maps.app.goo.gl/n6Jj6YzpqNfS8cHF7	1
	UNIDADE DESCENTRALIZADA 2	-	1
SMASC	SMASC - ALMOXARIFADO	https://maps.app.goo.gl/CZV2nUAkbYMhY6uq9	1
	SMASC - CASA BELBELITA	https://maps.app.goo.gl/DxddTbATc7X73Bns5	1
	SMASC - CASA DE PASSAGEM	https://maps.app.goo.gl/WrVThbciHZooSfgX6	1
	SMASC - CENTRO DE MULTIPLO USO	https://maps.app.goo.gl/Lz5UoPyGg42jrnUn8	1
	SMASC - CONSELHO TUTELAR	https://maps.app.goo.gl/tyQnNc8nTmMfQ3MW7	1
	SMASC - CRAS I	https://maps.app.goo.gl/xPiY5KnmduNnBgK49	1
	SMASC - CRAS II	https://maps.app.goo.gl/HPNPDMJ2U98R5tRm8	1
	SMASC - CREAS	https://maps.app.goo.gl/xoJqeaMyfF9Ds6g19	1
	SMASC - SAICA	https://maps.app.goo.gl/CCwLfifR6sWyhhdm7	1
	SMASC - GANHA TEMPO	https://maps.app.goo.gl/5AXCG6MYtbiF1gwV7	1
	UNIDADE DESCENTRALIZADA 3	-	1
SME	SME - SECRETARIA DE EDUCAÇÃO	https://maps.app.goo.gl/WbNKuCbpt1rDS5TE7	1
	SME - MERENDA	https://maps.app.goo.gl/byhFeQxucnAjkWfH8	1
	SME - CENTRO MUNICIPAL DE EDUCAÇÃO INFANTIL	https://maps.app.goo.gl/r9P3FHMDnqK3KTGUA	1

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

	SME - EM 16 DE MARÇO	https://goo.gl/maps/irEBgMynkLFUVdqDA	1
	SME - EM BRINCANDO E APRENDENDO	https://goo.gl/maps/qUYuASgJv5KN9z9v6	1
	SME - EM BURITI	https://goo.gl/maps/oJLMV4MMGaWkxdi7A	1
	SME - EM BUSCANDO O SABER	https://maps.app.goo.gl/52UwvjnQcLHDWQ7k6	1
	SME - EM CENTRO EDUCACIONAL DOM MÁXIMO BIENNÉS	https://goo.gl/maps/BDNwB6uZWrEapfWx5	1
	SME - EM DES. GABRIEL PINTO DE ARRUDA	https://goo.gl/maps/BDCMfHEfwrEELscN9	1
	SME - EM DR. JOSÉ RODRIGUES FONTES	https://maps.app.goo.gl/gN8iVN15FtGRnxbB9	1
	SME - EM DUQUE DE CAXIAS	https://goo.gl/maps/s5PAoUDUNHedzdks6	1
	SME - EM FAZENDO ARTE	https://maps.app.goo.gl/kTP6RNoQeYxuAfPNA	1
	SME - EM GARCÊS	https://goo.gl/maps/3J1HfZuFZ9v5WEcj9	1
	SME - EM GOTINHAS DO SABER	https://goo.gl/maps/mYM52pa2QkFA2j2C9	1
	SME - EM JARDIM GUANABARA	https://goo.gl/maps/Rfg8wh2T7iw4NrbP6	1
	SME - EM JARDIM PARAÍSO	https://goo.gl/maps/kkyMp6LAXieSyvPW9	1
	SME - EM NOVO ORIENTE	https://maps.app.goo.gl/4gacByZXhJ48UMvt5	1
	SME - EM PEQUENO SÁBIO	https://goo.gl/maps/EMEBFPffRm6Tb62a8	1
	SME - EM PROF. EDUARDO BENEVIDES LINDOTE	https://goo.gl/maps/Y43ifBkKTAwNN1U86	1
	SME - EM PROFª ISABEL CAMPOS	https://goo.gl/maps/1MgqjESG46yCxwe88	1
	SME - EM PROFA. ERENICE SIMÃO ALVARENGA	https://goo.gl/maps/yo4E1htCJ5EJYWE48	1
	SME - EM RAQUEL RAMÃO DA SILVA	https://goo.gl/maps/ke1dUMYCGWqwve6P8	1
	SME - EM SANTOS DUMONT	https://goo.gl/maps/uyBXsZNDDszodCxk6	1
	SME - EM TANCREDO NEVES	https://goo.gl/maps/fKVomd6j3LZtfjkS8	1
	SME - EM VILA IRENE	https://goo.gl/maps/aGdb2PV6NF3Yoxhe7	1
	SME - EM VILA REAL	https://goo.gl/maps/dfKNaDkEfK2V8YiJ8	1
	SME - EM VITÓRIA RÉGIA	https://goo.gl/maps/vP5EUrdTiHhhw13y6	1
	SME - EMEI FREI GRIGNION	https://goo.gl/maps/LmB1VSuePV8FtSXHA	1
	SME - EMEI IRENE COELHO CRUZ	https://goo.gl/maps/BiLhvdeg1tRmiuR37	1
	SME - EMEI MADRE MARIA ESTEVÃO	https://goo.gl/maps/kRXo9FN7eFvufAaV8	1
	SME - EMEI PROFESSORA DULSÂNGELA DE ALMEIDA SOUZA	https://maps.app.goo.gl/QZKQCN7SU9D2qwgd8	1
	SME- LIMOEIRO	https://goo.gl/maps/nrqaUDmiZV3xDpUN9	1
	SME - NOSSA SENHORA APARECIDA	https://goo.gl/maps/uYpxYHJzCmm6Qo1w8	1
	SME - PAULO FREIRE	https://maps.app.goo.gl/DE7sbzdMQVbaQXS77	1

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

	SME - PROFª LÉA MARIA LARA SILVA	https://maps.app.goo.gl/pjrMdwiU6wSSn3Uf7	1
	SME - PROVÍNCIA DE AREZZO	https://goo.gl/maps/NSNEbdrq1cjknywX8	1
	SME - ROÇA VELHA	https://goo.gl/maps/fGfEoY7trAGZhmS9A	1
	SME - SANTA CATARINA	https://goo.gl/maps/VzU6r8C8TVQJc3RM7	1
	SME - SANTO ANTÔNIO DO CARAMUJO	https://goo.gl/maps/ducAKNjzSQXECMHj9	1
	SME - SOTECO	https://maps.app.goo.gl/P32RY2iPJR7VLC9p7	1
	SME - TRANSPORTE EDUCAÇÃO	https://maps.app.goo.gl/cQumZ9jvaygvLQ159	1
	SME - EM UNIÃO	https://goo.gl/maps/zxtNZfD4YSyKrDVk8	1
	SME - CLARINÓPOLIS	https://goo.gl/maps/ducAKNjzSQXECMHj9	1
	SME - INFRAESTRUTURA EDUCAÇÃO	https://maps.app.goo.gl/b3bCUzB8qwz7vRd77	1
	SME - LARANJEIRA I	https://goo.gl/maps/jB1SZ3za3cdYev4a6	1
	SME - SÃO FRANCISCO	https://maps.app.goo.gl/sxzj1LsfxkFEX7Zy6	1
	UNIDADE DESCENTRALIZADA 4	-	1
	UNIDADE DESCENTRALIZADA 5	-	1
	UNIDADE DESCENTRALIZADA 6	-	1
	UNIDADE DESCENTRALIZADA 7	-	1
SMMADE	SMMADE	https://maps.app.goo.gl/zYaMoX5jtfJ1VQ2h8	1
	UNIDADE DESCENTRALIZADA 8	-	1
SMEL	SMEL - CIE	https://maps.app.goo.gl/Kkk4g4zUipLG7RDw6	1
	SMEL - DIDI PROFETA	https://maps.app.goo.gl/wUmbU83AgrRCFAjy6	1
	UNIDADE DESCENTRALIZADA 9	-	1
SMIL	SMIL - AEROPORTO	https://maps.app.goo.gl/N6nKAp5k4TpbGE1n6	1
	UNIDADE DESCENTRALIZADA 10	-	1
SMS	SMS - SECRETARIA DE SAUDE	https://maps.app.goo.gl/VWf4EYS5mnNdMk85A	1
	SMS - CAPS, AMBULATÓRIO DERMATOLÓGICO, LABORATORIO MUNICIPAL, ALMOXARIFADO, CMS	https://maps.app.goo.gl/3YsQdJ4PJUVqd6nG7	1
	SMS - CAPSI INFANTO JUVENIL	https://maps.app.goo.gl/NRE6n76fGEMAzeyy9	1
	SMS - CENTRO DE ESPECIALIDADES MEDICAS CEM	https://maps.app.goo.gl/zkjGjchEE1wsL14r8	1
	SMS - CENTRO DE SAUDE REFERENCIAL	https://maps.app.goo.gl/Z5MEaMJi68dU5hrG6	1
	SMS - CENTRO REAB DOM AQUINO CORREA CACERES CER II	https://maps.app.goo.gl/VhCQc4YayPyXp7sj8	1
	SMS - CEO	https://maps.app.goo.gl/wZMwZd1mfqVrkuRW6	1
	SMS - CTA CENTRO DE TESTAGEM E	https://maps.app.goo.gl/QPC3oTbJjodwapDV7	1

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

	ACONSELHAMENTO SAE CACERES		
	SMS - FARMACIA BASICA DA SMS	https://maps.app.goo.gl/YwUSzHzPiKE5h3Vy8	1
	SMS - FROTAS	https://maps.app.goo.gl/UQZEQZxDpudbq1wH7	1
	SMS - POSTO DE SAUDE DA PAIOL	https://maps.app.goo.gl/PHsDSTgdLW1CdkacA	1
	SMS - POSTO DE SAUDE DE VILA APARECIDA	https://maps.app.goo.gl/uGRnxEjReD6jHpJ9A	1
	SMS - POSTO DE SAUDE DO LIMAO	https://maps.app.goo.gl/CfPip6ysDGqhiWmT6	1
	SMS - POSTO DE SAUDE HORIZONTE DOESTE	https://maps.app.goo.gl/6bkzEYMH7wQsigL49	1
	SMS - POSTO DE SAUDE LARANJEIRAS	https://maps.app.goo.gl/XpkQdasWsWE86U9q6?g_st=aw	1
	SMS - POSTO DE SAUDE PROF VERA LYGIA BALDO FACAO	https://maps.app.goo.gl/f6PfkXjMQjTudKqZ8	1
	SMS - POSTO DE SAUDE SADIA	https://maps.app.goo.gl/H29oLsoimParvAwv8	1
	SMS - UNID DE SAUDE DA FAMILIA VISTA ALEGRE	https://maps.app.goo.gl/FirXbqEx2srZf787A	1
	SMS - UNID SAUDE DA FAMILIA VITORIA REGIA	https://maps.app.goo.gl/mZmvrRyEijHAnTFY7	1
	SMS - UNIDADE BASICA DE SAUDE DR ADEMAR ROCHA DE OLIVEIRA CAVALHADA	https://maps.app.goo.gl/8gjpYWP87HBqcoZ46	1
	SMS - UNIDADE BASICA DE SAUDE JARDIM DAS OLIVEIRAS	https://maps.app.goo.gl/tT5o6Y7N38AVLUkZ9	1
	SMS - UNIDADE BASICA DE SAUDE SANTA ISABEL	https://maps.app.goo.gl/kUwep6ZQ8h7MucdX7	1
	SMS - UNIDADE DE SAUDE DA FAMILIA COHAB NOVA	https://maps.app.goo.gl/2dwof9LpsMAPALtM7	1
	SMS - UNIDADE DE SAUDE DA FAMILIA DO CAIC	https://maps.app.goo.gl/oJAf3xrRqWLe5Jev8	1
	SMS - UNIDADE DE SAUDE DA FAMILIA DO RODEIO	https://maps.app.goo.gl/2jADTBF6EXEvx9Ew6	1
	SMS - UNIDADE DE SAUDE DA FAMILIA JD PARAISO	https://maps.app.goo.gl/TdhriFPJ8nPUpFVx6	1
	SMS - UNIDADE DE SAUDE DA FAMILIA VILA REAL	https://maps.app.goo.gl/E1nPn9mTybVmcB267	1
	SMS - UNIDADE DE SAUDE SANTOS DUMONT	https://maps.app.goo.gl/oZuia8p4RaSbPKzP7	1
	SMS - UNIDADE DE SAUDE UNIVERSITÁRIO	https://maps.app.goo.gl/vYJEuN1ufGKzoEeK7	1
	SMS - UNIDADE SAUDE FAMILIA DO CARAMUJO	https://maps.app.goo.gl/zhXa1oX3UQzTwcHj9	1
	SMS - UNIDADE SAUDE FAMILIA JARDIM GUANABARA	https://maps.app.goo.gl/bRE93W32464phEPJ7	1

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

	SMS - UPA PRONTO ATENDIMENTO JOSE SOUTO FARIAS	https://maps.app.goo.gl/mgaRTmkRznLoMFrY7	1
	SMS - VIGILANCIA EM SAÚDE	https://maps.app.goo.gl/YJFGaUT4mc3VeFoV6	1
	UNIDADE DESCENTRALIZADA 11	-	1
	UNIDADE DESCENTRALIZADA 12	-	1
	UNIDADE DESCENTRALIZADA 13	-	1
	UNIDADE DESCENTRALIZADA 14	-	1
SMTC	SMTC	https://maps.app.goo.gl/sMPDMtU3poAP51LF7	1
	SMTC - CASA DAVERON	https://maps.app.goo.gl/fHqLcuW2X5nJCHBv6	1
	SMTC - BIBLIOTECA	https://maps.app.goo.gl/6cGeYMDAR1YMQXTX6	1
	SMTC - CLUBINHO 2000	https://maps.app.goo.gl/vaUxdTdcihpHVacH9	1
	SMTC - MUSEU	https://maps.app.goo.gl/kKvwGsx58CZmAqDfA	1
	UNIDADE DESCENTRALIZADA 15	-	1
TOTAL			**115**

7.2.1.3.3. **Praças Públicas**

SECRETARIA	PRAÇA	LOCALIZAÇÃO	QUANTIDADE
SMEAE	SMEAE - AROLDO FANAIA	https://maps.app.goo.gl/8J86ycmMgagCRjCb6	1
	SMEAE - COHAB VELHA	https://maps.app.goo.gl/ExPmvCxJtbZ6Tsxk6	1
	SMEAE - PRAÇA BENJAMIN CONSTANT	https://goo.gl/maps/Bp9fHEKnFKQ4shkB7	1
	SMEAE - PRAÇA CARAMUJO	https://maps.app.goo.gl/7h6GapqJ9cnAkc8T7	1
	SMEAE - PRAÇA CIDADE ALTA	https://goo.gl/maps/MxXmDgoFqVtZdNex8	1
	SMEAE - PRAÇA CIDADE NOVA	https://maps.app.goo.gl/W8wgiTyN45SChQ9d8	1
	SMEAE - PRAÇA COHAB NOVA	https://goo.gl/maps/7xNnbDpDas9VePnN9	1
	SMEAE - PRAÇA DA FEIRA - CENTRO	https://goo.gl/maps/sjqGYtg7KatQcwcZ8	1
	SMEAE - PRAÇA DNER - BOMBEIROS	https://goo.gl/maps/3tgxS4Uz2pnsdPxH9	1
	SMEAE - PRAÇA DO GERALDÃO	https://goo.gl/maps/iGDeEFGjFZqQ3ct79	1
	SMEAE - PRAÇA DO MONTE VERDE	https://goo.gl/maps/VDYK2HWXctL7tgmV6	1
	SMEAE - PRAÇA DOM MÁXIMO	https://goo.gl/maps/om21uh8nLLWQdJs1A	1
	SMEAE - PRAÇA DUQUE DE CAXIAS - CENTRO	https://goo.gl/maps/sjqGYtg7KatQcwcZ8	1
	SMEAE - PRAÇA HORIZONTE D'OESTE	https://maps.app.goo.gl/yNFf1xADWNWK6NkZ6	1
	SMEAE - PRAÇA JARDIM AEROPORTO	https://goo.gl/maps/W6oEg6qd6pwi7MwF9	1
	SMEAE - PRAÇA JARDIM DA OLIVEIRA (EMPA)	https://maps.app.goo.gl/Z1yuZWjrLsYP5jwP7	1
	SMEAE - PRAÇA JARDIM PARAISO	https://maps.app.goo.gl/pYiSUbjpqciUhE3N9	1

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

	SMEAE - PRAÇA JARDIM SÃO LUIZ	https://maps.app.goo.gl/nBF5xryfXZoMWjUQ9	1
	SMEAE - PRAÇA JARDIM UNIVERSITÁRIO III	https://goo.gl/maps/ofActSaScSGdXz4R6	1
	SMEAE - PRAÇA JOSÉ DE ANCHIETA	https://goo.gl/maps/A8WHwD7BX6NUWhJT6	1
	SMEAE - PRAÇA JUNCO	https://maps.app.goo.gl/qXAReBWJ7BQRPpkM9	1
	SMEAE - PRAÇA MAJOR JOÃO CARLOS	https://goo.gl/maps/Qcwdn4CXJdT5VCWQ6	1
	SMEAE - PRAÇA MEDEIROS	https://goo.gl/maps/HUThKqHzuPa6ABpEA	1
	SMEAE - PRAÇA NOVA ERA (CAMPO)	https://maps.app.goo.gl/YQKX7SBhzB9dcjcj9	1
	SMEAE - PRAÇA PANTANAL	https://goo.gl/maps/AUKWENW5iR2gENDT7	1
	SMEAE - PRAÇA RESIDENCIAL ANA PAULA	https://goo.gl/maps/pA2tyTfhq8jqo5Fk7	1
	SMEAE - PRAÇA SANTA CRUZ	https://maps.app.goo.gl/KFsn7XrjbpDGFV1X9	1
	SMEAE - PRAÇA SANTA ISABEL	https://maps.app.goo.gl/TBJYXELoqvGd7Lkm9	1
	SMEAE - PRAÇA SANTO ANTONIO	https://maps.app.goo.gl/Tu2hhrXUFw4rSABn6	1
	SMEAE - PRAÇA SÃO JORGE	https://goo.gl/maps/MxXmDgoFqVtZdNex8	1
	SMEAE - PRAÇA SÃO LOURENÇO (CAMPO)	https://maps.app.goo.gl/bouowePQbhfCzuRm7	1
	SMEAE - PRAÇA SÃO MIGUEL	https://goo.gl/maps/TeYnV6RyQdD3d4Zo8	1
	SMEAE - PRAÇA VALTER FIDELIS - VILA REAL	https://maps.app.goo.gl/PyeiqkA6niDZH3hE9	1
	SMEAE - PRAÇA VILA APARECIDA	https://maps.app.goo.gl/Cjpoxp8VnhRTkBMa9	1
	SMEAE - PRAÇA VILA REAL	https://maps.app.goo.gl/Yp8X21VytfkPPvgw6	1
	SMEAE - PRAÇA VITÓRIA RÉGIA	https://goo.gl/maps/mJXKjDVQASbukgY37	1
	SMEAE - RODOVIÁRIA	https://maps.app.goo.gl/8LyQniCzZ74f3oCC7	1
	SMEAE - SADIA	https://maps.app.goo.gl/tc1GB5cCztjYFNtm9	1
	PRAÇA MUNICIPAL 1		1
	PRAÇA MUNICIPAL 2		1
	PRAÇA MUNICIPAL 3		1
	PRAÇA MUNICIPAL 4		1
SMTC	SMTC - PALCO DE EVENTOS SEMATUR	https://maps.app.goo.gl/WsUtv8cTtAgazbeP9	1
	SMTC - PRAÇA BARÃO	https://maps.app.goo.gl/vP3qT3xGyzzbTkVf8	1
	PRAÇA MUNICIPAL 5		1
	PRAÇA MUNICIPAL 6		1
TOTAL			**46**

7.2.2. **Fase de Prestação de Serviço Mensal** (até 180 meses após a assinatura do contrato):

7.2.2.1. Após a implantação, será iniciada a fase de operação contínua da solução, garantindo a manutenção preventiva e corretiva dos equipamentos, suporte técnico especializado, monitoramento em tempo real da infraestrutura de segurança cibernética e otimização do tráfego de rede com a tecnologia SD-WAN. Essa fase inclui a prestação de serviços de segurança

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

cibernética baseada em Inteligência Artificial Preditiva, bem como a consultoria contínua para aprimoramento da política de segurança da informação do município.

7.3. Além da estruturação física, a execução do contrato incluirá a implantação de links dedicados de internet para garantir alta disponibilidade, com redundância de ASN e rotas distintas, estabilidade para os serviços administrativos e operacionais e alternativa de contingência para evitar interrupções nos serviços

7.4. O serviço de Link de Internet para as localidades que serão contempladas com WI-FI Social deverá ser implantado impreterivelmente em até 30 (trinta) dias a partir da ordem de serviço emitida pelo Gestor do Contrato.

7.5. Para o **Lote único** a CONTRATADA deverá cumprir os eventos descritos na tabela a seguir, respeitando os prazos máximos estabelecidos

MARCOS DIA	PRAZOS MÁXIMOS (EM DIAS)	EVENTO	RESPONSÁVEL
D0		Assinatura do contrato entre o CONTRATANTE e a empresa licitante vencedora.	CONTRATANTE e a CONTRATADA
D1		Emissão da Ordem de Serviço pelo CONTRATANTE	CONTRATANTE
D2	D1+2	Entrega do projeto executivo	CONTRATADA
D3	D2+2	Aprovação do projeto executivo	CONTRATANTE
D4	D1+15	Entrega dos link de Internet e WI-FI nas praças, contemplando toda a solução de segurança de SDWAN e NGFW	CONTRATADA
D5	D4+3	Emissão do Termo de Recebimento provisório, para início da conferência do serviço entregue dos Links de Internet das praças	CONTRATANTE
D6	D5+5	Emissão do Termo de Recebimento Definitivo, autorização para emissão de faturamento e início do período de execução dos serviços dos Links de Internet das praças	CONTRATANTE
D7	D1+60	Conclusão da entrega, instalação e configuração dos equipamentos, capacitação e operacionalização de todos os links de comunicação, Firewall, IA Preditiva, sensores de cibersegurança, SDWAN, NGFW	CONTRATADA
D8	D7+3	Emissão do Termo de Recebimento provisório, para início da conferência do serviço entregue.	CONTRATANTE
D9	D8+5	Emissão do Termo de Recebimento Definitivo, autorização para emissão de faturamento e início do período de execução dos serviços de links de comunicação, Firewall, Sensores de Cibersegurança, SDWAN, NGFW	CONTRATANTE

7.6. A instalação da solução será realizada por uma empresa homologada e credenciada, com compromisso solidário ao fabricante, garantindo a fluidez da implantação dentro do prazo estipulado no edital. Para assegurar a operacionalidade da solução, serão promovidas capacitações técnicas para a equipe da Prefeitura, visando aprimorar a gestão e monitoramento dos sistemas implementados.

7.7. O modelo de execução do objeto visa garantir não apenas a segurança cibernética e a conectividade da administração pública municipal, mas também a eficiência na prestação de serviços essenciais à população, promovendo inovação, resiliência e modernização tecnológica.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

8. MODELO DE GESTÃO DO CONTRATO

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

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

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

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

8.5. Após a assinatura do contrato ou instrumento equivalente~~,~~ o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

8.6. **Fiscalização**

8.6.1. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput), nos termos do Decreto nº 665 de 09 de outubro de 2024.

8.6.2. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

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

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

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

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

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

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

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

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

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

8.6.5. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

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

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

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

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

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

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

9. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

9.1. Forma de Acompanhamento da Garantia e Níveis de Serviço

9.1.1. Para cumprir com os níveis de disponibilidade a prestadora de serviços deve trabalhar com duas variáveis principais: o MTBF (Tempo médio entre falhas) da solução, e o MTTR (Tempo médio de reparação de falhas). Para aumentar a disponibilidade deve-se aumentar o MTBF e diminuir o MTTR, de forma que o sistema apresente falhas com menor frequência e que estas sejam recuperadas mais rapidamente.

Abaixo estão listados os valores de disponibilidade mensal para cada Item deste Termo:

LOTE	ITEM	SERVIÇO	DISPONIBILIDADE
1 (ÚNICO)	1	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)	99,8%
	2	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	99,8%
	3	Serviço de Link dedicado de Acesso à internet, bloco /29 e Banda Mínima de Acesso Garantida de 500Mbps (Alta Disponibilidade) SEDE (Dois Link de ASN e Rota Diferentes)	99,8%
	4 5	Serviço de Link de acesso à Internet Sites Remotos, aplica-se ao WIFI Social	99,2%

9.2. Nas planilhas abaixo estão detalhados todos os indicadores destinados à aferição dos níveis mínimos de serviço da contratação pretendida. Na apuração dos indicadores poderão ser confrontados os dados da solução de gerenciamento da CONTRATADA e do sistema de monitoramento da CONTRATANTE.

MÉTRICA 1 - DISPONIBILIDADE (IMR-01)	
Indicador de Qualidade	Índice de Disponibilidade.
Métrica	Indicador é calculado com a seguinte forma: **IDM=[(To - Ti)/To]*100** Onde: IDM = índice de disponibilidade mensal do LINK em % To = período de operação (um mês) em minutos. Ti = somatório dos tempos de inoperância durante o período de operação (1 mês) em minutos. No caso de inoperância reincidente num período inferior a 3 horas, contado a partir do restabelecimento do link da última inoperância, considerar-se-á como tempo de indisponibilidade do enlace o início da primeira inoperância até o final da última inoperância, quando o link estiver totalmente operacional. Os tempos de inoperância serão os tempos em que os links apresentarem problemas que serão obtidos dos chamados abertos no sistema de abertura de chamados técnicos (Trouble Ticket) e os tempos de indisponibilidade computados pela violação do indicador de Retardo. Somente serão desconsiderados os tempos de inoperância causados por manutenções programadas com o CONTRATANTE ressalvados, contudo, os casos fortuitos e de força maior.
Periodicidade de Aferição	Mensal
Limiar de Qualidade	Vide Item 9.1 - Forma de Acompanhamento da Garantia e Níveis de Serviço
Pontos de Controle	A CONTRATADA realizará, por meio da sua solução de gerenciamento, a coleta e o armazenamento de informações a respeito de todos os serviços pelo tempo de duração do contrato.
Relatórios de Níveis de Serviço	A CONTRATADA deverá disponibilizar mensalmente à CONTRATANTE, relatórios com os índices apurados, totalizados e apresentados mensalmente por serviço. Nos relatórios citados deverão ser apresentados: o número do ticket, tempo de indisponibilidade (horas e minutos), o tempo de interrupções programadas, o tempo de interrupções de responsabilidade da CONTRATANTE.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

	A CONTRATADA deverá disponibilizar, quando demandada pelo CONTRATANTE, relatório detalhando os tempos de falhas (com hora de início e fim da inoperância), minutos excedentes ao prazo máximo para reparo e disponibilidade no período (mês) e motivo(s) da(s) indisponibilidade(s) apurada(s). Após análise do fiscal técnico, poderá ser desconsiderado do período de inoperância, o tempo decorrente da impossibilidade da CONTRATADA acessar os equipamentos nas instalações da CONTRATANTE, comprovando a CONTRATADA que o problema estava nas dependências da CONTRATANTE.

MÉTRICA 2 - TAXA DE ERRO (IMR-02)	
Indicador de Qualidade	Percentual de erros nos enlaces.
Métrica	Indicador é calculado com a seguinte fórmula: **TER = (QEQ / TTQ)* 100** Sendo: TER = Indicador de taxa de erro; TTQ = Quantidade total de quadros enviados ou recebidos em um determinado período; QEQ = Quantidade de erros identificados em um determinado período. Para efeito de mensuração desta métrica utiliza-se as seguintes considerações: • Quadro é a unidade de transferência de dados na camada de enlace do modelo OSI, ou seja, o frame Ethernet; • Os erros devem ser reportados pelo roteador da CONTRATADA utilizado na conexão com a rede da CONTRATANTE; • Serão considerados os erros em ambas as interfaces de ingresso e egresso no roteador da CONTRATADA.
Periodicidade de Aferição	Esta métrica deverá ser aferida, ininterruptamente, em intervalos de 5 minutos.
Limiar de Qualidade	0,5%
Pontos de Controle	O período utilizado no cálculo da métrica e, quando for o caso, o período considerado como indisponível será o do intervalo entre as aferições

MÉTRICA 3 - LATÊNCIA (IMR-03)	
Indicador de Qualidade	Tempo de latência de ida e volta do pacote através do link contratado
Métrica	A latência deve mensurar o tempo do trajeto de ida-e-volta (RTT - round trip time) de um pacote do tipo ICMP com tamanho de 1000 bytes. Para efeito de mensuração desta métrica utiliza-se as seguintes considerações: • Para os links Internet, as medições de latência devem ser feitas entre o Roteador Internet ou Appliance SD-WAN e o primeiro roteador da CONTATADA na Internet. • Pacote é a unidade de transferência de dados na camada de redes do modelo OSI, ou seja os datagramas TCP, UDP, ICMP e ARP; • O envio de pacotes para obtenção dos quantitativos utilizados no cálculo desta métrica deve ocorrer entre dois pontos distintos e remotos, um localizado no segmento de rede da CONTRATANTE onde estiver conectado o roteador da CONTRATADA, e outro localizado em segmento de rede de terceiros que estejam ligados a Internet por meio da rede da mesma CONTRATADA, ou em segmento de rede utilizado para troca de tráfego entre de operadoras de acesso à Internet (Pontos de Troca de Tráfego), podendo inclusive, tratar-se dos roteadores de borda da CONTRATADA conectados aos segmentos aqui mencionados. Serão desconsiderados os períodos em que os valores mensurados ultrapassem o limite aceitável desta métrica, caso a volume médio de utilização do link no mesmo período seja superior a 80% da velocidade do respectivo enlace.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

Mínimo aceitável	Links de Internet: 65 ms
Periodicidade Aferição	Esta métrica deverá ser aferida, ininterruptamente, em intervalos de 5 minutos. O período utilizado no cálculo da métrica será o período do intervalo entre as aferições

MÉTRICA 4 – PERDA DE PACOTES (IMR-04)	
Indicador de Qualidade	Percentual de perda de pacotes IP ao longo da rede da CONTRATADA em um determinado período.
Métrica	Indicador é calculado com a seguinte forma: **TPP = (QPP / QTP)* 100** Sendo: TPP = Indicador de perda de pacotes QTP = Quantidade total de pacotes enviados ou recebidos em um determinado período QPP = Quantidade de pacotes perdidos em um determinado período Para efeito de mensuração desta métrica utiliza-se as seguintes considerações: • Pacote é a unidade de transferência de dados na camada de redes do modelo OSI, ou seja os datagramas TCP, UDP, ICMP e ARP; • O envio de pacotes para obtenção dos quantitativos utilizados no cálculo desta métrica deve ocorrer entre dois pontos distintos e remotos, um localizado no segmento de rede da CONTRATANTE onde estiver conectado o roteador da CONTRATADA, e outro localizado em segmento de rede de terceiros que estejam ligados a Internet por meio da rede da mesma CONTRATADA, ou em segmento de rede utilizado para troca de tráfego entre de operadoras de acesso à Internet (Pontos de Troca de Tráfego), podendo inclusive, tratar-se dos roteadores de borda da CONTRATADA conectados aos segmentos aqui mencionados. Serão desconsiderados os períodos em que os valores mensurados ultrapassem o limite aceitável desta métrica, caso a volume médio de utilização do link no mesmo período seja superior a 80% da velocidade do respectivo enlace.
Máximo aceitável	3% de perda
Periodicidade Aferição	Esta métrica deverá ser aferida, ininterruptamente, em intervalos de 5 minutos. O período utilizado no cálculo da métrica será o período do intervalo entre as aferições.

MÉTRICA 5 – PRAZO PARA ALTERAÇÃO DE CONFIGURAÇÃO DOS EQUIPAMENTOS SOLICITADOS PELO CONTRATANTE	
Indicador de Qualidade	Prazo, em horas, para a contratada alterar a configuração dos equipamentos solicitada pelo CONTRATANTE.
Métrica	Apuração mensal do tempo que a contratada executa e apresente uma alteração na configuração de equipamentos, a partir do momento do registro da solicitação de alteração da configuração na base de dados relativa à solução de gerenciamento do Provedor e de comparação com o valor do Limiar de Qualidade desta tabela. **PA = Taa – Tsa** onde: PA = Prazo de alteração da configuração de equipamentos Taa = Instante da aceitação pela da alteração Tsa = Instante da solicitação da alteração
Periodicidade de Aferição	Mensal

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

Limiar de Qualidade	Prazo máximo: 48 horas após a solicitação de alteração da configuração pela CONTRATANTE. Em caso de agendamento pelo CONTRATANTE este prazo ficará suspenso.
Pontos de Controle	De acordo com os registros na Central de Atendimento.
Relatórios de Níveis de Serviço	A CONTRATADA deverá disponibilizar mensalmente à CONTRATANTE, relatórios com os índices apurados, totalizados e apresentados mensalmente por serviço. Nos relatórios citados deverão ser apresentados: o número do ticket, tempo de indisponibilidade (horas e minutos), o tempo de interrupções programadas, o tempo de interrupções de responsabilidade da CONTRATANTE.
Descontos	Para cada 1 (uma) hora acima do Prazo para Alteração de Configuração de Equipamentos (PAC), será implicado à contratada desconto correspondente a 2,0% (dois por cento), calculado sobre o valor mensal do circuito afetado. O referido desconto deverá ser retratado nos relatórios de prestação dos serviços, junto ao faturamento, apresentados mensalmente por enlace.

9.3. **Recebimento do Objeto**

9.3.1. A emissão do Termo de Recebimento Definitivo é o marco inicial da efetiva prestação do serviço contratado, nas condições em que foram definidas pela CONTRATANTE neste instrumento.

9.3.2. Os serviços serão recebidos provisoriamente, no prazo de até 3 (três) dias, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. (Art. 140, I, a , da Lei nº 14.133 e Arts. 22, X e 23, X do Decreto nº 11.246, de 2022);

9.3.2.1. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda do contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga;

9.3.2.2. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico. (Art. 22, X, Decreto nº 11.246, de 2022);

9.3.2.3. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo. (Art. 23, X, Decreto nº 11.246, de 2022)

9.3.2.4. O fiscal setorial do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo.

9.3.3. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato:

9.3.3.1. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

9.3.3.2. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório. (Art. 119 c/c art. 140 da Lei nº 14133, de 2021)

9.3.3.3. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

9.3.3.4. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

9.3.4. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

9.3.5. Os serviços serão recebidos definitivamente no prazo de 7(sete) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

9.3.5.1. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento (art. 21, VIII, Decreto nº 11.246, de 2022).

9.3.5.2. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções;

9.3.5.3. Emitir Termo Circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e

9.3.5.4. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

9.3.5.5. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão

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

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

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

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

9.3.9. Será permitido a emissão do Termo de Recebimento Definitivo, de forma individual, para serviço de Link de Internet WI-FI nas praças.

9.4. **Sanções Administrativas e Procedimentos Para Retenção ou Glosa no Pagamento**

9.4.1. **Descontos Aplicáveis em Caso de Descumprimento do IMR**

9.4.1.1. Durante a vigência do contrato poderão ser aplicados descontos na fatura, em caso de eventual descumprimento do Instrumento de Medição de Resultado (IMR), a título de glosa, limitando-se cada um ao limite do valor mensal do contrato.

9.4.1.2. Para fins de cálculo do valor do desconto de glosa contratual serão observados os critérios do **Item 9.1. Forma de Acompanhamento da Garantia e Níveis de Serviço**, nos termos do Instrumento de Medição de Resultado - IMR, aplicando os descontos correspondentes à disponibilidade mensal aferida, conforme a tabela abaixo:

LOTE	ITEM	SERVIÇO	FAIXA ATÉ 24H	FAIXA 24H ATÉ 48H	FAIXA ACIMA 48 H
1 (ÚNICO)	1	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN Sede (Alta Disponibilidade)	0,01% /min	0,02% /min	0,02% /min + multa moratória prevista no subitem 9.4.3.1
	2	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	0,01% /min	0,02% /min	0,02% /min + multa moratória prevista no subitem 9.4.3.1
	3	Serviço de Link dedicado de Acesso à internet, bloco /29 e Banda Mínima de Acesso Garantida de 500Mbps (Alta Disponibilidade) SEDE (Dois Link de ASN e Rota Diferentes)	0,01% /min	0,02% /min	0,02% /min + multa moratória prevista no subitem 9.4.3.1
	4 5	Serviço de Link de acesso à Internet Sites Remotos, aplica-se ao WIFI Social	0,009% /min	0,025% /min	0,025% /min

9.4.1.3. Em caso do não cumprimento da Métrica 5 do IMR o desconto será aplicado conforme abaixo:

MÉTRICA	FAIXA ATÉ 48H	FAIXA 48H ATÉ 72H	FAIXA ACIMA 72H
MÉTRICA 5 - Solicitação de alteração de configuração dos equipamentos - Prazo 48 horas	2,0% /hora	2,5% /hora	2,5% /hora + multa moratória prevista no subitem 9.4.3.1

9.4.1.4. Nos cálculos de desconto, em que a faixa for ultrapassada, todo o cálculo deverá ser feito na faixa posterior.

9.4.1.5. O valor do desconto será aplicado no mês imediatamente subsequente ao mês em que ocorreram os fatos causadores dos descontos, tendo como base o valor vigente do acesso do mês da ocorrência da interrupção.

9.4.1.6. Os descontos não poderão ultrapassar o valor do item do serviço prestado.

9.4.2. **Sanções Aplicáveis Fase de Instalação**

9.4.2.1. O atraso injustificado no cumprimento do objeto sujeitará a CONTRATADA às seguintes penalidades:

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

- Advertência;
- Multa moratória no valor de 1% do valor anual do contrato para o enlace, por dia de atraso, limitado a 10 dias, pelo atraso injustificado na entrega do projeto executivo, podendo ser adotadas medidas administrativas para rescisão contratual por inexecução total da obrigação. Entende-se por enlace/circuito como qualquer link Internet nos Sites Remotos e na Sede do CONTRATANTE;
- Multa moratória no valor de 1% do valor anual do contrato para o enlace, por dia de atraso, limitado a 30 dias, pelo atraso injustificado na instalação e configuração dos enlaces contratados, podendo ser adotadas medidas administrativas para rescisão contratual por inexecução total da obrigação. Entende-se por enlace/circuito como qualquer link Internet nos Sites Remotos e na Sede do CONTRATANTE.

9.4.3. **Sanções Aplicáveis Fase de Operação**

9.4.3.1. Caso a CONTRATADA ultrapasse a última faixa dos descontos aplicáveis, além da aplicação dos descontos, será imposta multa moratória de 1% do valor mensal do serviço não atendido no IMR, limitada a 10 dias.

9.4.3.2. A não manutenção das condições de habilitação da empresa ao longo da execução do contrato poderá ensejar sua rescisão unilateral pelo CONTRATANTE, após devido processo administrativo, assegurados o contraditório e a ampla defesa, além da aplicação de multa de 30% sobre o valor da parcela inadimplida.

9.4.3.3. A multa poderá ser aplicada cumulativamente com outras penalidades previstas no contrato ou na legislação vigente.

9.4.3.4. A inexecução total ou parcial do contrato poderá resultar em rescisão, nos termos deste instrumento e dos arts. 155 e 156 da Lei nº 14.133/21, incluindo indenização por eventuais prejuízos causados ao CONTRATANTE.

9.4.3.5. A aplicação das sanções será realizada mediante processo administrativo específico, assegurados o contraditório e a ampla defesa, com comunicação formal da penalidade à CONTRATADA.

9.4.3.5.1. A critério da autoridade competente, com base nos princípios da proporcionalidade e razoabilidade, as penalidades poderão ser atenuadas ou relevadas mediante comprovação fundamentada, desde que requeridas por escrito no prazo de 5 dias úteis a contar da notificação.

9.4.3.6. O atraso no pagamento de multas será corrigido pelo IPCA, divulgado pelo IBGE.

9.4.3.7. O CONTRATANTE registrará no SICAF todas as penalidades aplicadas à CONTRATADA.

9.4.4. **Sanções Administrativas**

9.4.4.1. Comete infração administrativa, nos termos da Lei nº 14.133/2021, a CONTRATADA que:

9.4.4.1.1. Der causa à inexecução parcial ou total do contrato, especialmente quando causar grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

9.4.4.1.2. Deixar de entregar documentação exigida no certame ou para a contratação;

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

9.4.4.1.3. Não manter a proposta, salvo por fato superveniente devidamente justificado;

9.4.4.1.4. Ensejar o retardamento injustificado da execução do objeto;

9.4.4.1.5. Apresentar declaração ou documentação falsa durante a licitação ou execução do contrato;

9.4.4.1.6. Fraudar a licitação ou praticar atos fraudulentos na execução do contrato;

9.4.4.1.7. Adotar comportamento inidôneo, praticar fraudes ou atos ilícitos visando frustrar os objetivos da licitação;

9.4.4.1.8. Praticar ato lesivo conforme o art. 5º da Lei nº 12.846/2013.

9.4.4.2. Pela inexecução total ou parcial do contrato, poderão ser aplicadas as seguintes sanções:

9.4.4.2.1. Advertência, quando não se justificar penalidade mais grave;

9.4.4.2.2. Multa, variando entre 0,5% e 30% do valor do contrato, conforme art. 155 da Lei nº 14.133/2021;

9.4.4.2.3. Impedimento de licitar e contratar, pelo prazo máximo de 3 anos, nos casos de infrações previstas nos incisos II a VII do art. 155 da Lei nº 14.133/2021, quando não for cabível penalidade mais severa;

9.4.4.2.4. Declaração de inidoneidade para licitar e contratar, pelo prazo de 3 a 6 anos, nos casos das infrações previstas nos incisos VIII a XII do art. 155 da Lei nº 14.133/2021, bem como naquelas previstas nos incisos II a VII que justifiquem penalidade mais grave.

9.4.4.3. Na aplicação das sanções, serão considerados:

9.4.4.3.1. A natureza e a gravidade da infração;

9.4.4.3.2. As peculiaridades do caso concreto;

9.4.4.3.3. Circunstâncias agravantes ou atenuantes;

9.4.4.3.4. Os danos causados à Administração Pública;

9.4.4.3.5. A existência de programa de integridade na empresa.

9.4.4.4. A sanção prevista no item 9.4.4.2.4. será precedida de análise jurídica observando as seguintes regras:

9.4.4.4.1. Quando aplicada por órgão do Poder Executivo, será de competência exclusiva de Ministro de Estado, Secretário Estadual ou Municipal, ou da autoridade máxima da autarquia ou fundação responsável;

9.4.4.4.2. Quando aplicada por órgãos dos Poderes Legislativo e Judiciário, Ministério Público ou Defensoria Pública, será de competência exclusiva de autoridade equivalente às referidas no item 9.4.4.4.1, conforme regulamento.

9.4.4.5. As sanções previstas nos itens 9.4.4.2.1., 9.4.4.2.3. e 9.4.4.2.4. poderão ser aplicadas cumulativamente com a prevista no item 9.4.4.2.2.

9.4.4.6. Se o valor das multas e indenizações exceder eventuais créditos da CONTRATADA junto à Administração, a diferença será descontada da garantia prestada ou cobrada judicialmente.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

9.4.4.7. A aplicação das sanções previstas nos itens 9.4.4.2.1., 9.4.4.2.2., 9.4.4.2.3. e 9.4.4.2.4. não exclui a obrigação de reparação integral dos danos causados à Administração.

9.4.4.8. A defesa quanto à aplicação das sanções previstas no item 9.4.4.2.2., poderá ser apresentada no prazo de 15 dias úteis a contar da intimação.

9.4.4.9. Para a aplicação das sanções previstas nos itens 9.4.4.2.3. e 9.4.4.2.4. será instaurado processo de responsabilização conduzido por comissão composta por, no mínimo, dois servidores estáveis, garantindo-se o direito à defesa no prazo de 15 dias úteis, nos termos do art. 158 da Lei nº 14.133/2021.

9.5. **Liquidação**

9.5.1. O faturamento mensal terá início somente após a emissão do Termo de Recebimento Definitivo, não sendo contada a fase de implantação do Item.

9.5.2. Para o serviço de Link de Internet nas localidades praças será permitido o faturamento após o Termo de Recebimento Definitivo de cada uma das unidades.

9.5.3. Durante a fase de prestação mensal a CONTRATANTE deverá validar minuciosamente as planilhas de memória de cálculo fornecidas pela CONTRATADA a fim de apurar os valores a serem faturados e os descontos aplicados, às planilhas de memória de cálculo deverão ser enviadas até o quinto dia após o fechamento do período de apuração.

9.5.4. CONTRATADA poderá optar por emitir a nota fiscal/fatura após a validação da memória de cálculo pela CONTRATANTE que terá prazo de 5 dias úteis para validação.

9.5.5. A CONTRATADA poderá emitir a nota fiscal/fatura com descontos apurados pela CONTRATADA e em caso de discordância dos descontos apurados por parte da CONTRATANTE, os descontos poderão ser aplicados na fatura do mês posterior.

9.5.6. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de 5 dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 6º, §1º do Decreto nº089/2024 .

9.5.6.1. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

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

a) o prazo de validade;
b) a data da emissão;
c) os dados do contrato e do órgão contratante;
d) o período respectivo de execução do contrato;
e) os descontos com mês referência;
f) o valor a pagar;
g) dados bancários para o recebimento do montante; e

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

h) eventual destaque do valor de retenções tributárias cabíveis.

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

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

9.5.10. A Administração deverá realizar consulta ao SICAF para:

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

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

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

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

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

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

9.6. **Prazo de pagamento**

9.6.1. O pagamento será efetuado no prazo de até 15 (quinze) dias úteis contados da finalização da liquidação da despesa, nos termos do art. 6º, §1º do Decreto nº089/2024.

9.7. **Forma de pagamento**

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

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

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

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

9.7.4. O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

9.8. **Reajuste**

9.8.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do Orçamento.

9.8.2. Após o interregno de um ano do orçamento estimado, mediante pedido expresso do contratado, os preços iniciais serão reajustados pelo contratante, mediante a aplicação do índice IPCA ou outro que reflita a inflação e seja mais vantajoso à Administração Pública Municipal, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

10. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

10.1. **Forma de seleção e critério de julgamento da proposta**

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

10.1.2. A presente aquisição adotará como regime de execução por preço unitário, a ser contratado mediante licitação, na modalidade Pregão Eletrônico, com lances abertos com intervalos mínimos entre lances de R$ 1,00 (um real) com valor de referência sigilos, levando em conta o objetivo da promoção de uma maior disputa entre os licitantes, com resultados satisfatórios para as empresas e o órgão público, considerando que o valor ultimado pelo mercado é variável, já que o referido objeto depende de tecnologias cada vez mais avançadas.

10.1.3. A presente licitação será julgada pelo critério de menor valor global, tendo em vista que o objeto consiste na contratação de empresa especializada para prestação de serviços de segurança cibernética com Inteligência Artificial Preditiva, garantindo alta disponibilidade, segurança, eficiência e sustentabilidade no atendimento às demandas do Município de Cáceres. Considerando a natureza integrada dos serviços, que envolvem soluções tecnológicas interdependentes, como conectividade segura, monitoramento preditivo, suporte técnico especializado e infraestrutura crítica de proteção de dados, a execução por um único fornecedor assegura a compatibilidade entre os componentes, a uniformidade dos padrões técnicos, a continuidade do serviço e a racionalização dos custos operacionais. Assim, a adoção do julgamento por valor global mostra-se técnica e economicamente mais vantajosa para a Administração Pública, promovendo a otimização dos recursos públicos e garantindo a eficiência na implementação da solução proposta.

10.1.4. É lícito o agrupamento em lotes de itens a serem contratados por meio de pregão, desde que possuam mesma natureza e que guardem relação entre si (Acórdão TCU nº 5.260/2011 – 1ª Câmara);

10.2. **Exigências de habilitação**

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

10.2.1.1. **Habilitação jurídica**

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

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

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

10.2.1.1.3. **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;

10.2.1.1.4. **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;

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

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

10.2.1.1.7. **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

10.2.1.1.8. **Sociedade cooperativa:** ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

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

10.2.1.2. **Habilitação fiscal, social e trabalhista**

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

10.2.1.2.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

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

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

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

10.2.1.2.6. Prova de regularidade com a Fazenda [Estadual/Distrital] e [Municipal/Distrital] do domicílio e sede do fornecedor, relativa à atividade em cujo exercício contrata e concorre;

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

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

10.2.1.3. **Qualificação Econômico-Financeira**

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

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

10.2.1.3.3. Índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), comprovados mediante a apresentação pelo licitante de balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais e obtidos pela aplicação das seguintes fórmulas:

I) Liquidez Geral (LG) = (Ativo Circulante + Realizável a Longo Prazo) / (Passivo Circulante + Passivo Não Circulante);

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

II) Solvência Geral (SG)= (Ativo Total) / (Passivo Circulante +Passivo não Circulante); e

III) Liquidez Corrente (LC) = (Ativo Circulante) / (Passivo Circulante).

10.2.1.3.4. 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] OU [patrimônio líquido mínimo] de 5% do valor total estimado do item.

10.2.1.4. **Qualificação Econômico-Financeira. (Justificativa)**

10.2.1.4.1. Ressalta-se que as exigências de habilitação relativas à qualificação econômico-financeira acima previstas e de acordo com o artigo 69 da Lei nº 14.133/21, têm a finalidade de viabilizar a aferição da situação financeira dos licitantes pela Administração. Dessa forma, será possível verificar se o interessado reúne condições indispensáveis para suportar as despesas relativas à satisfatória execução do objeto contratual, como dado objetivo de comprovação da qualificação econômico-financeira dos licitantes e para efeito de garantia ao adimplemento do contrato a ser ulteriormente celebrado, visando assegurar que a empresa contratada possa cumprir suas obrigações de curto e longo prazo, cumprindo as obrigações previstas no Edital e contrato, por se tratar de registro de preço o índice de 5% do valor de cada item, a Administração escolheu este valor por entender ser o mínimo a exigir de uma empresa para se manter um contrato, dentro de um nível de segurança e equilíbrio. Ademais, com o objetivo de não restringir o universo de concorrentes, resolveu não exigir valor acima da unidade. Ante o exposto, a exigência do Edital nada mais fez que traduzir em critérios objetivos o disposto no art. 37, XXI, da Constituição Federal, ademais, os índices escolhidos foram democráticos, na medida em que estabelecem um "mínimo" de segurança na contratação. Desta forma, atende plenamente a Lei Federal nº 14.133/21 limitando-se a exigir índices que demonstrem a capacidade financeira dos licitantes com vistas ao compromisso a ser assumido para plena execução do contrato.

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

10.2.1.4.3. O balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos. (Lei nº 14.133, de 2021, art. 69, §6º)

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

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

10.2.1.5. **Qualificação Técnica**

10.2.1.5.1. Apresentação de, no mínimo, 3 (três) Atestados de Capacidade Técnica, em nome da licitante, emitidos por pessoa jurídica de direito público ou privado, que comprovem o fornecimento e a instalação de equipamentos similares aos ofertados, bem como a prestação de serviços de instalação, configuração e suporte técnico. Tal exigência encontra amparo no inciso III do art. 67 da Lei nº 14.133/2021, sendo justificada pela complexidade e especificidade do objeto contratado, que demanda experiência comprovada na execução de soluções integradas de segurança cibernética com Inteligência Artificial Preditiva, visando garantir a eficiência, a continuidade dos serviços e a mitigação de riscos operacionais, em observância aos princípios da legalidade, eficiência e interesse público.

10.2.1.5.2. Os atestados devem especificar explicitamente a marca, os modelos e as quantidades fornecidas, comprovando a experiência da licitante em projetos de porte e natureza semelhantes.

10.2.1.5.3. A licitante deve comprovar que dispõe de, no mínimo, dois (02) técnicos certificados pelo fabricante da solução proposta, os quais participarão diretamente da execução dos serviços previstos.

10.2.1.5.4. As certificações devem ser reconhecidas pelo fabricante e estar atualizadas, garantindo conhecimento técnico adequado às demandas do projeto.

10.2.1.5.5. O fornecedor deve fornecer todas as informações e documentos necessários para validar a legitimidade dos atestados apresentados, incluindo:

- Cópia do contrato que deu origem à prestação dos serviços mencionados nos atestados;
- Endereço atual da contratante que emitiu o atestado;
- Local onde os serviços foram executados;
- Outros documentos complementares, se solicitados pela Administração.

10.2.1.5.6. A licitante deve comprovar experiência em projetos de complexidade e escopo semelhantes, preferencialmente na área pública ou em ambientes corporativos de grande porte, apresentando histórico de projetos realizados com soluções NGFW, SD-WAN e links de redundância.

10.2.1.5.7. A licitante deverá demonstrar a capacidade técnica necessária para atender aos requisitos específicos do projeto, incluindo:

- Disponibilidade de suporte técnico especializado durante todo o período contratual;
- Experiência em integrar soluções de segurança em redes heterogêneas e complexas;

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

- Conhecimento comprovado em tecnologias de alta disponibilidade, criptografia e gestão de redes com políticas de segurança.

10.2.1.5.8. Sempre que solicitado pela Administração, a licitante deverá apresentar documentação adicional que comprove a qualificação técnica e a capacidade operacional para executar o objeto contratado, garantindo transparência e segurança no processo de contratação.

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

11.1. O custo estimado da contratação possui caráter sigiloso e será tornado público apenas e imediatamente após o julgamento das propostas nos termos do Art. 9º do Decreto municipal 240/23.

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

12. DA PARTICIPAÇÃO DE CONSORCIO

12.1. Trata-se da vedação da participação de consórcios quanto ao registro de preços para CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA PRESTAÇÃO DE SERVIÇOS DE SEGURANÇA CIBERNÉTICA COM INTELIGÊNCIA ARTIFICIAL PREDITIVA, GARANTINDO ALTA DISPONIBILIDADE, SEGURANÇA, EFICIÊNCIA E SUSTENTABILIDADE NO ATENDIMENTO ÀS DEMANDAS DO MUNICÍPIO DE CÁCERES.

12.2. Art. 14 da Lei 14.133/21, conferiu a discricionaridade à Administração para permitir ou vetar a formação de consórcio em certame licitatório. É sabido que, em regra, a formação de consórcio é admitida quando o objeto a ser licitado envolve questões de alta complexidade técnica ou de relevante vulto, em que, isoladamente, as empresas não teriam condições de suprir os requisitos de habilitação do edital.

12.3. Tratando-se do objeto em questão, a ausência de consórcio não trará prejuízos à competitividade do certame por se tratar de um registro de preços, de serviços comuns, a ser executado ao longo de 12 (doze) meses em sua totalidade ou não, que não demandam especialidades diferentes entre as empresas, as quais poderiam impedir à execução dos serviços por uma única empresa. É nítido, neste caso também que, a reunião de empesas em consórcio, ao invés de estabelecer uma disputa entre as empresas, as mesmas formalizariam acordo para eliminar a competição caso estivessem reunidas em consórcio.

12.4. Diante de todo o exposto e, considerando que existem diversas empresas com capacidade para fornecer os serviços a serem contratados facilmente comprovados através do número de cotações inseridas no processo, fica vedada à participação de consórcios na licitação.

13. ADESÃO A ATA DE REGISTRO DE PREÇO

13.1. Em conformidade com a Lei nº 14.133/2021, a Lei nº 14.770/2023 e demais regulamentos aplicáveis, a adesão à Ata de Registro de Preços (ARP) configura-se como mecanismo de cooperação interfederativa, baseado na

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

manifestação de interesse mútuo entre os entes públicos. Tal procedimento visa proporcionar maior eficiência administrativa e econômica, especialmente diante das dificuldades enfrentadas por órgãos e entidades para realizar processos licitatórios frequentes, seja por limitações de pessoal, infraestrutura ou outras razões justificáveis.

13.2. A adesão à ARP pelos demais entes federados será viabilizada desde que respeitados os limites quantitativos previstos no instrumento convocatório e nas legislações mencionadas, bem como observadas as condições estabelecidas neste Termo de Referência. A formalização da adesão deverá ocorrer mediante solicitação formal do ente interessado, acompanhada da anuência do órgão gerenciador e da CONTRATADA, conforme exigido pela legislação vigente.

13.3. A adesão não poderá resultar em prejuízo ao fornecimento ou à prestação dos serviços destinados ao órgão gerenciador e demais participantes da ARP. Caso o volume decorrente das adesões comprometa o atendimento das quantidades inicialmente previstas, a CONTRATADA deverá priorizar o fornecimento ao órgão gerenciador e aos participantes originais, conforme os prazos e condições estabelecidos neste instrumento.

13.4. Os entes federados que aderirem à ARP assumem integral responsabilidade pela gestão e fiscalização dos contratos celebrados diretamente com a CONTRATADA, sem qualquer interferência ou solidariedade do órgão gerenciador. Caberá ao ente aderente zelar pelo cumprimento das obrigações pactuadas, inclusive no que se refere às condições de pagamento, prazos de entrega e demais cláusulas contratuais.

13.5. O órgão gerenciador poderá, a qualquer tempo, solicitar relatórios à CONTRATADA para acompanhar as adesões realizadas, garantindo o cumprimento dos limites quantitativos e demais disposições legais aplicáveis. Eventuais irregularidades deverão ser comunicadas ao órgão gerenciador, que adotará as providências cabíveis em conformidade com a legislação vigente.

14. ADEQUAÇÃO ORÇAMENTÁRIA

14.1. As despesas oriundas da presente aquisição correrão por conta de todas as dotações vigentes, conforme especificado pelas Secretarias no momento do empenho.

FICHA	ÓRGÃO UNIDADE	FUNCIONAL PROGRAMÁTICA	NATUREZA DE DESPESA	FONTE DE RECURSOS	SECRETARIA
243	020201	04 126 1002 2014 0000	3.3.90	1.1.500	SMEAE
233	020201	04 122 1002 2012 0000	3.3.90	1.1.500	SMEAE

Cáceres-MT, 16 de maio 2025.

GIRLANE VIEIRA PEREIRA
Coordenadora de Informações Sistêmicas e Tecnologia de Informação

JEREMIAS PEREIRA LEITE
Secretário Municipal Especial de Assuntos Estratégicos

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02 e informe o código 37F7-8C4F-BD72-1A02

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: 37F7-8C4F-BD72-1A02

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

✓ JEREMIAS PEREIRA LEITE (CPF 045.XXX.XXX-72) em 27/05/2025 09:48:54 GMT-04:00
Papel: Parte
Emitido por: AC SOLUTI Multipla v5 << AC SOLUTI v5 << Autoridade Certificadora Raiz Brasileira v5 (Assinatura ICP-Brasil)

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

https://caceres.1doc.com.br/verificacao/37F7-8C4F-BD72-1A02

De: GIRLANE P. - SMA

Para: SMA-CPL - Comissão Permanente de Licitação

Data: 26/05/2025 às 16:14:20

_

Girlane Vieira Pereira

Coordenadora de Informações Sistêmicas e Tecnologia de Informação

De: Igor O. - SMA-CPL

Para: SMEAE - Secretaria Municipal Especial de Assuntos Estratégicos

Data: 26/05/2025 às 16:17:25

Senhor Secretário,

Segue em anexo edital de abertura referente ao pregão eletrônico 15/2025, com o número 90015/2025 no compras.gov.br, abertura prevista para o dia 11/06/2025.

Atenciosamente;

_

Igor de Souza Oliveira
Pregoeiro Oficial

Anexos:

EDITAL_PE_15_2025_FIREWALL.pdf

Assinado digitalmente (anexos) por:

Assinante	Data	Assinatura	
Jeremias Pereira Leite	26/05/2025 16:41:49	ICP-Brasil	JEREMIAS PEREIRA LEITE CPF 045.XXX.XXX-72

Para verificar as assinaturas, acesse **https://caceres.1doc.com.br/verificacao/** e informe o código: **D822-BE8B-F69C-28C2**

EDITAL PREGÃO ELETRÔNICO N° 15/2025
(Processo Administrativo n° 29/2025)
Número da licitação no compras.gov.br 90015/2025

Torna-se público, para conhecimento dos interessados, que a PREFEITURA MUNICIPAL DE CÁCERES, por meio da SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO, sediada na AV. BRASIL, 119, COC, BAIRRO JARDIM CELESTE, realizará licitação, para registro de preços, na modalidade PREGÃO, na forma ELETRÔNICA, **com critério de julgamento menor preço global, modo de disputa aberto**, nos termo da lei n.º 14.133 de 2021 e demais legislação aplicável e de acordo com as condições estabelecidas neste Edital.

Data da sessão: 11 de junho de 2025
Horário: 09h00min horário de Brasília
Portal de Compras do Governo Federal: compras.gov.br
UASG: 989047

1. DO OBJETO

Registro de Preço para futura e eventual contratação de empresa especializada para prestação de serviços de segurança cibernética com Inteligência Artificial Preditiva, garantindo alta disponibilidade, segurança, eficiência e sustentabilidade no atendimento às demandas do Município de Cáceres, conforme condições e exigências estabelecidas neste instrumento.

1.2. A licitação será dividida em itens, conforme tabela constante do Termo de Referência, facultando-se ao licitante a participação em quantos itens for de seu interesse.

1.3. O critério de julgamento adotado será o menor preço por item, observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto. **Havendo qualquer divergência entre a especificação do CATSER e a deste Edital, prevalecerá a especificação deste Edital.**

2. DOS REGISTROS DE PREÇOS.

2.1. As regras referentes aos órgãos gerenciador e participante, bem como a eventuais adesões são as que constam da minuta de Ata de Registro de Preços.

2.2 Será admitida a adesão à ata de registro de preços decorrente desta licitação , conforme lei 14.133/2021 e 14.770/2023.

3. DO CREDENCIAMENTO.

3.1. O Credenciamento é o nível básico do registro cadastral no SICAF, que permite a participação dos interessados na modalidade licitatória Pregão, em sua forma eletrônica.

3.2. O cadastro no SICAF deverá ser feito no Portal de Compras do Governo Federal, no sítio **compras.gov.br** por meio de certificado digital conferido pela Infraestrutura de Chaves Pública Brasileira – ICP - Brasil.

3.3. O credenciamento junto ao provedor do sistema implica a responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes a este Pregão.

3.4. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluídos a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

3.5. É de responsabilidade de o cadastrado conferir a exatidão dos seus dados cadastrais no SICAF e mantê- los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

3.5.1. A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação.

4. DA PARTICIPAÇÃO NO PREGÃO

4.1. Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal(**compras.gov.br**), por meio de Certificado Digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil.

4.1.1. Os interessados deverão atender às condições exigidas no cadastramento no Sicaf até o terceiro dia útil anterior à data prevista para recebimento das propostas.

4.2. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

4.3. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais nos Sistemas relacionados no item anterior e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

4.4. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

4.4.1. Não poderão disputar esta licitação:

4.4.2. Aquele que não atenda às condições deste Edital e seu(s) anexo(s);

4.4.3. pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

4.4.4. 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 do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

4.4.5. Empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

4.4.6. 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;

4.4.7. Pessoas jurídicas reunidas em consórcio;

4.4.8. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

4.4.9. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato 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 n.º 14.133, de 2021.

4.5. O impedimento de que trata **o item 4.5.3** 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. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

5.1. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço ou o percentual de desconto, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública.

5.2. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:

5.3. Está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

5.4. Não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

5.5. Não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal.

5.6. Cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

5.7. O licitante organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021.

5.8. O fornecedor enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021.

5.9. No item exclusivo para participação de microempresas e empresas de pequeno porte, a assinalação do campo "não" impedirá o prosseguimento no certame, para aquele item;

5.10. Nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte a assinalação do campo "não" apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006 mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.

5.11. A falsidade da declaração de que trata os itens 5.7 ou 5.8 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

5.12. Os licitantes poderão retirar ou substituir a proposta ou, na hipótese de a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, os documentos de habilitação anteriormente inseridos no sistema, até a abertura da sessão pública.

5.13. Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

5.14. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.

5.15. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo quando do cadastramento da proposta e obedecerá às seguintes regras:

5.16. A aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta;

5.17. Os lances serão de envio automático pelo sistema, respeitado o valor final mínimo estabelecido e o intervalo de que trata o subitem acima.

5.18. O valor final mínimo ou o percentual de desconto final máximo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

5.18.1. Palor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço; e

5.18.2. Percentual de desconto inferior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por maior desconto

5.18.3. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

5.19. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

6. DO PREENCHIMENTO DA PROPOSTA

6. 1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

6.1.1. Valor unitário e total;

6.1.2. Marca (quando for o caso);

6.1.3. Descrição do objeto, contendo as informações similares à especificação do Termo de Referência;

6.2. Todas as especificações do objeto contidas na proposta vinculam o licitante;

6.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, , tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

6.4. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto;

6.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, , a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses;

6.6. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos, na fonte os percentuais estabelecidos na legislação vigente.

6.7. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

6.8. O prazo de validade da proposta não será inferior a 60(sessenta) dias, a contar da data de sua apresentação.

6.9. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas, quando participarem de licitações públicas.

6.10. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização pelo Tribunal de Contas da União e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

7. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES.

7.1. A abertura da presente licitação dar-se-á em sessão pública, por meio de sistema eletrônico, na data, horário e local indicado neste Edital.

7.2. Os licitantes poderão retirar ou substituir a proposta ou os documentos de habilitação, quando for o caso, anteriormente inseridos no sistema, até a abertura da sessão pública.

7.2.1. Serão aceitos somente lances em moeda corrente nacional (R$), com no máximo 02 (duas) casas decimais, considerando as quantidades constantes no TERMO DE REFERENCIA (anexo I) do presente edital.

7.2.2. Também será desclassificada a proposta que identifique o licitante.

7.2.3. A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

7.2.4. A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.

7.3. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

7.4. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

7.5. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

7.5.1. O lance deverá ser ofertado pelo valor unitário do item.

7.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

7.7. O licitante somente poderá oferecer lance de valor inferior ou percentual de desconto superior ao último por ele ofertado e registrado pelo sistema.

7.8. Será adotado para o envio de lances no pregão eletrônico o modo de disputa "aberto", em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

7.8.1. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de de R$ 0,01(um centavo) com valor de referência sigilos.

7.8.2. O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

7.9. A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

7.10. A prorrogação automática da etapa de lances, de que trata o item anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

7.11. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

7.11.1. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

7.11.2. Após o reinício previsto no item supra, os licitantes serão convocados para apresentar lances intermediários.

7.12. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

7.13. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

7.14. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

7.15. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

7.16. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

7.17. A melhor classificada nos termos do subitem anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

7.17.1. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

7.17.2. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

7.18. Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

7.18.1.1. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133, de 2021, nesta ordem:

7.18.1.2. Disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

7.18.1.3. Avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos nesta Lei;

7.18.1.4. Desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;

7.18.1.5. Desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

7.18.2. Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

7.18.2.1. Empresas estabelecidas no território do Estado ou do Distrito Federal do órgão ou entidade da Administração Pública estadual ou distrital licitante ou, no caso de licitação realizada por órgão ou entidade de Município, no território do Estado em que este se localize;

7.18.2.2. Empresas brasileiras;

7.18.2.3. Empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

7.18.2.4. Empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de dezembro de 2009.

7.19. Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo ou inferior ao desconto definido para a contratação, o pregoeiro poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

7.19.1. A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela Administração.

7.19.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

7.19.3. O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório

7.20. O pregoeiro solicitará ao licitante mais bem classificado que, no prazo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

7.21. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

7.22. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

8. DA FASE DE JULGAMENTO

8.1. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e no item 21 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

a) SICAF;

b) Cadastro Nacional de Empresas Inidôneas e Suspensas CEIS, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/ceis); e

C) Cadastro Nacional de Empresas Punidas – CNEP mantido pela Controladoria -Geral da União (https://www.portaltransparencia.gov.br/sancoes/cnep)

8.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei n° 8.429, de 1992.

8.3. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas. (IN nº 3/2018, art. 29, caput).

8.4. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros. (IN nº 3/2018, art. 29, §1º).

8.5. O licitante será convocado para manifestação previamente a uma eventual desclassificação. (IN nº 3/2018, art. 29, §2º).

8.6. Constatada a existência de sanção, o licitante será reputado inabilitado, por falta de condição de participação.

8.7. Caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

8.8. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício, em conformidade com o item 4.6 deste edital.

8.9. Verificadas as condições de participação e de utilização do tratamento favorecido, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no artigo 29 a 35 da IN SEGES nº 73, de 30 de setembro de 2022.

8.10. Será desclassificada a proposta vencedora que:

8.10.1.1. contiver vícios insanáveis;

8.10.1.2. não obedecer às especificações técnicas contidas no Termo de Referência;

8.10.1.3. apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

8.10.1.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

8.10.1.5. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

8.10.2.1. No caso de bens e serviços em geral, é indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

8.10.2.2. A inexequibilidade, na hipótese de que trata o **caput**, só será considerada após diligência do pregoeiro, que comprove:

8.10.2.3. Que o custo do licitante ultrapassa o valor da proposta; e

8.10.2.4. Inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

8.11. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a exequibilidade da proposta.

8.12. Erros no preenchimento da proposta não constituem motivo para a desclassificação da proposta. A proposta poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço.

8.12.1. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas;

8.12.2. Considera-se erro no preenchimento da proposta passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

8.13. Caso o Termo de Referência exija a apresentação de amostra, o licitante classificado em primeiro lugar deverá apresentá-la, conforme disciplinado no Termo de Referência, sob pena de não aceitação da proposta.

8.14. Por meio de mensagem no sistema, será divulgado o local e horário de realização do procedimento para a avaliação das amostras, cuja presença será facultada a todos os interessados, incluindo os demais licitantes.

8.15. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

8.16. No caso de não haver entrega da amostra ou ocorrer atraso na entrega, sem justificativa aceita pelo Pregoeiro, ou havendo entrega de amostra fora das especificações previstas neste Edital, a proposta do licitante será recusada.

8.16.1. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas;

8.16.2. Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

8.17. Caso o Termo de Referência exija a apresentação de amostra, o licitante classificado em primeiro lugar deverá apresentá-la, conforme disciplinado no Termo de Referência, sob pena de não aceitação da proposta.

8.18. Por meio de mensagem no sistema, será divulgado o local e horário de realização do procedimento para a avaliação das amostras, cuja presença será facultada a todos os interessados, incluindo os demais licitantes.

8.19. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

8.20. No caso de não haver entrega da amostra ou ocorrer atraso na entrega, sem justificativa aceita pelo Pregoeiro, ou havendo entrega de amostra fora das especificações previstas neste Edital, a proposta do licitante será recusada.

8.20.1. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas;

8.20.2. Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

8.21. Caso o Termo de Referência exija a apresentação de amostra, o licitante classificado em primeiro lugar deverá apresentá-la, conforme disciplinado no Termo de Referência, sob pena de não aceitação da proposta.

8.22. Por meio de mensagem no sistema, será divulgado o local e horário de realização do procedimento para a avaliação das amostras, cuja presença será facultada a todos os interessados, incluindo os demais licitantes.

8.23. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

8.24. No caso de não haver entrega da amostra ou ocorrer atraso na entrega, sem justificativa aceita pelo Pregoeiro, ou havendo entrega de amostra fora das especificações previstas neste Edital, a proposta do licitante será recusada.

8.25. Se a(s) amostra(s) apresentada(s) pelo primeiro classificado não for(em) aceita(s), o Pregoeiro analisará a aceitabilidade da proposta ou lance ofertado pelo segundo classificado Seguir-se-á com a verificação da(s) amostra(s) e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no Termo de Referência.

9. DA FASE DE HABILITAÇÃO

9.1. Os documentos previstos no Termo de Referência, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021.

9.2. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, poderá ser substituída pelo registro cadastral no SICAF.

9.3. Na hipótese de o licitante vencedor ser empresa estrangeira que não funcione no País, para fins de assinatura do contrato ou da ata de registro de preços, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

9.4. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas na forma da lei (art. 63, I, da Lei nº 14.133/2021)

9.5. O licitante deverá apresentar, sob pena de desclassificação, declaração de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

9.6. A habilitação será verificada por meio do Sicaf, nos documentos por ele abrangidos.

9.6.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir. (IN nº 3/2018, art. 4º, §1º, e art. 6º, §4º).

9.6. É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no Sicaf e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados. (IN nº 3/2018, art. 7º, *caput*).

9.7. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

9.7.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de ***[NO MÍNIMO, DUAS HORAS]***, prorrogável por igual período, contado da solicitação do pregoeiro.

9.8. A verificação no Sicaf ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante vencedor.

9.8.1. Os documentos relativos à regularidade fiscal que constem do Termo de Referência somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

9.9. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para (Lei 14.133/21, art. 64, e IN 73/2022, art. 39, §4º):

9.9.1. Complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

9.9.2. Atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;

9.10. Na análise dos documentos de habilitação, o pregoeiro poderá sanar erros ou falhas, que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

9.11. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital, observado o prazo disposto no edital.

9.12. Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.

9.13. A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte somente será exigida para efeito de contratação, e não como condição para participação na licitação (art. 4º do Decreto nº 8.538/2015).

9.14. **Habilitação jurídica:**

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

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

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

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

9.14.5. **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;

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

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

9.14.8. **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

9.14.9. **Sociedade cooperativa:** ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

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

9.15. **Regularidade fiscal e trabalhista:**

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

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

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

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

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

9.15.6. Prova de regularidade com a Fazenda [Estadual/Distrital] e [Municipal/Distrital] do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre.

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

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

9.16. **Qualificação Econômico-Financeira.**

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

9.16.2. Certidão Negativa de Falência e Concordata expedida pelo distribuidor da sede da pessoa jurídica, datada de, no máximo, 30 (trinta) dias antes da data da abertura do certame, caso não apresente o seu prazo de validade.

Obs: Caso a Certidão seja Positiva de Recuperação, deverá a empresa apresentar a comprovação que seu Plano de Recuperação foi acolhido judicialmente, na forma do Art. 58 da Lei nº 11.101/2005, sob pena de inabilitação.

9.16.3. Atenção: Senhores licitantes, ao solicitar as Certidões de Falência e Concordata, ou Recuperação Judicial ou Extrajudicial, perante o Poder Judiciário do Estado De Mato Grosso, devem ser selecionadas as opções AUTOR e RÉU, para o cumprimento do Art. 69, II da Lei nº 14.133/2021. Para os licitantes dos demais estados, caso não contenha os termos acima, deverão certificar que as certidões expedidas em suas comarcas atestam a inexistência de ações de Falência e Concordata movidas ou em desfavor da empresa solicitante. Podendo o Agente de Contratação e/ou Pregoeiro realizar diligência a fim de verificar o atendimento da Lei Federal nº 14.133/2021, em vistas do art. 97 da Lei nº 11.101/05.

9.16.4. Índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), comprovados mediante a apresentação pelo licitante de **balanço patrimonial na forma da lei** e demais demonstrações contábeis **dos 2 (dois) últimos exercícios sociais** e obtidos pela aplicação das seguintes fórmulas:
I - Liquidez Geral (LG) = (Ativo Circulante + Realizável a Longo Prazo)/(Passivo Circulante + Passivo Não Circulante);II - Solvência Geral (SG)= (Ativo Total)/(Passivo Circulante +Passivo não Circulante); e III - Liquidez Corrente (LC) = (Ativo Circulante)/(Passivo Circulante).

9.16.5. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC)), será exigido para fins de habilitação [patrimônio líquido mínimo] de 5% do valor total de cada item.

9.16.6. 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).

9.16.7. O balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos. (Lei nº 14.133, de 2021, art. 69, §6º).

9.17. Qualificação Técnica

9.17.1. Comprovação de aptidão para o fornecimento de bens em características, compatíveis com o objeto desta licitação, ou com o item pertinente, por meio da apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado.

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

9.17.3. A existência de restrição relativamente à regularidade fiscal e trabalhista não impede que a licitante qualificada como microempresa ou empresa de pequeno porte seja declarada vencedora, uma vez que atenda a todas as demais exigências do edital.

9.17.4. A declaração do vencedor acontecerá no momento imediatamente posterior à fase de habilitação.

9.17.5. Caso a proposta mais vantajosa seja ofertada por licitante qualificada como microempresa ou empresa de pequeno porte, e uma vez constatada a existência de alguma restrição no que tange à regularidade fiscal e trabalhista, a mesma será convocada para, no prazo de 5 (cinco) dias úteis, após a declaração do vencedor, comprovar a regularização. O prazo poderá ser prorrogado por igual período, a critério da administração pública, quando requerida pelo licitante, mediante apresentação de justificativa.

9.17.6. A não-regularização fiscal e trabalhista no prazo previsto no subitem anterior acarretará inabilitação do licitante, sem prejuízo das sanções previstas neste Edital, sendo facultada a convocação dos licitantes remanescentes, na ordem de classificação. Se, na ordem de classificação, seguir-se outra microempresa, empresa de pequeno porte ou sociedade cooperativa com alguma restrição na documentação fiscal e trabalhista, será concedido o mesmo prazo para regularização.

9.17.7. Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no "chat" a nova data e horário para a continuidade da mesma.

9.17.8. Será inabilitado o licitante que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste Edital.

9.17.9. Nos itens não exclusivos a microempresas e empresas de pequeno porte, em havendo inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

9.17.10. O licitante provisoriamente vencedor em um item, que estiver concorrendo em outro item, ficará obrigado a comprovar os requisitos de habilitação cumulativamente, isto é, somando as exigências do item em que venceu às do item em que estiver concorrendo, e assim sucessivamente, sob pena de inabilitação, além da aplicação das sanções cabíveis.

9.17.11. Não havendo a comprovação cumulativa dos requisitos de habilitação, a inabilitação recairá sobre o(s) itens de menor(es) valor(es) cuja retirada(s) seja(m) suficiente(s) para a habilitação do licitante nos remanescentes.

9.17.12. Constatado o atendimento às exigências de habilitação fixadas no Edital, o licitante será declarado vencedor.

10. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

10.1. A proposta final do licitante declarado vencedor deverá ser encaminhada no prazo de 2 (duas) horas, a contar da solicitação do Pregoeiro no sistema eletrônico e deverá:

10.1.1. Ser redigida em língua portuguesa, datilografada ou digitada, em uma via, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada e as demais rubricadas pelo licitante ou seu representante legal.

10.1.2. Conter a indicação do banco, número da conta e agência do licitante vencedor, para fins de pagamento.

10.2. A proposta final deverá ser documentada nos autos e será levada em consideração no decorrer da execução do contrato e aplicação de eventual sanção à Contratada, se for o caso.

10.2.1. Todas as especificações do objeto contidas na proposta, tais como marca, modelo, tipo, fabricante e procedência, vinculam a Contratada.

10.3. Os preços deverão ser expressos em moeda corrente nacional, o valor unitário em algarismos e o valor global em algarismos e por extenso.

10.3.1. Ocorrendo divergência entre os preços unitários e o preço global, prevalecerão os primeiros; no caso de divergência entre os valores numéricos e os valores expressos por extenso, prevalecerão estes últimos.

10.4. A oferta deverá ser firme e precisa, limitada, rigorosamente, ao objeto deste Edital, sem conter alternativas de preço ou de qualquer outra condição que induza o julgamento a mais de um resultado, sob pena de desclassificação.

10.5. A proposta deverá obedecer aos termos deste Edital e seus Anexos, não sendo considerada aquela que não corresponda às especificações ali contidas ou que estabeleça vínculo à proposta de outro licitante.

10.6. As propostas que contenham a descrição do objeto, o valor e os documentos complementares estarão disponíveis na internet, após a homologação.

11. DOS RECURSOS

11.6. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021.

11.7. O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata.

ório - 029/2025 | [illegible]

11.8. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:

11.8.1. A intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;

11.8.2. O prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

11.8.3. Na hipótese de adoção da inversão de fases prevista no § 1º do art. 17 da Lei nº 14.133, de 2021, o prazo para apresentação das razões recursais será iniciado na data de intimação da ata de julgamento.

11.9. Os recursos deverão ser encaminhados em campo próprio do sistema.

11.10. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

11.11. Os recursos interpostos fora do prazo não serão conhecidos.

11.12. O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de 3 (três) dias úteis, contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.

11.13. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

11.14. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

11.15. Os autos do processo permanecerão com vista franqueada aos interessados no sítio eletrônico licitacao@caceres.gov.mt.br.

12. DA REABERTURA DA SESSÃO PÚBLICA

12.1. A sessão pública poderá ser reaberta:

12.1.1. Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.

12.1.2. Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal

e trabalhista, nos termos do art. 43, §1º da LC nº 123/2006. Nessas hipóteses, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

12.2. Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.

12.2.1. A convocação se dará por meio do sistema eletrônico ("chat"), e-mail, ou, ainda, fac-símile, de acordo com a fase do procedimento licitatório.

12.2.2. A convocação feita por e-mail ou fac-símile dar-se-á de acordo com os dados contidos no SICAF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

13. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

13.1. Encerradas as fases e julgamento e habilitação, e exauridos os recursos adminitrativos, o ,processo licitatório será encaminhada à autoridade superior para adjudicar o objeto e homologar o procedimento, observado no art. 71 da lei n.º 14.133, de 2021.

14. DA GARANTIA DA EXECUÇÃO

14.1 Não será exigida a prestação de garantia na presente contratação, Termo de Referência.

15. A ATA DE REGISTRO DE PREÇOS

15.1. Homologado o resultado da licitação, terá o adjudicatário o prazo de 2 (dois) dias, contados a partir da data de sua convocação, para assinar a Ata de Registro de Preços, cujo prazo de validade encontra-se nela fixado, sob pena de decair do direito à contratação.

15.2. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura da Ata de Registro de Preços, a Administração poderá encaminhá-la para assinatura,meio eletrônico, para que seja assinada e devolvida no prazo de 2 (dois) dias, a contar da data de seu recebimento.

15.3. O prazo estabelecido no subitem anterior para assinatura da Ata de Registro de Preços poderá ser prorrogado uma única vez, por igual período, quando solicitado pelo(s) licitante(s) vencedor(s), durante o seu transcurso, e desde que devidamente aceito.

15.4. Serão formalizadas tantas Atas de Registro de Preços quanto necessárias para o registro de todos os itens constantes no Termo de Referência, com a indicação do licitante vencedor, a descrição do(s) item(ns), as respectivas quantidades, preços registrados e demais condições.

15.5. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades legalmente estabelecidas e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação.

16. DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE

16.1. Após a homologação da licitação, em sendo realizada a contratação, será firmado Termo de Contrato ou emitido instrumento equivalente.

16.2.1. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato ou aceite do instrumento equivalente, a Administração poderá encaminhá-lo para assinatura ou aceite da Adjudicatária, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinado ou aceito no prazo de 3 (três) dias, a contar da data de seu recebimento.

16.2.2. O prazo previsto no subitem anterior poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

16.3. O Aceite da Nota de Empenho ou do instrumento equivalente, emitida à empresa adjudicada, implica no reconhecimento de que:

16.3.2. A contratada se vincula à sua proposta e às previsões contidas no edital e seus anexos;

16.5. Previamente à contratação a Administração realizará consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018, e nos termos do art. 6º, III, da Lei nº 10.522, de 19 de julho de 2002, consulta prévia ao CADIN.

16.5.2. Na hipótese de irregularidade do registro no SICAF, o contratado deverá regularizar a sua situação perante o cadastro no prazo de até 05 (cinco) dias úteis, sob pena de aplicação das penalidades previstas no edital e anexos.

16.6. Na assinatura do contrato ou da ata de registro de preços, será exigida a comprovação das condições de habilitação consignadas no edital, que deverão ser mantidas pelo licitante durante a vigência do contrato ou da ata de registro de preços.

16.7. Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no edital ou se recusar a assinar o contrato ou a ata de registro de preços, a Administração, sem prejuízo da aplicação das sanções das demais cominações legais cabíveis a esse licitante, poderá convocar outro licitante, respeitada a ordem de classificação, para, após a comprovação dos requisitos para habilitação, analisada a proposta e eventuais documentos complementares e, feita a negociação, assinar o contrato ou a ata de registro de preços.

17. DO REAJUSTAMENTO EM SENTIDO GERAL

17.1. As regras acerca do reajustamento em sentido geral do valor contratual são as estabelecidas no Termo de Referência, anexo a este Edital.

18. DO RECEBIMENTO DO OBJETO E DA FISCALIZAÇÃO

18.1. Os critérios de recebimento e aceitação do objeto e de fiscalização estão previstos no Termo de Referência.

19. DO RECEBIMENTO DO OBJETO E DA FISCALIZAÇÃO

19.1. As obrigações da Contratante e da Contratada são as estabelecidas no Termo de Referência.

20. DO PAGAMENTO

20.1. As regras acerca do pagamento são as estabelecidas no Termo de Referência, anexo a este Edital.

21. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

21.6. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:

21.6.1. Deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a pregoeiro/a durante o certame;

21.6.2. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:

21.6.2.1. Não enviar a proposta adequada ao último lance ofertado ou após a negociação;

21.6.2.2. Recusar-se a enviar o detalhamento da proposta quando exigível;

21.6.2.3. Pedir para ser desclassificado quando encerrada a etapa competitiva; ou

21.6.2.4. Deixar de apresentar amostra;

21.6.2.5. Apresentar proposta ou amostra em desacordo com as especificações do edital;

21.6.3. Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

21.6.3.1. Recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

21.6.4. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação

21.6.5. Fraudar a licitação

21.6.6. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

21.6.6.1. Agir em conluio ou em desconformidade com a lei;

21.6.6.2. Induzir deliberadamente a erro no julgamento;

21.6.6.3. Apresentar amostra falsificada ou deteriorada;

21.6.7. Praticar atos ilícitos com vistas a frustrar os objetivos da licitação

21.6.8. Praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.

21.7. Com fulcro na Lei nº 14.133, de 2021, a Administração poderá, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

21.7.1. Advertência;
21.7.2. Multa;
21.7.3. Impedimento de licitar e contratar e
21.7.4. Declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

21.8. Na aplicação das sanções serão considerados:
21.8.1. A natureza e a gravidade da infração cometida.
21.8.2. As peculiaridades do caso concreto
21.8.3. As circunstâncias agravantes ou atenuantes
21.8.4. Os danos que dela provierem para a Administração Pública
21.8.5. A implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.
21.8.6. A multa será recolhida em percentual de 5% (cinco por cento) incidente sobre o valor incidente sobre o valor do contrato licitado, recolhida no prazo máximo de 30 (trinta) dias úteis, a contar da comunicação oficial.
21.8.7. Para as infrações previstas no Termo de Referência, a multa será de 5% (cinco por cento) do valor do contrato licitado.
21.8.8. Para as infrações previstas no Termo de Referência, a multa será de 5% (cinco por cento) do valor do contrato licitado.
21.8.9. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.
21.9. Na aplicação da sanção de multa será facultada a defesa do interessado no prazo de 15 quinze) dias úteis, contado da data de sua intimação.
21.10. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas no Termo de Referência, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.
21.10.1. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos Termo de Referência, que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar cuja duração observará o prazo previsto no art. 156 da lei n.º 14.133/2021.
21.10.2. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 21.6.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação, nos termos do [art. 45, §4º da IN SEGES/ME n.º 73, de 2022.]
21.10.3. A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15

(quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produz.

21.11. Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

21.11.1. Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

21.12. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

21.12.1. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causado.

22. DA FORMAÇÃO DO CADASTRO DE RESERVA

22.1. Após o encerramento da etapa competitiva, os licitantes poderão reduzir seus preços ao valor da proposta do licitante mais bem classificado.

22.2. A apresentação de novas propostas na forma deste item não prejudicará o resultado do certame em relação ao licitante melhor classificado.

22.3. Havendo um ou mais licitantes que aceitem cotar suas propostas em valor igual ao do licitante vencedor, estes serão classificados segundo a ordem da última proposta individual apresentada durante a fase competitiva.

22.4. Esta ordem de classificação dos licitantes registrados deverá ser respeitada nas contratações e somente será utilizado acaso o melhor colocado no certame não assine a ata ou tenha seu registro cancelado nas hipóteses previstas nos regulamentos vigentes.

23. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

23.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da Lei nº 14.133, de 2021, devendo protocolar o pedido até 3 (cinco) dias úteis antes da data da abertura do certame.

23.1.1. A resposta à impugnação ou ao pedido de esclarecimento será divulgado em sítio eletrônico oficial no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

23.2. A impugnação poderá ser realizada por forma eletrônica, pelo **e-mail licitacao@caceres.mt.gov.br**, ou por petição dirigida ou protocolada diretamente na Secretaria de administração: Sala de licitações, da Prefeitura Municipal de Cáceres/MT – Endereço: Av. Brasil, 119, COC, Bairro Jardim Celeste – CEP 78.206- 910 – Cáceres – MT, dirigida ao(à) pregoeiro(a), contendo os documentos necessários de qualificação do requerente, sendo em qualquer dos casos durante o seguinte horário: das 07:30 as 11:30h e das 13:30 as 17:30 (horário local).

23.3. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

23.4. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro, nos autos do processo de licitação.

23.5. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

24. DA PUBLICAÇÃO

24.1. Incumbirá ao contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, *caput,* da Lei n.º 14.133, de 2021, e ao art. 8º, §2º, da Lei n. 12.527, de 2011, c/c art. 7º,
§3º, inciso V, do Decreto n. 7.724, de 2012.

25. DAS DISPOSIÇÕES GERAIS

25.6. Será divulgada ata da sessão pública no sistema eletrônico.

25.7. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.

25.8. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília - DF.

25.9. A homologação do resultado desta licitação não implicará direito à contratação.

25.10. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

25.11. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

25.12. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir- se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

25.13. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

25.14. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

24.10. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital. Havendo divergência entre as especificações dos itens do CATSER e do termo de referência, prevalecerá o termo de referência.

24.11. O Edital está disponibilizado, na íntegra, no endereço eletrônico **http://www.caceres.mt.gov.br/licitacao/,** e também poderão ser lidos e/ou obtidos no endereço **compras.gov.br** nos dias úteis, no horário das 07h:30min às 11h:30min das 13h:30min às 17h:30min mesmo endereço e período no qual os autos do processo administrativo permanecerão com vista franqueada aos interessados.

24.12. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

24.12.1. ANEXO I – TERMO DE REFERÊNCIA

24.12.2. ANEXO II – MINUTA DA ATA DE REGISTRO DE PREÇO

24.12.3. ANEXO III – MINUTA DO TERMO DE CONTRATO

Cáceres/MT, 26 de maio de 2025.

JEREMIAS PEREIRA LEITE
Secretário Municipal Especial de Assustos estratégicos

ANEXO I - TERMO DE REFERÊNCIA 01/2025

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Registro de Preço para futura e eventual contratação de empresa especializada para prestação de serviços de segurança cibernética com Inteligência Artificial Preditiva, fornecimento, em regime de comodato, instalação e configuração de Next Generation Firewall (NGFW) e SD-WAN, redundância composta por links primário e secundário de ASN e rotas diferentes, manutenção contínua, suporte técnico, software de gerenciamento, conectividade segura para unidades externas e praças públicas, capacitação certificada da equipe e atendimento técnico especializado, garantindo alta disponibilidade, segurança, eficiência e sustentabilidade no atendimento às demandas do Município de Cáceres, conforme condições e exigências estabelecidas neste instrumento.

ITEM	CÓDIGO TCE-MT	CÓDIGO CAT MAT	ESPECIFICAÇÃO	UNIDADE	QUANTIDADE	QUANTIDADE ANUAL
1	257560-4	609340	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)	Serviço	173	2076
2	152969	481647	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	Serviço	2	24
3	00065206	26174	Serviço de Link dedicado de Acesso à internet, bloco /29 e Banda Mínima de Acesso Garantida de 500Mbps (Alta Disponibilidade) SEDE (Link de ASN e Rota Diferentes)	Serviço	2	24
4	152970	26484	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 150Mbps Sites Remotos (Fibra Óptica)	Serviço	171	2052
5	152972	26557	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G)	Serviço	171	2052
6	339905-2	1988	Implantação da Solução	Serviço	1	1

7	404876-8	16837	Capacitação especializada da equipe com emissão de certificação.	Treinamento	1	1
8	332679-9	27340	Consultoria Política de Segurança	Serviço	1	1

1.2. **As empresas interessadas deverão apresentar lances para todos os itens do certame, uma vez que a administração deverá ser conduzida por uma única contratada, razão pela qual não haverá divisão por lotes.**

1.3. A análise da documentação terá por finalidade verificar a habilitação da empresa, bem como sua capacidade de operar um projeto dessa complexidade.

1.3.1. Caso as exigências não sejam atendidas, será convocada a empresa subsequente que tenha apresentado o preço global imediatamente superior, observadas as regras de negociação.

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

1.5. O prazo de vigência da contratação é de 12 meses contados a partir da assinatura do contrato, podendo ser prorrogada por iguais e sucessivos períodos, limitada a 15 (quinze) anos, na forma do artigo 114 da Lei n° 14.133, de 2021.

1.6. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico do Estudo Técnico Preliminar, apêndice deste Termo de Referência.

3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

3.1. A Fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada em tópico específico do Estudo Técnico Preliminar, apêndice deste Termo de Referência.

3.2. O objeto da contratação está previsto no Plano de Contratações Anual [2025], conforme detalhamento a seguir:

I) ID PCA no PNCP: 03214145000183-0-000001/2025;

II) Data de publicação no PNCP: 28/01/2025;

III) Id do item no PCA: 166;

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

4.1. A solução tem por objetivo proporcionar uma infraestrutura robusta, segura e eficiente para o ambiente de tecnologia da informação da Prefeitura Municipal de Cáceres, assegurando a continuidade dos serviços públicos e a proteção dos dados institucionais. O ciclo de vida da solução contempla todas as fases essenciais, desde a implantação até a operação contínua, manutenção e eventuais atualizações tecnológicas, garantindo um alto padrão de qualidade e desempenho ao longo da vigência do contrato.

4.2. A solução contempla segurança cibernética avançada, conectividade de alto desempenho e suporte especializado, alinhando-se às melhores práticas de governança digital e proteção de ativos públicos.

4.3. A implantação e execução do contrato seguem um modelo estruturado em duas fases principais:

4.3.1. **Fase de Implantação**, com prazo de até 60 dias após a assinatura do contrato, abrangendo a instalação dos equipamentos, ativação dos links, integração das unidades externas e capacitação da equipe técnica.

4.3.2. **Fase de Prestação de Serviço Mensal**, com duração de até 180 meses, garantindo manutenção contínua, suporte técnico especializado, atualizações tecnológicas e otimização da infraestrutura de segurança e comunicação de dados.

4.4. O ciclo de vida da solução envolve etapas bem definidas, assegurando que a infraestrutura implementada esteja sempre atualizada e alinhada com as necessidades da Prefeitura.

4.4.1. **Planejamento e Implantação**

4.4.1.1. Na fase inicial, serão executadas as atividades necessárias para a estruturação da solução contratada, garantindo que todos os componentes sejam devidamente configurados e operacionalizados. Essa etapa inclui:

4.4.1.1.1. Instalação e configuração dos equipamentos de segurança cibernética, incluindo Next Generation Firewall (NGFW) e SD-WAN, visando a proteção contra ameaças digitais e a otimização do tráfego de rede.

4.4.1.1.2. Implementação de serviços de segurança cibernética baseados em Inteligência Artificial Preditiva, permitindo a detecção e resposta antecipada a incidentes.

4.4.1.1.3. Ativação dos links dedicados de internet, garantindo 500 Mbps na sede, 150 Mbps nos sites remotos e 35 Mbps como link de contingência, assegurando conectividade estável para as operações administrativas e serviços públicos digitais.

4.4.1.1.4. Integração das unidades externas e praças públicas à infraestrutura de rede segura, possibilitando um acesso seguro e confiável aos sistemas municipais.

4.4.1.1.5. Capacitação certificada da equipe técnica da Prefeitura, garantindo a qualificação necessária para a gestão e monitoramento da solução implementada.

4.4.2. **Operação e Manutenção**

4.4.2.1. Após a implantação, a solução entrará em operação contínua, garantindo que os serviços contratados sejam entregues de forma eficiente e dentro dos padrões de qualidade exigidos. Esta fase inclui:

4.4.2.1.1. Monitoramento contínuo da infraestrutura, com análises preditivas para detecção de ameaças e otimização do desempenho dos sistemas.

4.4.2.1.2. Suporte técnico especializado, disponível para resolver quaisquer incidentes ou necessidades de ajustes na configuração da solução.

4.4.2.1.3. Gestão e atualização dos equipamentos e software, garantindo que os firewalls, SD-WAN e demais componentes tecnológicos operem sempre com as versões mais recentes e seguras.

4.4.2.1.4. Consultoria contínua para aprimoramento da política de segurança da informação, com foco na proteção de dados, conformidade regulatória e mitigação de riscos cibernéticos.

4.4.2.1.5. Garantia de alta disponibilidade, com suporte a redundância de links e contingência operacional para evitar interrupções nos serviços municipais.

4.4.3. **Evolução e Sustentabilidade da Solução**

4.4.3.1. Ao longo do ciclo de vida da solução, serão adotadas práticas que garantam sua evolução tecnológica e sustentabilidade, permitindo que o investimento realizado permaneça eficiente e alinhado às necessidades do município. Entre essas práticas, destacam-se:

4.4.3.1.1. Adoção de tecnologias emergentes para otimizar a performance e segurança da infraestrutura de TIC.

4.4.3.1.2. Revisão periódica da estratégia de segurança cibernética, considerando as tendências de ameaças digitais e as melhores práticas do setor.

4.4.3.1.3. Expansão escalável da solução, permitindo a incorporação de novas unidades e serviços de forma ágil e estruturada.

4.4.3.1.4. Otimização do consumo de recursos tecnológicos, garantindo um uso eficiente da infraestrutura contratada e contribuindo para a sustentabilidade financeira e operacional do município.

4.5. **Especificação do Produto**

4.5.1. **Funcionamento Geral da Solução**

4.5.1.1. A contratação deverá englobar além das soluções de defesa cibernética a prestação de serviços de rede de longa distância (WAN) para manter a interligação da Sede da Prefeitura de Cáceres aos Sites Remotos, localizados no interior do Município e fora dele.

4.5.1.2. A contratação também inclui a prestação de serviço de acesso à internet nos Sites Remotos e na sede da Prefeitura Municipal de Cáceres MT.

4.5.1.3. A contratação deverá englobar o fornecimento de um conjunto de equipamentos de redes incluindo recursos de IP para trabalhar em alta disponibilidade na Sede e cada equipamento deverá permitir no mínimo 4(quatro) conexões à Internet.

4.5.1.4. A nova solução de comunicação de dados entre os Sites Remotos e a Sede utilizará equipamentos com a tecnologia SD-WAN com o objetivo de balancear o tráfego de forma inteligente para otimizar o uso da rede. Para que o tráfego corporativo seja protegido quando trafegar pela internet, serão configurados túneis VPN IPSEC entre os equipamentos SD-WAN da Sede da Prefeitura e dos Sites Remotos.

4.5.1.5. Os equipamentos SD-WAN da Sede deverão trabalhar em alta disponibilidade.

4.5.1.6. A relação dos Sites Remotos e da Central nos quais os serviços serão prestados encontra-se descrita no item 7.2.1.3 deste Termo de Referência.

4.5.1.7. Em situações normais, os tráfegos de sistemas da prefeitura sobretudo os administrativos, além do tráfego de telefonia IP, devem ser encaminhados pela via IPSEC pelo melhor link. Por outro lado, os serviços de videoconferência das Plataformas Zoom, Google, Webex e Microsoft Teams devem ser acessados diretamente sem a necessidade de utilização deste túnel, além da navegação de Internet das redes dos assessores, colaboradores e cidadãos que acessam a rede social da Prefeitura.

4.5.1.8. Em situações de falha ou de uso intenso da rede, alternativamente os tráfegos corporativos devem ser encaminhados entre os Sites Central e remotos utilizando também túnel VPN IPSEC pelo link secundário estabelecidos pela Internet. Os túneis VPN devem utilizar a topologia hub-and-spoke, com centralização nos equipamentos SD-WAN na Sede.

4.5.1.9. Em situações de falha de um dos links de Internet dos Sites remotos, o tráfego deve ser encaminhado pela conexão de internet secundária até o Site Central da Prefeitura.

4.5.1.10. A configuração do encaminhamento do tráfego e da contingência em casos de falha deve ser feita utilizando tecnologia SD-WAN em que o encaminhamento de tráfego é feito com base no perfil de tráfego em vez da utilização de rotas.

4.5.1.11. A prestação dos serviços descritos em cada ITEM deverá ser considerada como entregue, a partir da assinatura do Termo de Recebimento Definitivo.

4.5.1.12. A prestação dos serviços será baseada no modelo de remuneração em função dos resultados apresentados, em que os pagamentos serão feitos após mensuração e verificação de métricas quantitativas e qualitativas, contendo indicadores de desempenho e metas, com Instrumento de Medição de Resultado (IMR) definido em contrato, de modo a resguardar a eficiência e a qualidade na prestação dos serviços.

4.5.1.13. Os serviços a serem prestados incluem, ainda, a elaboração prévia de um Projeto Executivo de rede, a ser analisado pela equipe técnica da Prefeitura para aprovação, conforme especificações incluídas neste documento. Esse documento deverá conter, no mínimo:

a) Definição de topologias físicas e lógicas;

b) Plano de Endereçamento;

c) Plano de balanceamento do tráfego;

d) Parâmetros de qualidade de serviço;

e) Dimensionamento de enlaces e interfaces de comunicação;

f) Documentação dos últimos 1000 metros de passagem das fibras ópticas.

4.5.1.14. Não haverá aquisição de equipamentos, incluindo roteadores, modens, appliances SD- WAN e demais ativos de rede. Contudo, deverão ser fornecidos equipamentos juntamente com a prestação

dos serviços de tecnologia da informação e comunicações como parte integrante da solução contratada.

4.5.1.15. O CONTRATANTE poderá solicitar a desativação do serviço prestado a qualquer sítio, bem como mudança de local de prestação dos serviços. Entende-se por mudanças de local de prestação dos serviços a mudança de endereços de instalação dos equipamentos e acessos dentro da cidade.

4.5.1.16. Após a conclusão da etapa de instalação dos serviços, a CONTRATADA deverá apresentar documentação técnica da solução (As Built), contendo: topologia física e lógica da rede, descrição de equipamentos e circuitos de comunicação de dados, descrição dos níveis mínimos de serviços contratados, dados para acesso ao portal de monitoramento dos serviços e dados para abertura de chamados de suporte técnico.

4.5.1.17. A CONTRATADA deverá também realizar repasse de conhecimento na modalidade presencial para a equipe técnica do CONTRATANTE sobre a solução implantada, conforme descrito no item 5.2 deste Termo de Referência.

4.5.2. Topologia Da Solução

4.5.2.1. A solução foi estruturada com base nas necessidades específicas da Prefeitura Municipal de Cáceres, visando garantir conectividade segura, eficiente e de alta disponibilidade para todas as unidades envolvidas. A infraestrutura foi projetada para suportar um volume significativo de acessos simultâneos, assegurando a qualidade da comunicação de dados, a integridade das informações e a segurança cibernética dos sistemas institucionais.

4.5.2.1.1. Estruturação dos Sites e Capacidade dos Links

4.5.2.1.1.1. A topologia da solução foi desenhada considerando a divisão dos Sites Remotos e do Site Central em dois tipos distintos de tecnologia e capacidade de conexão, com base na demanda estimada de usuários simultâneos e nos requisitos operacionais de cada localidade.

4.5.2.1.1.1.1. **Sites Remotos:** A estrutura contempla unidades como Postos de Saúde, Centros de Saúde e espaços públicos, onde os serviços de tecnologia da informação serão utilizados para fins administrativos e sociais. A demanda estimada para os Postos de Saúde varia entre 7 e 10 usuários simultâneos, enquanto os Centros de Saúde podem atender de 15 a 50 usuários simultaneamente. O tráfego nesses locais incluirá tanto o acesso aos sistemas institucionais da Prefeitura quanto a utilização de serviços públicos digitais pelos cidadãos.

4.5.2.1.1.1.2. **Site Central:** A Sede da Prefeitura concentra entre 400 e 500 usuários simultâneos, entre servidores e colaboradores, acessando tanto recursos internos quanto externos. Devido ao alto volume de tráfego e à criticidade dos serviços processados, a conexão do Site Central conta com dois links dedicados de alta capacidade (500 Mbps cada), providos por ASN distintos e rotas diferentes, garantindo redundância e continuidade operacional.

4.5.2.1.1.2. A configuração dos links de internet e a implementação da tecnologia SD- WAN asseguram balanceamento inteligente do tráfego, priorização de pacotes críticos e segurança reforçada para as comunicações entre as unidades.

4.5.2.1.2. Topologia Lógica da Solução

4.5.2.1.2.1. A topologia lógica da solução foi elaborada para representar a interconexão dos elementos envolvidos e demonstrar o produto final desta contratação. A arquitetura contempla os seguintes componentes essenciais:

4.5.2.1.2.1.1. Next Generation Firewalls (NGFW) instalados no Site Central, atuando como pontos de controle de segurança cibernética, prevenindo ataques e garantindo a integridade dos dados trafegados entre as unidades.

4.5.2.1.2.1.2. Solução de segurança cibernética com utilização de Inteligência Preditiva.

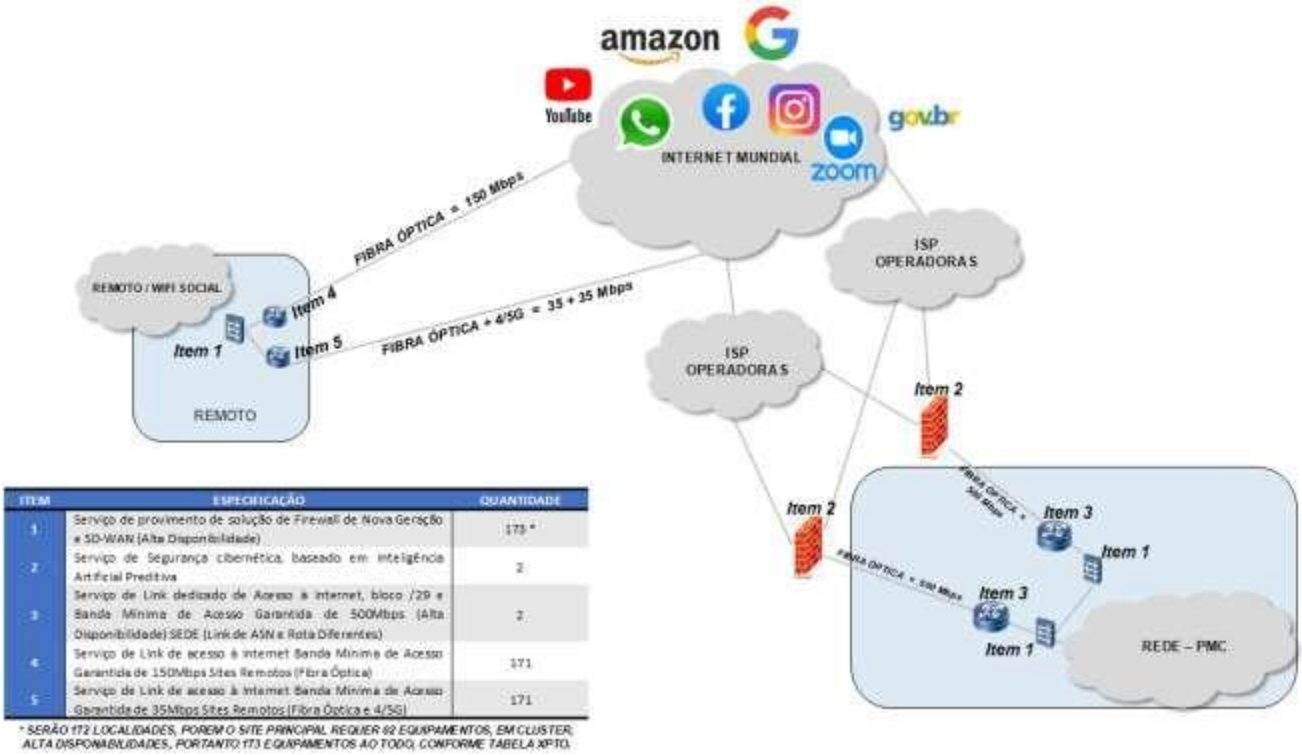
4.5.2.1.2.1.3. Dispositivos SD-WAN implementados na Sede e nos Sites Remotos, possibilitando gerenciamento eficiente do tráfego, redundância e otimização dos links de comunicação.

4.5.2.1.2.1.4. VPN IPSEC configurada em topologia hub-and-spoke, assegurando segurança na troca de informações entre os Sites Remotos e o Site Central.

4.5.2.1.2.1.5. Monitoramento centralizado, por meio de um software de gestão e segurança, permitindo a visualização em tempo real do tráfego da rede, detecção de anomalias e gerenciamento proativo de incidentes.

4.5.2.1.2.1.6. Consultoria especializada e capacitação da equipe técnica da Prefeitura, garantindo conhecimento sobre a administração da solução e autonomia na gestão da infraestrutura implantada.

4.5.2.1.2.2. Foi elaborada uma topologia lógica da solução demonstrando o produto final desta contratação:



ITEM	ESPECIFICAÇÃO	QUANTIDADE
1	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)	173 *
2	Serviço de Segurança cibernética baseado em Inteligência Artificial Preditiva	2
3	Serviço de Link dedicado de Acesso à internet, bloco /29 e Banda Mínima de Acesso Garantida de 500Mbps (Alta Disponibilidade) SEDE (Link de ASN e Rota Diferentes)	2
4	Serviço de Link de acesso à internet Banda Mínima de Acesso Garantida de 150Mbps Sites Remotos (Fibra Óptica)	171
5	Serviço de Link de acesso à internet Banda Mínima de Acesso Garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G)	171

** SERÃO 172 LOCALIDADES, POREM O SITE PRINCIPAL REQUER 02 EQUIPAMENTOS, EM CLUSTER, ALTA DISPONABILIDADES, PORTANTO 173 EQUIPAMENTOS AO TODO, CONFORME TABELA XPTO.*

4.5.3. **Equipamentos e Funcionalidades Chave**

4.5.3.1. **Os equipamentos do ITEM 1 deverão ser entregues no formato e características técnicas bem como funcionalidades conforme especificações abaixo:**

4.5.3.1.1.Appliance NGFW de 5 Gbps de Capacidade de Firewall 4.5.3.1.1.1. Características do Hardware

4.5.3.1.1.1.1. O equipamento deve se instalar em mesa ocupando no máximo 1U (44,45mm) da referida mesa;

4.5.3.1.1.1.2. Dispor de fonte de alimentação com tensão de entrada de 110V

/ 220V AC automática e frequência de 50-60 Hz;

4.5.3.1.1.1.3. Deverão ser fornecidos todos os cabos de energia, serial (RS- 232/RJ45), para instalação e funcionamento do dispositivo;

4.5.3.1.1.1.4. Possuir led indicador on/off, disco e devices de rede;

4.5.3.1.1.1.5. Possuir throughput mínimo de 5 Gbps para tráfego UDP; 4.5.3.1.1.1.6. Suportar no mínimo 4.000.000 (quatro milhões) conexões simultâneas;

4.5.3.1.1.1.7. Suportar no mínimo 37.000 (trinta e sete mil) novas conexões por segundo;

4.5.3.1.1.1.8. Possuir throughput mínimo de 300 Mbps para tráfego IPS/IDS; 4.5.3.1.1.1.9. Possuir throughput mínimo de 280 Mbps para tráfego VPN IPSEC com criptografia (AES-256);

4.5.3.1.1.1.10. Possuir throughput mínimo de 140 Mbps para tráfego VPN SSL com criptografia (AES-256);

4.5.3.1.1.1.11. Possuir throughput mínimo de 150 Mbps para SSL Inspection; 4.5.3.1.1.1.12. Possuir throughput mínimo de 200 Mbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

4.5.3.1.1.1.13. Possuir no mínimo 4 (quatro) interfaces de rede Gigabit Ethernet 10/100/1000/2500 Mbps com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

4.5.3.1.1.1.14. Possuir dispositivo de armazenamento interno de no mínimo 64 GB padrão SSD e deve suportar expansão futura para, no mínimo, 120 GB;

4.5.3.1.1.1.15. Possuir no mínimo 1 (uma) porta console de conexão para acesso a interface de comando CLI específica para esta finalidade, utilizando cabo do tipo serial RS-232 ou RJ-45;

4.5.3.1.1.1.16. Possuir pelo menos 1 (uma) portas USB para conexão de dispositivos externos;

4.5.3.1.1.1.17. Deve possuir modem interno 3G/4G/LTE para conexão de link de Internet. O modulo deverá estar incluso no valor do equipamento;

4.5.3.1.2.Appliance NGFW de 9.7 Gbps de Capacidade de Firewall 4.5.3.1.2.1. Características do Hardware

4.5.3.1.2.1.1. O equipamento deve se instalar em mesa ocupando no máximo 1U (44,45mm) da referida mesa;

4.5.3.1.2.1.2. Dispor de fonte de alimentação com tensão de entrada de 110V

/ 220V AC automática e frequência de 50-60 Hz;

4.5.3.1.2.1.3. Deverão ser fornecidos todos os cabos de energia, serial (RS- 232/RJ45) ou similar, para instalação e funcionamento do dispositivo;

4.5.3.1.2.1.4. Possuir led indicador on/off, disco e devices de rede.

4.5.3.1.2.1.5. Possuir throughput mínimo de 9.7 Gbps para tráfego UDP; 4.5.3.1.2.1.6. Suportar no mínimo 6.000.000 (seis milhões) conexões simultâneas;

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
ório - 029/2025 [illegible] (129/250) [illegible]
ICP Brasil

4.5.3.1.2.1.7. Suportar no mínimo 45.000 (quarenta e cinco mil) novas conexões por segundo;

4.5.3.1.2.1.8. Possuir throughput mínimo de 1.25 Gbps para tráfego IPS/IDS;

4.5.3.1.2.1.9. Possuir throughput mínimo de 2.0 Gbps para tráfego VPN IPSEC com criptografia (AES-256);

4.5.3.1.2.1.10. Possuir throughput mínimo de 1.2 Gbps para tráfego VPN SSL com criptografia (AES-256);

4.5.3.1.2.1.11. Possuir throughput mínimo de 700 Mbps para tráfego SSL Inspection;

4.5.3.1.2.1.12. Possuir throughput mínimo de 850 Mbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

4.5.3.1.2.1.13. Possuir no mínimo 4 (quatro) interfaces de rede Gigabit Ethernet 10/100/1000/2500 Mbps com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

4.5.3.1.2.1.14. Possuir dispositivo de armazenamento interno de no mínimo 64 GB padrão SSD e deve suportar expansão futura para, no mínimo, 120 GB;

4.5.3.1.2.1.15. Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento;

4.5.3.1.2.1.16. Possuir pelo menos 1 (uma) porta USB para conexão de dispositivos externos;

4.5.3.1.2.1.17. A interface USB deve suportar o uso de modem 3G/4G/LTE para conexão de link de Internet;

4.5.3.1.3.Appliance NGFW de 11.8 Gbps de Capacidade de Firewall 4.5.3.1.3.1. Características do Hardware

4.5.3.1.3.1.1. O equipamento deve se instalar em mesa ocupando no máximo 1U (44,45mm) da referida mesa;

4.5.3.1.3.1.2. Dispor de fonte de alimentação com tensão de entrada de 110V

/ 220V AC automática e frequência de 50-60 Hz;

4.5.3.1.3.1.3. Deverão ser fornecidos todos os cabos de energia, serial (RS- 232/RJ45) ou similar, para instalação e funcionamento do dispositivo;

4.5.3.1.3.1.4. Possuir led indicador on/off, disco e devices de rede; 4.5.3.1.3.1.5. Possuir throughput mínimo de 11.8 Gbps para tráfego UDP; 4.5.3.1.3.1.6. Suportar no mínimo 7.000.000 (sete milhões) conexões simultâneas;

4.5.3.1.3.1.7. Suportar no mínimo 52.000 (cinquenta e duas mil) novas conexões por segundo;

4.5.3.1.3.1.8. Possuir throughput mínimo de 1.5 Gbps para tráfego IPS/IDS; 4.5.3.1.3.1.9. Possuir throughput mínimo de 2.5 Gbps para tráfego VPN IPSEC com criptografia (AES-256);

4.5.3.1.3.1.10. Possuir throughput mínimo de 1.5 Gbps para tráfego VPN SSL com criptografia (AES-256);

4.5.3.1.3.1.11. Possuir throughput mínimo de 900 Mbps para tráfego SSL Inspection;

4.5.3.1.3.1.12. Possuir throughput mínimo de 1.0 Gbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

4.5.3.1.3.1.13. Possuir no mínimo 6 (seis) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

4.5.3.1.3.1.14. Possuir dispositivo de armazenamento interno de no mínimo 120 GB padrão SSD;

4.5.3.1.3.1.15. Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento;

4.5.3.1.3.1.16. Possuir pelo menos 1 (uma) porta USB para conexão de dispositivos externos;

4.5.3.1.3.1.17. A interface USB deve suportar o uso de modem 3G/4G/LTE para conexão de link de Internet;

4.5.3.1.4. Appliance NGFW de 19.4 Gbps de Capacidade de Firewall 4.5.3.1.4.1. Características do Hardware

4.5.3.1.4.1.1. Deverá ser entregue dois equipamentos idênticos para atender a funcionalidade de cluster;

4.5.3.1.4.1.2. O equipamento deve se instalar em rack com largura padrão de

19 polegadas, padrão EIA-310, ocupando no máximo 1U (44,45mm) do referido rack;

4.5.3.1.4.1.3. Dispor de fonte de alimentação interna com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;

4.5.3.1.4.1.4. Possuir painel/led indicador on/off, disco e devices de rede; 4.5.3.1.4.1.5. Possuir throughput de no mínimo 19.4 Gbps para tráfego UDP; 4.5.3.1.4.1.6. Suportar no mínimo 8.200.000 (oito milhões e duzentas mil) conexões simultâneas;

4.5.3.1.4.1.7. Suportar no mínimo 65.000 (sessenta e cinco mil) novas conexões por segundo;

4.5.3.1.4.1.8. Possuir throughput mínimo de 3.0 Gbps para tráfego IPS/IDS; 4.5.3.1.4.1.9. Possuir throughput mínimo de 3.0 Gbps para tráfego VPN IPSEC com criptografia (AES-256);

4.5.3.1.4.1.10. Possuir throughput mínimo de 1.8 Gbps para tráfego VPN SSL com criptografia (AES-256);

4.5.3.1.4.1.11. Possuir throughput mínimo de 1.3 Gbps para tráfego SSL Inspection;

4.5.3.1.4.1.12. Possuir throughput mínimo de 2.5 Gbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

4.5.3.1.4.1.13. Possuir pelo menos 6 (seis) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

4.5.3.1.4.1.14. Possuir dispositivo de armazenamento interno de no mínimo 120 GB padrão SSD;

4.5.3.1.4.1.15. Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento;

4.5.3.1.4.1.16. Possuir no mínimo 1 (uma) porta USB para conexão de dispositivos externos;

4.5.3.1.4.1.17. A interface USB deve suportar o uso de modem 3G/4G/LTE para conexão de link de Internet;

4.5.3.2. **Especificações Gerais de Software NGFW Para Todos os Itens**

4.5.3.2.1.Das Funcionalidades do Firewall, SD-Wan, VPN IPsec/SSL 4.5.3.2.1.1. Características Gerais

4.5.3.2.1.1.1. Quaisquer licenças que forem entregues para atender aos recursos da solução especificado no termo de referência, deverão ter seu vencimento de acordo com o período de contrato.

4.5.3.2.1.1.2. O desempenho e as interfaces solicitados deverão ser comprovados através de datasheet público na internet. Caso haja divergência entre métricas do mesmo datasheet, será aceito o valor de menor capacidade.

4.5.3.2.1.1.3. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

4.5.3.2.1.1.4. Todos os recursos listados neste termo de referência deverão ser suportado e estar disponíveis na versão mais atual do software fornecido;

4.5.3.2.1.1.5. Os desempenhos dos appliances ofertados devem ser mensurados através da metodologia baseada em proxy (Proxy Based), não serão aceitos appliances mensurados somente no método baseado em fluxo (Flow Based);

4.5.3.2.1.1.6. Interface em português, espanhol e inglês;

4.5.3.2.1.1.7. Suportar notificação de vencimento da licença na janela de alertas com os dias restantes da data vencimento;

4.5.3.2.1.1.8. Suportar acesso à Web por HTTP e CLI por TELNET;

4.5.3.2.1.1.9. Permitir alterar a porta padrão para os acessos a interface de

administração via HTTP, HTTPs e CLI;

4.5.3.2.1.1.10. Atualização de modo “offline”, onde pode ser baixado na base do fabricante e posteriormente fazer o upload do arquivo na solução.

4.5.3.2.1.1.11. Restore de Snapshot sem executar o Wizard e sem licenciamento;

4.5.3.2.1.1.12. A solução deve oferecer suporte ao NAT444 (CGNAT) ou funcionalidade que implemente a persistência no NAT de saída independente da porta de destino, de forma que o endereço IP e porta traduzidos para um determinado usuário se mantenham os mesmos nas novas sessões que cheguem com o mesmo endereçamento IP e porta de origem;

4.5.3.2.1.1.13. Suportar segundo fator de autenticação (2FA/MFA) via token

/ OTP (One Time Password); 4.5.3.2.1.1.14. Deve suportar sistemas virtuais;

4.5.3.2.1.1.15. 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 diferentemente;

4.5.3.2.1.1.16. Qualquer interface de rede do equipamento deverá ser utilizada como gerenciamento, ou seja, não deve haver nenhuma interface exclusiva para a função de gerenciamento;

4.5.3.2.1.1.17. O sistema deve permitir o acesso à interface de gerenciamento WEB por qualquer interface de rede configurada;

4.5.3.2.1.1.18. O software deverá ser fornecido em sua versão mais atualizada, não sendo permitido qualquer tipo de comprovação futura.

4.5.3.2.1.1.19. Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução.

4.5.3.2.1.1.20. Todos os recursos detalhados no termo de referência deverão ser providos por um único software.

4.5.3.2.1.1.21. Tanto os Gateways de Segurança bem como a Gerência Centralizada deverão suportar monitoramento através de SNMP v1, v2 e v3.

4.5.3.2.1.1.22. Deverá possuir uma janela para monitoramento do tráfego de rede com informações do throughput e da quantidade de conexões simultâneas;

4.5.3.2.1.1.23. A Solução deverá prover inspeção SSL:

4.5.3.2.1.1.24. Deve suportar cluster do tipo Failover (HA) com replicação da tabela de estado;

4.5.3.2.1.1.25. Suportar a utilização de um proxy para atualização do software e licenciamento e deverá permitir as seguintes opções de configuração:

a) Endereço do servidor;

b) Porta do servidor;

c) Usuário;

d) Senha;

4.5.3.2.1.1.26. Deverá permitir o monitoramento SNMP, no mínimo, dos seguintes itens:

a) Desempenho total (throughput);

b) Conexões simultâneas;

c) Usuários autenticados;

d) Serviços habilitados ou desabilitados;

e) Quantidade de endereços distribuídos pelo DHCP.

4.5.3.2.1.1.27. Deverá implementar a funcionalidade de "zero touch" para sua

primeira implementação ou substituição. Dessa forma, deverá ser possível provisionar a configuração do equipamento via sistema de gerenciamento centralizado, transformando a atividade em uma simples conexão física de equipamento, sem a necessidade de configurações individuais nos equipamentos;

4.5.3.2.1.1.28. A Solução deve permitir ao administrador associar na solução de gerenciamento centralizado o número de série dos equipamentos ao site onde será instalado, de maneira que ao se ativar um equipamento no site remoto, esse equipamento se conecte com a Sistema Central e receba a configuração;

4.5.3.2.1.1.29. Ao instalar um equipamento no site remoto, cabeá-lo e energizá-lo, ele deverá tentar localizar Sistema Central para receber a sua configuração, sem que seja necessária qualquer configuração via console local do equipamento;

4.5.3.2.1.1.30. Deverá possuir um painel centralizado para exportação e agendamento de relatórios e deverá permitir exportá-los nos formatos: HTML, PDF, CSV;

4.5.3.2.1.1.31. Implementar protocolo de coleta de informações de fluxos que circulam pelo equipamento, como Netflow v5, v9 e v10 (IPFIX):

4.5.3.2.1.1.32. Os módulos de IPS, SD-WAN, Controle de aplicativos, Proxy WEB e Antimalware devem ser disponibilizados em perfis e estes devem ser inseridos em uma única política;

4.5.3.2.1.1.33. Deve implementar o protocolo ECMP;

4.5.3.2.1.1.34. O sistema deverá implementar otimização de fluxos TCP em conjunto com mecanismo para evitar retransmissão ou implementar métodos de correção de erros que permitam à unidade receptora recuperar pacotes que venham a ser perdidos na transmissão.

4.5.3.2.1.1.35. Deve possuir suporte ao protocolo de encapsulamento de redes MPLS;

4.5.3.2.1.1.36. Esta condição deve permitir conectar links MPLS diretamente no equipamento sem a necessidade de estar plugado a um segundo roteador/dispositivo.

4.5.3.2.1.1.37. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;

4.5.3.2.1.1.38. 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;

4.5.3.2.1.2. Recursos Gerais de Firewall

4.5.3.2.1.2.1. Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas;

4.5.3.2.1.2.2. Possuir um sistema de armazenamento remoto para salvar backups da solução com suporte a conexões utilizando os protocolos Network File System (NFS), SSH e que permita salvar em dispositivo USB conectado localmente;

4.5.3.2.1.2.3. Possibilitar a visualização dos países de origem e destino nos logs de eventos, de acessos e ameaças.

4.5.3.2.1.2.4. Possuir mecanismo que permita a realização de cópias de segurança (backups) do sistema e restauração remota, através da interface gráfica, a solução deve permitir o agendamento diário ou semanal;

4.5.3.2.1.2.5. O sistema deve permitir configurar o período ou número de cópias que deseja manter no repositório remoto e executar a manutenção de período automaticamente.

4.5.3.2.1.2.6. As cópias de segurança devem ser salvas compactadas e criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;

4.5.3.2.1.2.7. O sistema ainda deve contemplar um recurso de cópia de segurança do tipo snapshot, que contemple a cópia completa das configurações dos serviços e recursos do sistema;

4.5.3.2.1.2.8. Deve possibilitar a restauração do snapshot através da interface web de qualquer ponto remoto, de modo a contribuir para uma restauração imediata sem a necessidade de reinicialização do sistema;

4.5.3.2.1.2.9. Deve permitir habilitar ou desabilitar o registro de log por política de firewall.

4.5.3.2.1.2.10. Possuir controle de acesso à internet por endereço IP de origem e destino;

4.5.3.2.1.2.11. Possuir controle de acesso à internet por sub-rede

4.5.3.2.1.2.12. Possuir suporte a tags de VLAN (802.1q);

4.5.3.2.1.2.13. Suportar agregação de links, segundo padrão IEEE 802.3ad; 4.5.3.2.1.2.14. Possuir ferramenta de diagnóstico do tipo tcpdump; 4.5.3.2.1.2.15. Possuir integração com Servidores de

Autenticação RADIUS, TACACS+, LDAP e Microsoft Active Directory;

4.5.3.2.1.2.16. Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

4.5.3.2.1.2.17. Possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para- um, vários para vários e vários para um.

4.5.3.2.1.2.18. Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;

4.5.3.2.1.2.19. Permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br;

4.5.3.2.1.2.20. Possuir suporte a roteamento dinâmico RIP V1, V2, OSPFv2, OSPFv3, BGP e suportar duplicação de pacotes;

4.5.3.2.1.2.21. Possuir funcionalidades de DHCP Cliente, Servidor e Relay; 4.5.3.2.1.2.22. Deve ser possível configurar um servidor RADIUS para a validação de usuários;

4.5.3.2.1.2.23. A solução deve consultar o Servidor Radius integrado, caso o Servidor Radius autorize, o NGFW deve entregar o endereço IP do range; caso contrário, não fornece endereço IP e a máquina não recebe o endereço, ficando sem acesso à rede.

4.5.3.2.1.2.24. Deverá suportar aplicações multimídia como: H.323, SIP; 4.5.3.2.1.2.25. Possuir tecnologia de firewall do tipo Stateful;

4.5.3.2.1.2.26. Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo-passivo;

4.5.3.2.1.2.27. Permitir o funcionamento em modo transparente tipo “bridge”; 4.5.3.2.1.2.28. Permitir a criação de mínimo 4090 VLANS no padrão IEEE 802.1q por interface de rede;

4.5.3.2.1.2.29. Possuir conexão entre estação de gerência e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando);

4.5.3.2.1.2.30. Deverá suportar forwarding de multicast;

4.5.3.2.1.2.31. Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP;

4.5.3.2.1.2.32. Permitir o agrupamento de serviços; 4.5.3.2.1.2.33. Possuir mecanismo de anti-spoofing;

4.5.3.2.1.2.34. Possuir a funcionalidade de balanceamento e contingência de links;

4.5.3.2.1.2.35. Possibilitar a configuração dos timeouts de resposta dos protocolos de conexão, devendo suportar no mínimo a definição das opções do timeout padrão do ICMP, estabelecimento do TCP, envio do SYN em sessões TCP.

4.5.3.2.1.2.36. Permitir a configuração de regras de entrada baseado em zona de rede, possibilitando habilitar recursos de autenticação e restrição por origem baseado em IP.

4.5.3.2.1.2.37. Deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas, suportando ao menos: Yahoo! Messenger, MSN Messenger, ICQ, Telegram, Whatsapp, WeChat, Snapchat BitTorrent, UTorrent, Vuze, eDonkey, GNUTella, Skype e Microsoft Teams.

4.5.3.2.1.2.38. A solução deverá suportar nativamente o recurso SIMET (nic.br) medidor de Internet.

4.5.3.2.1.3. Política de Segurança

4.5.3.2.1.3.1. Permitir limitar a quantidade máxima de pacotes por segundo no Firewall, evitando ataques distribuídos ou anomalias de tráfego causadas por possíveis malwares na rede;

4.5.3.2.1.3.2. A configuração de proteção DOS deve estar disponível para habilitar em modo global e por política de segurança;

4.5.3.2.1.3.3. Possuir recurso de validação das políticas de segurança para identificar regras duplicadas ou que se ofusquem;

4.5.3.2.1.3.4. Possui uma única janela de configuração de política de segurança onde seja possível inserir os perfis de Proxy WEB, IPS, APP control, SD-WAN e ATP.

4.5.3.2.1.3.5. Deverá permitir implementar filtros de IPS, WEB Filter, Threat Protection, SSL Inpection, Application Control, assim como definir roteamento de aplicativos por SD-Wan, limitação de taxa de DOS por pacotes em uma única política.

4.5.3.2.1.3.6. Exibir na própria política a visualização de quais módulos estão habilitados, sem que seja necessário a edição da regra de proteção.

4.5.3.2.1.3.7. Possibilitar a edição de objetos vinculados, sem a necessidade de recriar a política.

4.5.3.2.1.3.8. Possibilitar a duplicação de uma política, otimizando tempo de configuração;

4.5.3.2.1.4. Identificação de Usuário

4.5.3.2.1.4.1. Deve possuir a capacidade de criação de políticas de acesso de Firewall, VPN, IPS e Controle de aplicação integradas ao repositório de usuários sendo: Active Directory, LDAP, TACAC´S e Radius;

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

4.5.3.2.1.4.3. Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador (Captive Portal), sem a necessidade de agente;

4.5.3.2.1.4.4. Deve possuir Captive Portal com suporte a Autenticação Social (Facebook, Twitter, Google);

4.5.3.2.1.4.5. A solução deverá ser capaz de identificar nome do usuário, login, máquina/computador registrados no Microsoft Active Directory;

4.5.3.2.1.4.6. Para o sistema de controles no serviço de autenticação o produto deve possuir, no mínimo, as seguintes condições para o Controle de Autenticação:

a) Usuários e Grupos de Usuários;

b) Datas (Objetos de Datas)

c) Horários (Objetos de Horário)

d) Lista de palavras chave ou conjunto de combinações de expressões regulares, (Objetos de Dicionários)

e) Endereços Remotos (Objetos de IPv4 e IPv6)

f) Zona de Rede (Múltiplas Zonas)

4.5.3.2.1.4.7. A solução deve suportar autenticação por SSO utilizando WMI (Windows Management Instrument) ou seja, não deve ser necessário instalar nenhum agente no servidor de autenticação.

4.5.3.2.1.4.8. A solução deve suportar o sincronismo entre vários NGFW em relação a replicação das sessões autenticadas da filial (Branch) na matriz (Head Office) e vice-versa, sem a necessidade de agentes externos.

4.5.3.2.1.4.9. A solução deverá suportar múltiplos Servidores de Autenticação (MS AD e/ou Ldap) atuando no modo failover;

4.5.3.2.1.5. Das Funcionalidades Da Vpn:

4.5.3.2.1.5.1. VPN baseada em appliance;

4.5.3.2.1.5.2. Possuir algoritmos de criptografia para túneis VPN: AES, 3DES;

4.5.3.2.1.5.3. Suporte a certificados PKI X.509 para construção de VPNs; 4.5.3.2.1.5.4. Possuir suporte a VPNs IPSec site-to-site:

4.5.3.2.1.5.5. Criptografia, 3DES, AES128, AES256, AES-GCM-128

4.5.3.2.1.5.6. Integridade MD5, SHA-1, SHA-256, SHA384 e AES-XCBC;

4.5.3.2.1.5.7. Algoritmo Internet Key Exchange (IKE) versões I e II;

4.5.3.2.1.5.8. AES 128 e 256 (Advanced Encryption Standard);

4.5.3.2.1.5.9. Suporte a Diffie-Hellman Grupo 1, Grupo 2, Grupo 5, Grupo

14; Grupo 15, Grupo 16, Grupo 17, Grupo 18, Grupo 19, Grupo

20, Grupo 21, Grupo 22, Grupo 23, Grupo 24, Grupo 25, Grupo

26, Grupo 27, Grupo 28, Grupo 29, Grupo 30, Grupo 31, Grupo

32;

4.5.3.2.1.5.10. Possuir suporte a VPN SSL;

4.5.3.2.1.5.11. Possuir capacidade de realizar SSL VPNs utilizando certificados digitais;

4.5.3.2.1.5.12. Suportar VPN SSL Clientless, sem a necessidade de utilização de Java, no mínimo, para os serviços abaixo:

a) RDP;

b) VNC;

c) SSH;

d) WEB;

e) SMB.

4.5.3.2.1.5.13. Deve permitir a arquitetura de vpn hub and spoke;

4.5.3.2.1.5.14. Suporte a VPNs IPSec client-to-site;

4.5.3.2.1.5.15. Deverá possuir cliente próprio para Windows para o estabelecimento da VPN client-to-site.

4.5.3.2.1.5.16. Suporte à inclusão em autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol);

4.5.3.2.1.5.17. Possuir funcionalidades de Auto-Discovery VPN capaz de permitir criar tuneis de VPN dinâmicos entre múltiplos dispositivos (spokes) com um gateway centralizador (hub).;

4.5.3.2.1.5.18. A funcionalidade de AD-VPN deve suportar criar os seguintes tipos de tuneis:

a) Site-to-Site;

b) Full-Mesh;

c) Star.

4.5.3.2.1.5.19. Suportar configuração VTI (virtual interface) na configuração de túneis VPN site-to-site com BGP (Border Gateway Protocol). Os túneis são utilizados para prover uma comunicação criptografada e encapsulada, por rotas, entre o peer (NGFW local) e o host;

4.5.3.2.1.5.20. A solução poderá atuar como cliente de tuneis VPN IPSec com suporte à autenticação XAuth/PSK e/ou XAuth/RSA.

4.5.3.2.1.5.21. A VPN client-to-site deve suportar o estabelecimento automático da VPN nos protocolos ICMP ou DNS (53/UDP), caso o cliente remoto identifique que a porta padrão está sendo bloqueada;

4.5.3.2.1.5.22. Possuir recurso para configurar vários túneis simultâneos da VPN cliente-to-site, com o objetivo de aumentar o desempenho do tráfego;

4.5.3.2.1.5.23. Suportar segundo fator de autenticação (2FA/MFA) via token / OTP (One Time Password);

4.5.3.2.1.6. SD-WAN:

4.5.3.2.1.6.1. Entende-se como tecnologia SD-WAN (Software Defined WAN) a rede de área ampla definida por software que centraliza a gerência da rede WAN em uma console única, eliminando a necessidade de intervenções manuais em roteadores em localidades remotas, proporcionando visibilidade do tráfego seleção de caminho dinâmico baseado em políticas de QoS, aplicação ou performance e utilização de túneis VPN para comunicação entre os sites remotos;

4.5.3.2.1.6.2. Possuir o balanceamento automático para conexões externas à internet através das interfaces físicas;

4.5.3.2.1.6.3. Suportar modo de duplicação de pacotes de dados pelo links WAN, para que em caso de queda do link principal, possa ser enviado ao link secundário uma cópia do pacote de dados perdido permitindo assim a maior integridade e disponibilidade do tráfego;

4.5.3.2.1.6.4. Permitir utilizar VPN IPsec para interligar unidades remotas; 4.5.3.2.1.6.5. Possuir recurso de “persistência de link” para impedir a queda de conexões em aplicações que não suportam o load balance de link;

4.5.3.2.1.6.6. O balanceamento deverá ser baseado em critérios de desempenho, devendo no mínimo, permitir verificar o monitoramento do consumo de banda, perda de pacotes, jitter e latência;

4.5.3.2.1.6.7. Deve possuir uma janela web ou dashboard capaz de fornecer informações dos eventos e com informações do monitoramento de desempenho relacionado ao recurso SD-WAN;

4.5.3.2.1.6.8. O recurso de SD-WAN deverá suportar o roteamento de tráfego por política baseado em aplicação;

4.5.3.2.1.6.9. O appliance SD-WAN deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link monitorado recuperado seja avaliado. Deve suportar especificar um valor variando de 1 a 100.

4.5.3.2.1.6.10. O recurso de SD-WAN deverá permitir o monitoramento de, no mínimo 03 (três) endereços alvos para verificar a disponibilidade e desempenho do link;

4.5.3.2.1.6.11. A solução de SD-WAN NGFW deve permitir a configuração da funcionalidade de SD-WAN em qualquer interface WAN de forma agnóstica, independente se é internet, 3G/4G/LTE, entre outras;

4.5.3.2.1.6.12. A solução deverá suportar os seguintes métodos de seleção de link:

a) Failover;

b) Load Balance;

c) Spillover;

d) Dynamic Selection;

4.5.3.2.1.6.13. Deverá oferecer um monitor capaz de prover em tempo real as seguintes informações em uma única janela:

a) Consumo de banda;

b) Perda de pacotes;

c) Jitter;

d) Latência.

4.5.3.2.1.6.14. A Solução de SD-WAN deve desempenhar a função de Packet Duplication (PD) permitindo encaminhar o pacote por mais de um circuito para em casos de falhas não haver retransmissão;

4.5.3.2.1.7. Das Funcionalidades de QoS

4.5.3.2.1.7.1. Adotar solução de Qualidade de Serviço baseada em appliance;

4.5.3.2.1.7.2. Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;

4.5.3.2.1.7.3. Permitir modificação de valores DSCP;

4.5.3.2.1.7.4. Limitar individualmente a banda utilizada por programas de compartilhamento de arquivos do tipo peer-to-peer;

4.5.3.2.1.7.5. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

4.5.3.2.1.7.6. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;

4.5.3.2.1.7.7. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;

4.5.3.2.1.7.8. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino;

4.5.3.2.1.7.9. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

4.5.3.2.1.8. Alta Disponibilidade

4.5.3.2.1.8.1. Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Standby, com as implementações de Fail Over.

4.5.3.2.1.8.2. O Sincronismo dos servidores deve ser por interface exclusiva de Heartbeat;

4.5.3.2.1.8.3. No caso de falha do H.A. Ativo Primário, o H.A. Ativo secundário deve assumir de uma forma transparente sem impacto ao usuário ou perda de serviço;

4.5.3.2.1.8.4. Deverá suportar a persistências de sessão de usuarios e conexões estabelecidas, entre os membros da Alta Disponibilidade;

4.5.3.2.2. Das Funcionalidades de Controle de Aplicação e Web Proxy 4.5.3.2.2.1. Controle de Aplicações

4.5.3.2.2.1.1. As funcionalidades abaixo devem ser baseadas em appliance: 4.5.3.2.2.1.2. Deverá reconhecer no mínimo 4000 aplicações;

4.5.3.2.2.1.3. Deverá possuir, no mínimo, 19 categorias para classificação de aplicações;

4.5.3.2.2.1.4. Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações como:

a) P2P;

b) Web;

c) Transferência de arquivos;

d) Social;

4.5.3.2.2.1.5. Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;

4.5.3.2.2.1.6. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

4.5.3.2.2.1.7. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

4.5.3.2.2.1.8. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;

4.5.3.2.2.1.9. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP; 4.5.3.2.2.1.10. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

4.5.3.2.2.1.11. Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino;

4.5.3.2.2.1.12. Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.

4.5.3.2.2.2. Filtro de Conteúdo Web

4.5.3.2.2.2.1. Possuir solução de filtro de conteúdo web integrado a solução de segurança

4.5.3.2.2.2.2. Possuir pelo menos 80 categorias para classificação de sites web 4.5.3.2.2.2.3. Possuir base mínima contendo, 48 milhões de sites internet web já registrados e classificados;

4.5.3.2.2.2.4. Possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites web como:

a) Webmail;

b) Instituições de Saúde;

c) Notícias;

d) Pornografia;

e) Restaurante;

f) Mídias Sociais;

g) Esporte;

h) Educação;

i) Games;

j) Compras;

4.5.3.2.2.2.5. Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

4.5.3.2.2.2.6. Possuir sistema de cache interno, armazenando requisições WEB em disco local e memória;

4.5.3.2.2.2.7. Deve permitir a definição do tamanho mínimo dos objetos salvos em cache no disco;

4.5.3.2.2.2.8. Deve permitir a definição do tamanho máximo dos objetos salvos em cache em memória;

4.5.3.2.2.2.9. Deve atender a estrutura de navegação através de hierarquia de proxy com e sem autenticação;

4.5.3.2.2.2.10. Possibilitar a integração com servidores de cache WEB externos;

4.5.3.2.2.2.11. Deve ser capaz de armazenar cache dinâmicos para as atualizações Microsoft Windows Update;

Youtube, Sourceforge Downloads, Facebook, Google Maps;

4.5.3.2.2.2.12. Deve possuir a capacidade de excluir URL's específicas do cache web, configurável por listas de palavras chaves com suporte inclusive a expressões regulares;

4.5.3.2.2.2.13. Integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;

4.5.3.2.2.2.14. Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory, LDAP , TACACS+ e Radius;

4.5.3.2.2.2.15. Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança da contratante;

4.5.3.2.2.2.16. Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;

4.5.3.2.2.2.17. Deverá permitir o bloqueio de URLs inválidas cujo campo CN do certificado SSL não contém um domínio válido;

4.5.3.2.2.2.18. Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web;

4.5.3.2.2.2.19. Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;

4.5.3.2.2.2.20. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

4.5.3.2.2.2.21. Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem;

4.5.3.2.2.2.22. Possuir Logs e Relatórios de tempo de navegação de sites web

- Domínios Web;

4.5.3.2.2.2.23. Possuir recurso capaz de controlar e restringir o acesso a sites com base em seus nomes de domínio conhecido como DNS Content Filter;

4.5.3.2.2.3. Recursos do Proxy

4.5.3.2.2.3.1. Deverá funcionar em modo Proxy Explícito para HTTP, HTTPS, FTP, POP3 e SMTP e em Proxy

Transparente;

4.5.3.2.2.3.2. A solução deve ser capaz de identificar o comportamento do protocolo SSH onde pode ser feito através da inspeção do protocolo;

4.5.3.2.2.3.3. Deverá permitir configurar a porta do Proxy Explícito;

4.5.3.2.2.3.4. O equipamento deverá poder suportar funcionalidades de antispam sem a necessidade de equipamento dedicado.

4.5.3.2.3.Das Funcionalidades da Detecção de Intrusão e ATP 4.5.3.2.3.1. Das Funcionalidades da Detecção de Intrusão

4.5.3.2.3.1.1. A Detecção de Intrusão deverá ser baseada em appliance: 4.5.3.2.3.1.2. Possuir no mínimo 82.000 (oitenta e duas mil) assinaturas ou regras de IPS/IDS;

4.5.3.2.3.1.3. Permitir a criação de assinaturas customizadas pelo administrador do NGFW;

4.5.3.2.3.1.4. O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;

4.5.3.2.3.1.5. Possuir tecnologia de detecção baseada em assinatura;

4.5.3.2.3.1.6. Deverá suportar a implantação em modo Gateway, inline e em modo sniffer;

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

4.5.3.2.3.1.8. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação.

4.5.3.2.3.1.9. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos.

4.5.3.2.3.1.10. Possuir opção para administrador as listas de Blacklist, Whitelist e Quarentena com suporte a endereços IPv6.

4.5.3.2.3.1.11. Possuir capacidade de remontagem de pacotes para identificação de ataques;

4.5.3.2.3.1.12. Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque; Exemplo:

agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de Servidores Web;

4.5.3.2.3.1.13. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;

4.5.3.2.3.1.14. Mecanismos de detecção/proteção de ataques;
4.5.3.2.3.1.15. Reconhecimento de padrões;
4.5.3.2.3.1.16. Análise de protocolos; 4.5.3.2.3.1.17. Detecção de anomalias;
4.5.3.2.3.1.18. Detecção de ataques de RPC (Remote procedure call); 4.5.3.2.3.1.19. Proteção contra-ataques de Windows ou NetBios; 4.5.3.2.3.1.20. Proteção contra-ataques de SMTP (Simple Message Transfer
Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);
4.5.3.2.3.1.21. Proteção contra-ataques DNS (Domain Name System); 4.5.3.2.3.1.22. Proteção contra-ataques a FTP, SSH , Telnet e rlogin; 4.5.3.2.3.1.23. Proteção contra-ataques de ICMP (Internet Control Message
Protocol);

4.5.3.2.3.1.24. Alarmes na console de administração;
4.5.3.2.3.1.25. Alertas via correio eletrônico;

4.5.3.2.3.1.26. Monitoração do comportamento do appliance através de SNMP, o dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;

4.5.3.2.3.1.27. Capacidade de resposta/logs ativa a ataques;
4.5.3.2.3.1.28. Terminação de sessões via TCP resets;

4.5.3.2.3.1.29. Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;

4.5.3.2.3.1.30. O Sistema de detecção de Intrusos deverá atenuar os efeitos dos ataques de negação de serviços;

4.5.3.2.3.1.31. Possuir filtros de ataques por anomalias;

4.5.3.2.3.1.32. Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;

4.5.3.2.3.1.33. Permitir filtros de anomalias de protocolos;

4.5.3.2.3.1.34. Suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;

4.5.3.2.3.1.35. Suportar verificação de ataque nas camadas de aplicação;

4.5.3.2.3.2. Das Funcionalidades Do Threat Protection

4.5.3.2.3.2.1. Possuir funções de Antivírus, Anti-spyware;

4.5.3.2.3.2.2. Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, POP3, SMB/CIFS e FTP;

4.5.3.2.3.2.3. Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.)

4.5.3.2.3.2.4. Permitir o bloqueio de download de arquivos por extensão e tipo de arquivo;

4.5.3.2.4.Solução de Gerenciamento Centralizado de Firewall 4.5.3.2.4.1. Funcionalidades de Gerenciamento

4.5.3.2.4.1.1. Como boa prática de segurança e de mercado, a solução de gerência deverá ser separada do gateway de segurança, onde irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste projeto;

4.5.3.2.4.1.2. A solução de gerenciamento centralizado deve possibilitar o gerenciamento de todos os Firewall contratados.

4.5.3.2.4.1.3. A solução de gerenciamento centralizado deverá ser do mesmo fabricante da solução de segurança.

4.5.3.2.4.1.4. O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance físico deve ser compatível com rack 19 polegadas e possuir todos os acessórios necessários para sua instalação. Caso seja entregue em appliance virtual, deverá ser compatível com VMware ESXi e todo custo da infraestrutura necessária para suportar o appliance virtual é responsabilidade da CONTRATANTE;

4.5.3.2.4.1.5. Centralizar a administração de regras e políticas do(s) cluster(s), usando uma única interface de gerenciamento;

4.5.3.2.4.1.6. A solução deverá permitir seu gerenciamento por: CLI (Command Line Interface) via SSH, Web GUI utilizando protocolo HTTPS ou console gráfica;

4.5.3.2.4.1.7. Deve manter um canal de comunicação segura, com encriptação baseada em certificados, entre todos os componentes que fazem parte da solução de firewall.

gerência, armazenamento de logs e emissão de relatórios;

4.5.3.2.4.1.8. A solução deve incluir a opção de segmentar a base de regra utilizando rótulos ou títulos de seção para organizar melhor a política facilitando a localização e gestão do administrador;

4.5.3.2.4.1.9. A solução de gerência deverá prover fácil administração na aplicação das políticas para os gateways, sendo capaz de realizar o processo de alteração de regras e configuração de todas as soluções de segurança, que pode ser aplicada nos gateways remotos em uma única sessão, evitando qualquer tipo de retrabalho.

4.5.3.2.4.1.10. Deve possibilitar a realização de “backup” e restauração de dados.

4.5.3.2.4.1.11. Deve possibilitar a gerência de “logs”, realizando as configurações de relatórios de todos os “firewalls” integrados.

4.5.3.2.4.1.12. Deve permitir buscas e realizar análise de usuários e grupos, rastreando toda a sua atividade e uso da internet.

4.5.3.2.4.1.13. O gerenciamento deve permitir/possuir:

4.5.3.2.4.1.14. Criação e administração de políticas de Firewall, Controle de aplicação e IPS, Antivírus e Anti-Malware, Filtro de URL e prevenção contra ameaças avançadas;

4.5.3.2.4.1.15. Monitoração de logs;

4.5.3.2.4.1.16. Debugging;

4.5.3.2.4.1.17. Deve permitir usar palavras chaves para facilitar identificação de regras;

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

4.5.3.2.4.1.19. Autenticação integrada à base de dados local;

4.5.3.2.4.1.20. Deve possuir ferramenta para localização de objetos (por exemplo: endereço IP, Range de IP, subrede) na base de regras;

4.5.3.2.4.1.21. Criação de regras que fiquem ativas em horário definido; 4.5.3.2.4.1.22. Habilidade de upgrade via interface de gerenciamento; 4.5.3.2.4.1.23. Deverá ter a capacidade de gerar um relatório gráfico, que permita visualizar as mudanças na utilização de aplicações na rede, no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações, no tempo presente com relação ao passado;

4.5.3.2.4.1.24. Controle sobre todos os equipamentos da plataforma de proteção em uma única console, com administração de privilégios e funções;

4.5.3.2.4.1.25. Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de proteção;

4.5.3.2.4.1.26. Deve permitir a criação de objetos e políticas compartilhadas; 4.5.3.2.4.1.27. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

4.5.3.2.4.1.28. Solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

4.5.3.2.4.1.29. A solução deve permitir gerenciar templates de customização visual e marca do produto pelo sistema de gerenciamento centralizado e permitir aplicar nos NGFW´s gerenciados. Portanto, deve ser possível customizar a interface gráfica nos seguintes itens:

a) Título da Página;

b) Ícone (favicon);

c) Logotipo;

d) Imagem de fundo;

e) Cores do menu (primária e secundária);

4.5.3.2.4.1.30. O sistema deve ser capaz de gerenciar de modo central as políticas de backup do equipamento remotos;

4.5.3.2.4.1.31. O sistema deve permitir habilitar uma mensagem de Disclaimer na página de login da Interface de Administração. Ou seja, a página de login deverá apresentar um banner com uma mensagem customizada pelo administrador. Essa mensagem poderá ser utilizada para avisos de políticas de uso e compliance do sistema.

4.5.3.2.4.1.32. Deve suportar sistema de cluster do tipo Alta Disponibilidade para a solução ofertada;

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

4.5.3.2.4.1.34. Deve permitir inserir uma notificação do tipo "Login Disclaimer" que deve ser exibida na página de login da Interface de Administração da solução de gerenciamento centralizado.

4.5.3.2.4.1.35. Suportar API para integração com sistemas de terceiros;

4.5.3.2.4.2. Alta Disponibilidade

4.5.3.2.4.2.1. Deve suportar recurso de Alta-Disponibilidade (HA), sendo um primário e outros em modo secundário com sincronização e replicação das configurações;

4.5.3.2.4.2.2. O sistema de cluster deve suportar utilizar 02 (duas) interfaces como heatbeat;

4.5.3.2.4.2.3. Deve suportar definir o intervalo do sincronismo em minutos; 4.5.3.2.4.2.4. Permitir definir o número máximo de falhas dos testes do heartbeat e a solução somente irá convergir para o segundo equipamento após atingir o valor definido;

4.5.3.2.4.2.5. Suportar inserir um endereço de email para receber notificações relacionadas ao cluster.

4.5.3.2.4.3. Armazenamento e Gerenciamento de Logs e Eventos

4.5.3.2.4.3.1. A solução de armazenamento e gerenciamento de logs e eventos, deverá suportar, no mínimo, e estar licenciada para receber no mínimo 50GB de logs por dia;

4.5.3.2.4.3.2. A solução de armazenamento e gerenciamento de logs e eventos poderá ser entrega na mesma solução de gerenciamento centralizado, desde que atenda aos requisitos solicitados.

4.5.3.2.4.3.3. A solução de armazenamento e gerenciamento de logs e eventos deverá ser do mesmo fabricante da solução de segurança e compatível com a ferramenta de gerenciamento centralizado.

4.5.3.2.4.3.4. Deverá prover análise de tráfego de rede de modo centralizado; 4.5.3.2.4.3.5. Deve possuir análise de tráfego de rede e ameaças por geolocalização;

4.5.3.2.4.3.6. Deverá ser capaz de receber os logs e eventos com o objetivo de prover os seguintes tipos de análises:

4.5.3.2.4.3.7. Análise de ameaças e incidentes de segurança; 4.5.3.2.4.3.8. Análise de tráfego e uso de categorias Web; 4.5.3.2.4.3.9. Análise de tráfego e uso de aplicativos; 4.5.3.2.4.3.10. Análise de tráfego e ameaças por usuário; 4.5.3.2.4.3.11. Análise de desempenho de políticas de segurança;

4.5.3.2.4.3.12. A solução ofertada deve ser capaz de fazer o gerenciamento centralizado de logs, consolidação de logs, arquivamento de logs, busca avançada de logs;

4.5.3.2.4.3.13. Deverá possuir ferramenta para salvar consultas avançadas; 4.5.3.2.4.3.14. Deve possuir relatórios personalizados;

4.5.3.2.4.3.15. Deverá ser capaz de efetuar o arquivamento de relatórios; 4.5.3.2.4.3.16. Deve possuir agendamento de relatórios;

4.5.3.2.4.3.17. Os Relatórios deverão, no mínimo, serem exportados em formatos flexíveis (PDF, CSV);

4.5.3.2.4.3.18. Logs e Relatórios de tempo de navegação de sites web - Domínios Web;

4.5.3.2.4.3.19. Permitir o envio de relatórios por e-mail; 4.5.3.2.4.3.20. Relatório por Dispositivo/Consolidado;

4.5.3.2.5. Tabela de Distribuição do Item 1

SUBITEM DO TR Nº	DESCRIÇÃO	QTDE
4.5.3.1.1	APPLIANCE NGFW DE 5 GBPS DE CAPACIDADE DE FIREWALL	157
4.5.3.1.2	APPLIANCE NGFW DE 9.7 GBPS DE CAPACIDADE DE FIREWALL	11
4.5.3.1.3	APPLIANCE NGFW DE 11.8 GBPS DE CAPACIDADE DE FIREWALL	3
4.5.3.1.4	APPLIANCE NGFW DE 19.4 GBPS DE CAPACIDADE DE FIREWALL	2
4.5.3.2.4	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE FIREWALL	1

4.5.3.3. **A solução de segurança cibernética de bloqueio de ameaças, conforme ITEM 2, deve possuir as seguintes características:**

4.5.3.3.1. Interface e Gestão:

4.5.3.3.1.1. Deve ser instalado em equipamento com S.O. Linux, Unix ou BSD.
4.5.3.3.1.2. Deve ter uma interface amigável para configuração e gestão.
4.5.3.3.1.3. Não deve possuir endereçamento IP nas interfaces pelas quais passam o tráfego internet.
4.5.3.3.1.4. Não deve permitir a identificação da existência da solução.
4.5.3.3.1.5. Não ser suscetível à exploração externa de possíveis

vulnerabilidades no software.

4.5.3.3.1.6. Deve permitir instalação de forma transparente, sem necessidade de alterações nas configurações lógicas de rede, IP ou do roteamento do ambiente atual.

4.5.3.3.1.7. Deve atuar diretamente no tráfego de entrada da internet.

4.5.3.3.1.8. Deve proporcionar proteção abrangente para toda a infraestrutura, desde o firewall podendo incluir os roteadores à internet.

4.5.3.3.1.9. O aumento de latência no tráfego de rede não deve ser superior a 5 milésimos de segundo.

4.5.3.3.1.10. Deve permitir comunicação com a internet através de proxy.

4.5.3.3.1.11. Deve possuir painel para configuração de mecanismo para detecção de acesso indesejado.

4.5.3.3.1.12. Deve possuir painel para configuração de origens confiáveis.

4.5.3.3.1.13. Deve possuir mecanismo de autoproteção.

4.5.3.3.1.14. Deve possuir log de auditoria de tudo que foi feito na solução, devendo no mínimo identificar user, data-hora e atividade realizada.

4.5.3.3.1.15. Deve armazenar no mínimo os últimos 8.000 registros de log de auditoria.

4.5.3.3.2. Inteligência Artificial Avançada:

4.5.3.3.2.1. Deve ser uma solução baseada em Inteligência Artificial Preditiva.

4.5.3.3.2.2. Deve ser capaz de analisar padrões de comportamento no tráfego de internet. 4.5.3.3.2.3. Deve identificar origens maliciosas e neutralizá-las imediatamente e automaticamente, sem intervenção humana.

4.5.3.3.2.4. A solução não deve depender de assinaturas para reconhecer tráfegos indesejados.

4.5.3.3.2.5. Deve criar uma blacklist local com as origens maliciosas.

4.5.3.3.2.6. Deve possuir mecanismo de gestão do tempo de guarda dos dados da blacklist. 4.5.3.3.2.7. Deve possuir capacidade de aprendizado de acessos indesejados.

4.5.3.3.3. Taxa de Falso Positivo:

4.5.3.3.3.1. Deve apresentar uma taxa de falso positivo inferior a 0,0001% (uma identificação errada a cada um milhão de identificações), garantindo precisão nas identificações e bloqueios.

4.5.3.3.4. Proteção Contra Ataques de "Zero Day":

4.5.3.3.4.1. Deve oferecer proteção eficaz contra ataques de "Zero Day", mesmo aqueles que ainda não tenham sido identificados e que ainda não possuam "assinatura de identificação" ou "patch de correção".

dos fabricantes das outras soluções informáticas que o órgão disponibiliza na internet.

4.5.3.3.5. Visibilidade:

4.5.3.3.5.1. Deve fornecer visibilidade das origens maliciosas dos ataques.

4.5.3.3.5.2. Deve fornecer visibilidade das tentativas de acessos bloqueadas.

4.5.3.3.5.3. Deve fornecer visibilidade dos serviços de rede alvos de ataques.

4.5.3.3.5.4. Deve possuir funcionalidade que permita identificar de forma fácil e ágil o motivo do bloqueio do ataque.

4.5.3.3.5.5. Deve apresentar um dashboard para a equipe de monitoramento (SOC) com mapa dos países dos IPS atacantes.

4.5.3.3.5.6. Deve apresentar um dashboard para a equipe de monitoramento (SOC) com mapa dos países de onde foram gerados os ataques.

4.5.3.3.5.7. Deve permitir a consulta através de vários tipos de indicadores como por exemplo, IP de origem, IP de Destino, Porta de origem, Porta de destino entre outros.

4.5.3.3.5.8. Deve possuir funcionalidade de geolocalização de IP identificado como malicioso.

4.5.3.3.5.9. Deve possuir busca de CVEs na base do MITRE.

4.5.3.3.5.10. Deve possuir mecanismo de autogestão do armazenamento dos logs de ataque.

4.5.3.3.6. Relatórios e Integrações:

4.5.3.3.6.1. Deve permitir integração, através de API, com outros equipamentos/soluções de segurança como por exemplo firewall ou soluções de observabilidade.

4.5.3.3.6.2. Deve permitir envio dos logs de ataques para servidor externo.

4.5.3.3.6.3. Deve possuir integração com rede externa de Inteligência de Ameaças Global, com capacidade de aprendizado sobre novas ameaças identificadas exercendo atividade hacker recente pelo mundo e, de forma automática e pró-ativa, ativar proteção contra essas origens.

4.5.3.3.6.4. Deve gerar relatório gerencial mensal com pelo menos as seguintes informações: quantidade de ataques, bloqueios, origens mais frequentes, países de origem e serviços mais atacados.

4.5.3.3.6.5. Deve possuir capacidade suficiente para armazenar e disponibilizar consultas aos relatórios gerenciais mensais de pelo menos 5 anos.

4.5.3.3.6.6. Deve permitir exportar os relatórios para PDF.

4.5.3.3.7. Especificações Técnicas do Equipamento

4.5.3.3.7.1. **O equipamento físico deve atender aos seguintes requisitos:**

4.5.3.3.7.1.1. Dimensões e Montagem:

4.5.3.3.7.1.1.1. Deve ser compatível com rack de 19 polegadas, com tamanho de 1U ou 2U.

4.5.3.3.7.1.2. Conectividade:

4.5.3.3.7.1.2.1. Deve possuir no mínimo 8 interfaces de rede Gigabit Ethernet com conexão do tipo RJ45.

4.5.3.3.7.1.2.2. Deve ter porta console para configuração local. 4.5.3.3.7.1.2.3. Deve possuir interface de rede exclusiva para acesso e gerenciamento interno do equipamento.

4.5.3.3.7.1.3. Alimentação elétrica:

4.5.3.3.7.1.3.1. Deve ter fonte de alimentação elétrica VAC automática nos padrões brasileiros conforme a continuidade operacional.

4.5.3.4. Os serviços e equipamentos do ITEM 3 deverão ser entregues no formato e características técnicas bem como funcionalidades conforme especificações abaixo:

4.5.3.4.1. O serviço de acesso à Internet compreenderá a instalação, operação, manutenção e gerenciamento da infraestrutura de acesso à Internet através de roteador PE, integrado imediatamente ao roteamento BGP da Operadora. Entende-se operadora, Provedor de Internet Autônomo, ou seja, que possua ASN (Autonomous System Number) vinculado a um CNPJ de um ISP distinto, ou seja, a CONTRATADA deverá suportar a operação através de dois link dedicado distintos, oriundo de 02(dois) ASN diferentes, através de infraestrutura de chegada ao prédio da Prefeitura percorrida por caminhos diferentes, visando a eventual queda de um dos link não haver impacto na operação como um todo.

4.5.3.4.2. Cada link deverá ser entregue com blocos blocos IPV4 /29 e IPV6 /64, públicos, os quais serão cadastrados no portal numeração.br, compreendendo inicialmente banda de 500 Mbps mas a porta de rede não pode haver limite rate, devendo suportar os serviço em wire speed, pois eventual queda de um dos link, a operadora redundante deverá suportar o tráfego na integralidade.

4.5.3.4.3. Conforme topologia da rede, a CONTRATADA deverá entregar o link em duas portas distintas, uma porta conectada no equipamento de cibersegurança A e outra porta a ser conectada no equipamento de cibersegurança B. Tal feito se repetirá em cada ASN, conforme topologia apresentada.

4.5.3.4.4. Em caso de falha no equipamento A, o serviço deverá realizar a migração automática para o equipamento redundante em regime de failover, sem necessidade de configurações

adicionais ou intervenções técnicas. O mesmo procedimento deverá ocorrer em situação inversa. Caso este Termo de Referência não detalhe alguma instrução específica, caberá à CONTRATADA assegurar a entrega da solução em pleno funcionamento, incluindo todos os custos inerentes à implantação, sem qualquer cobrança adicional.

4.5.3.4.5. A CONTRATADA deverá fornecer todos os equipamentos, acessórios e demais componentes indispensáveis à disponibilização do serviço no local designado, ainda que não estejam expressamente mencionados neste Termo de Referência, desde que sejam essenciais à operação da solução ou ao cumprimento das funcionalidades e configurações exigidas, sem gerar ônus adicionais à CONTRATANTE.

4.5.3.4.6. O acesso entre a operadora e o ambiente de TI da CONTRATANTE deverá ser feito exclusivamente por meio de fibra óptica da CONTRATADA.

4.5.3.4.7. Devem transportar pacotes IPv4 e IPv6 com no mínimo 1500 bytes sem exigir a fragmentação dos mesmos na camada 3 do modelo OSI.

4.5.3.4.8. Os links devem suportar IPv6, sendo necessário o fornecimento de endereçamento para as redes internas do CONTRATANTE.

4.5.3.4.9. Deverão ser fornecidos 1 (roteador) por link dedicado que irá compor o ambiente de alta disponibilidade.

4.5.3.4.10. Deverá suportar todos os protocolos de roteamento necessários para suportar as conexões WANs em ambiente de alta disponibilidade (OSPF, BGP, RIP etc).

4.5.3.4.11. Cada equipamento deve possuir no mínimo 2 (duas) interfaces WAN de 1 Gbps e 2 (duas) ou mais interfaces LAN de 1 Gbps.

4.5.3.4.12. Possuir LEDs de diagnóstico sobre alimentação, atividade e diagnóstico das portas. 4.5.3.4.13. Deve possuir funcionalidades necessárias para monitoramento, diagnóstico e features como QoS, permitir a atualização remota do SO e arquivos de configuração via ethernet ou serial, FTP e TFTP; Permitir a gravação de log externo via syslog; Suportar o recurso port mirroring para um endereço IP; e suportar protocolo de coleta de tráfego Netflow ou IPFIX para a realização de coleta de informações de fluxo, tráfego que circulam no equipamento.

4.5.3.5. Os serviços e equipamentos dos ITENS 4 e 5 deverão ser entregues no formato e características técnicas bem como funcionalidades conforme especificações abaixo:

4.5.3.5.1. As velocidades de acesso à internet contratadas serão classificadas da seguinte maneira: 4.5.3.5.1.1. Link principal (item 4): 150Mbps
4.5.3.5.1.2. Link redundante (item 5): 75Mbps

4.5.3.5.1.2.1. A CONTRATADA deverá comprovar que possui capacidade de operar com dois circuitos distintos, em fibra óptica.

4.5.3.5.1.2.2. A CONTRATADA deverá comprovar que possui capacidade operacional através de redes espectrais.

4.5.3.5.2. A CONTRATADA deverá garantir largura de banda simétrica (download/upload) de 100% da velocidade contratada, em link único para o link principal (Item 4), não sendo aceita a agregação de múltiplos links para atingir a velocidade contratada.

4.5.3.5.3. A CONTRATADA deverá garantir largura de banda simétrica (download/upload) de pelo menos 70% da velocidade contratada, podendo ser em 02(dois) link (Item 4), um link performando em fibra óptica e outro através de chip especial para suportar esta operação estruturante, não sendo possível chip de dados convencionais, com limite de dados. Neste caso específico será aceito a agregação desses 2 link em comento, para atingir a velocidade contratada.

4.5.3.5.4. A localização e classificação de cada unidade está relacionada nos itens 7.2.1.3.1, 7.2.1.3.2 e 7.2.1.3.3.

4.5.3.5.5. O acesso de fibra óptica até o ambiente de TI da CONTRATANTE deverá ser feito exclusivamente por meio de fibra óptica da CONTRATADA, exceto chip 4/5Gbps.

4.5.3.5.6. Cada acesso de fibra óptica ao ambiente de TI deve ser percorrido por caminhos distintos; não serão aceitos acessos de redes convergindo para um mesmo ISP, sendo necessária a validação de comprovação deste quesito no momento do certame.

4.5.3.6. Requisitos Tecnológicos Mínimos Para Suportar a Conectividade das Praças

4.5.3.6.1. Ponto de Acesso Outdoor Wi-Fi 6 2x2 4.5.3.6.1.1. Conectividade:

4.5.3.6.1.1.1. Deve possuir, no mínimo, 1 porta uplink ethernet 100/1000/2.5G Base-T em conector RJ45 com suporte a alimentação PoE compatível com o padrão IEEE 802.3at e com reconhecimento automático de crossover MDI/MDIX;

4.5.3.6.1.1.2. Deve possuir 1 porta LAN ethernet 100/1000Base-T em conector RJ45 e com reconhecimento automático de crossover MDI/MDIX;

4.5.3.6.1.1.3. Possuir porta de console para gerenciamento e configuração via linha de comando (CLI – command line interface) com conector RJ-45 diferente da porta de rede solicitada anteriormente;

4.5.3.6.1.1.4. Deve possuir 2 rádios operando nas frequências de 2,4GHz e 5GHz simultaneamente;

4.5.3.6.1.1.5. Deve possuir rádio Bluetooth Low-Energy (BLE) integrado ao equipamento;

4.5.3.6.1.1.6. Deve possuir antenas omnidirecionais internas ao equipamento com ganho mínimo de 5 dBi na frequência de 2,4GHz, 6 dBi na frequência de 5GHz;

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

4.5.3.6.1.1.8. Deve possuir LEDs indicadores de conectividade;

4.5.3.6.1.2. Funcionalidades WLAN Deve Atender aos Seguintes Padrões:

4.5.3.6.1.2.1. IEEE 802.11a/b/g/n/ac/ax; 4.5.3.6.1.2.2. Dupla banda 2,4 e 5GHz simultâneas;

4.5.3.6.1.2.3. Deve operar em MIMO 2x2 com suporte a 2 spatial streams e suporte a MU-MIMO;

4.5.3.6.1.2.4. Deve suportar as seguintes taxas de dados:

a) IEEE 802.11b: 1, 2, 5.5, 11 Mbps;

b) IEEE 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps;

c) IEEE 802.11n: 6.5 – 300 Mbps (20 / 40 MHz);

d) IEEE 802.11ac: 6.5 – 866 Mbps (20 / 40 / 80 MHz);

e) IEEE 802.11ax: 3.6 - 574 Mbps (2.4GHz, 20 / 40 MHZ)

f) IEEE 802.11ax: 3.6 - 2400 Mbps (5GHz, 20 / 40 / 80 / 160MHz)

4.5.3.6.1.2.5. Deve oferecer potência mínima de transmissão RF de 26dBm em 2,4GHz e 25dBm em 5GHz;

4.5.3.6.1.2.6. Deve suportar no mínimo 16 SSIDs simultaneamente por rádio totalizando até 32 SSIDs no sistema;

4.5.3.6.1.2.7. Deve suportar a configuração de no mínimo 16 VLANs ativas simultaneamente por rádio totalizando até 32 VLANs ativas simultaneamente no sistema;

4.5.3.6.1.2.8. O equipamento proposto deverá poder operar nos seguintes modos:

a) Access Point;

b) Wireless Mesh;

4.5.3.6.1.2.9. Deverá permitir o controle de tráfego para cada SSID; 4.5.3.6.1.2.10. Deverá selecionar dinamicamente os canais de operação; 4.5.3.6.1.2.11. Deverá selecionar automaticamente a melhor opção de conexão dos clientes (Band Steering);

4.5.3.6.1.3. Gerenciamento

4.5.3.6.1.3.1. Deve suportar gerenciamento SNMP v2c;

4.5.3.6.1.3.2. Deve permitir configuração dos parâmetros IP através de serviço DHCP Cliente;

4.5.3.6.1.3.3. Deve permitir acesso remoto a console via HTTP e HTTPs;

4.5.3.6.1.3.4. Deve permitir a atualização de firmware via TFTP ou HTTP;

4.5.3.6.1.3.5. Deve suportar sincronização de relógio através de SNTP ou NTP;

4.5.3.6.1.3.6. Deve suportar atualização automática do firmware quando estiver operando em modo gerenciado;

4.5.3.6.1.3.7. Deve suportar plataforma em nuvem que permite o gerenciamento de pontos de acesso de diferentes fabricantes;

4.5.3.6.1.4. Segurança

4.5.3.6.1.4.1. Deve suportar autenticação através de servidor RADIUS;

4.5.3.6.1.4.2. Deve suportar WiFi Protected Access (WPA/WPA2);

4.5.3.6.1.4.3. Deve suportar WPA/WPA2 (PSK);

4.5.3.6.1.4.4. Deve suportar WPA3;

4.5.3.6.1.4.5. Deve permitir bloqueio da divulgação do SSID;

4.5.3.6.1.5. Gerais

4.5.3.6.1.5.1. Deve suportar fonte de alimentação DC externa operando em tensões de 100 a 240 V e em frequências de 50 a 60 Hz automaticamente;

4.5.3.6.1.5.2. Deve possuir a classificação IP68 de resistência a intempéries;

4.5.3.6.1.5.3. Deve permitir montagem em parede ou poste;

4.5.3.6.1.5.4. Deve suportar temperatura de operação entre - 40°C a 60°C;

4.5.3.6.1.5.5. Deve suportar sistema operacional em conformidade com o OpenWiFi da Telecom Infra Project;

4.5.3.6.1.5.6. Deverá suportar o padrão OpenRoaming para garantir a facilidade e segurança de conexão dos clientes à rede sem fio, permitindo a ampla utilização da rede pelos usuários finais;

4.5.3.6.1.5.7. A controladora deve permitir que o access point seja controlado simultaneamente com access points de diferentes fabricantes

4.5.3.6.1.5.8. A empresa fornecedora da solução deverá apresentar uma prova de conceito (PoC) comprovando o funcionamento da controladora gerenciando no mínimo 2 access points de fabricantes diferentes

4.5.3.6.1.5.9. A empresa fornecedora deverá possuir atestado de capacidade de implementação de solução equivalente com ecossistema OpenWiFi

4.5.3.6.2. Ponto de Acesso Indoor Wi-Fi 6 2x2 4.5.3.6.2.1. Conectividade

4.5.3.6.2.1.1. Deve possuir, no mínimo, 1 porta uplink ethernet 100/1000/2.5G Base-T em conector RJ45 com suporte a alimentação PoE compatível com o padrão IEEE 802.3at e com reconhecimento automático de crossover MDI/MDIX;

4.5.3.6.2.1.2. Deve possuir 1 porta LAN ethernet 100/1000Base-T em conector RJ45 e com reconhecimento automático de crossover MDI/MDIX;

4.5.3.6.2.1.3. Possuir porta de console para gerenciamento e configuração via linha de comando (CLI – command line interface) com conector RJ-45 diferente da porta de rede solicitada anteriormente;

4.5.3.6.2.1.4. Deve possuir 1 porta USB;

4.5.3.6.2.1.5. Deve possuir 2 rádios operando nas frequências de 2,4GHz e 5GHz simultâneamente;

4.5.3.6.2.1.6. Deve possuir rádio Bluetooth Low-Energy (BLE) integrado ao equipamento;

4.5.3.6.2.1.7. Deve possuir antenas omnidirecionais internas ao equipamento com ganho mínimo de 4 dBi na frequência de 2,4GHz, 6 dBi na frequência de 5GHz e 4 dBi para BLE;

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

4.5.3.6.2.1.9. Deve possuir LEDs indicadores de conectividade WLAN e Power/Diag;

4.5.3.6.2.2. Funcionalidades WLAN Deve Atender aos Seguintes Padrões:

4.5.3.6.2.2.1. IEEE 802.11a/b/g/n/ac/ax; 4.5.3.6.2.2.2. Dupla banda 2,4 e 5GHz simultâneas;

4.5.3.6.2.2.3. Deve operar em MIMO 2x2 com suporte a 2 spatial streams e suporte a MU-MIMO;

4.5.3.6.2.2.4. Deve suportar as seguintes taxas de dados:

a) IEEE 802.11b: 1, 2, 5.5, 11 Mbps;

b) IEEE 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps;

c) IEEE 802.11n: 6.5 – 300 Mbps (20 / 40 MHz);

d) IEEE 802.11ac: 6.5 – 866 Mbps (20 / 40 / 80 MHz);

e) IEEE 802.11ax: 3.6 - 574 Mbps (2.4GHz, 20 / 40 MHZ)

f) IEEE 802.11ax: 3.6 - 1200 Mbps (5GHz, 20 / 40 / 80 MHz)

4.5.3.6.2.2.5. Deve oferecer potência mínima de transmissão RF de 23dBm em 2,4GHz e 23dBm em 5GHz;

4.5.3.6.2.2.6. Deve suportar Wi-Fi Multimedia (WMM);

4.5.3.6.2.2.7. Deve suportar no mínimo 16 SSIDs simultaneamente por rádio totalizando até 32 SSIDs no sistema;

4.5.3.6.2.2.8. Deve suportar a configuração de no mínimo 16 VLANs ativas simultaneamente por rádio totalizando até 32 VLANs ativas simultaneamente no sistema;

4.5.3.6.2.2.9. O equipamento proposto deverá poder operar nos seguintes modos:

a) Access Point;

b) Wireless Mesh;

4.5.3.6.2.2.10. Deverá permitir o controle de tráfego para cada SSID; 4.5.3.6.2.2.11. Deverá selecionar dinamicamente os canais de operação; 4.5.3.6.2.2.12. Deverá selecionar automaticamente a melhor opção de conexão dos clientes (Band Steering);

4.5.3.6.2.3. Gerenciamento

4.5.3.6.2.3.1. Deve suportar gerenciamento SNMP v2c;

4.5.3.6.2.3.2. Deve permitir configuração dos parâmetros IP através de serviço DHCP Cliente;

4.5.3.6.2.3.3. Deve permitir acesso remoto a console via HTTP e HTTPs;

4.5.3.6.2.3.4. Deve permitir a atualização de firmware via TFTP ou HTTP;

4.5.3.6.2.3.5. Deve suportar sincronização de relógio através de SNTP ou NTP;

4.5.3.6.2.3.6. Deve suportar atualização automática do firmware quando estiver operando em modo gerenciado;

4.5.3.6.2.3.7. Deve suportar plataforma em nuvem que permite o gerenciamento de pontos de acesso de diferentes fabricantes;

4.5.3.6.2.4. Segurança

4.5.3.6.2.4.1. Deve suportar autenticação através de servidor RADIUS;

4.5.3.6.2.4.2. Deve suportar WiFi Protected Access (WPA/WPA2);

4.5.3.6.2.4.3. Deve suportar WPA/WPA2 (PSK);

4.5.3.6.2.4.4. Deve suportar WPA3;

4.5.3.6.2.4.5. Deve permitir bloqueio da divulgação do SSID;

4.5.3.6.2.4.6. Desempenho

4.5.3.6.2.4.7. Deve possibilitar a conexão de até 250 clientes concorrentes por rádio totalizando 500 simultaneamente;

4.5.3.6.2.5. Gerais

4.5.3.6.2.5.1. Deve suportar fonte de alimentação DC externa operando em tensões de 100 a 240 V e em frequências de 50 a 60 Hz automaticamente;

4.5.3.6.2.5.2. Deve permitir montagem em parede ou teto e vir acompanhado dos devidos kits de instalação;

4.5.3.6.2.5.3. Deve permitir a instalação de trava tipo Kensington; 4.5.3.6.2.5.4. Deve suportar temperatura de operação entre 0°C a 50°C; 4.5.3.6.2.5.5. Possuir certificado válido de homologação emitido pela Anatel. 4.5.3.6.2.5.6. Deverá ser apresentado certificado válido de interoperabilidade fornecido pela Wi-Fi Alliance na categoria de Enterprise Access Point;

4.5.3.6.2.5.7. Deve suportar sistema operacional em conformidade com o OpenWiFi da Telecom Infra Project;

4.5.3.6.2.5.8. Deverá suportar o padrão OpenRoaming para garantir a facilidade e segurança de conexão dos clientes à rede sem fio, permitindo a ampla utilização da rede pelos usuários finais;

4.5.3.6.2.5.9. A controladora deve permitir que o access point seja controlado simultaneamente com access points de diferentes fabricantes

4.5.3.6.2.5.10. A empresa fornecedora da solução deverá apresentar uma prova de conceito (PoC) comprovando o funcionamento da controladora gerenciando no mínimo 2 access points de fabricantes diferentes

4.5.3.6.2.5.11. A empresa fornecedora deverá possuir atestado de capacidade de implementação de solução equivalente com ecossistema OpenWiFi

4.5.3.6.3. Switch de Acesso POE 8 Portas 2.5base-T e 2 Portas 10G SFP+ 4.5.3.6.3.1. Conectividade

4.5.3.6.3.1.1. Deve possuir 8 portas padrão 2.5G/1000 Base-T em conector RJ45 compatível com o padrão IEEE 802.3az de eficiência energética;

4.5.3.6.3.1.2. Deve possuir no mínimo 2 portas 10G Base-X padrão SFP+ para a instalação de módulos padrão SFP+ ou cabos DAC;

4.5.3.6.3.1.3. As portas Base-T deverão suportar autonegociação de velocidade, modo de operação e detecção MDI/MDIX;

4.5.3.6.3.1.4. Deve possuir porta console serial padrão RS-232 em conector DB-9 ou RJ45 acompanhado do respectivo cabo para conexão ao PC;

4.5.3.6.3.2. PoE

4.5.3.6.3.2.1. Deve suportar alimentação PoE conforme o padrão IEEE 802.3af/802.3at nas 8 portas RJ45 dentro da disponibilidade de potência destinada a esse fim;

4.5.3.6.3.2.2. Deve suportar alimentação PoE++ conforme o padrão IEEE 802.3bt em, no mínimo, 4 portas RJ45 de forma simultânea;

4.5.3.6.3.2.3. Deve possibilitar visualização da alimentação através de LED exclusivo ou de múltipla funcionalidade;

4.5.3.6.3.2.4. Deve disponibilizar no mínimo 240W para utilização exclusiva no PoE sem utilização de fonte adicional para esse fim;

4.5.3.6.3.3. Controle

4.5.3.6.3.3.1. Deve suportar Jumbo Frames de 12K;

4.5.3.6.3.3.2. Deve suportar até 4K VLANs segundo o protocolo IEEE 802.1Q, por porta e por protocolo;

4.5.3.6.3.3.3. Deve suportar implementação de VLANs Privativas;

4.5.3.6.3.3.4. Deve suportar implementação de Voice VLANs;

4.5.3.6.3.3.5. Deve implementar suporte a QinQ;

4.5.3.6.3.3.6. Possuir no mínimo oito filas em hardware para priorização de tráfego por porta;

4.5.3.6.3.3.7. Implementar QoS com base no protocolo 802.1p e DSCP;

4.5.3.6.3.3.8. Deve implementar controle de fluxo com o protocolo 802.3X e Back Pressure;

4.5.3.6.3.3.9. Deve implementar IGMP Snooping v1, v2 e v3;

4.5.3.6.3.3.10. Deve implementar IGMP Filtering, Immediate Leave e Querier;

4.5.3.6.3.3.11. Deve implementar MLD Snooping;

4.5.3.6.3.3.12. Deve possibilitar a limitação de Broadcast, Multicast e Unicast;

4.5.3.6.3.3.13. Deve implementar o gerenciamento de banda com valores distintos para entrada e saída;

4.5.3.6.3.3.14. Deve implementar os mecanismos de controle de fila: SP (Strict Priority) e WRR (Weighted Round Robin);

4.5.3.6.3.4. Disponibilidade

4.5.3.6.3.4.1. Implementar o protocolo Spanning Tree (802.1D);
4.5.3.6.3.4.2. Implementar o protocolo Rapid Spanning Tree (802.1w); 4.5.3.6.3.4.3. Deve implementar o protocolo Multiple Spanning Tree
(802.1s);

4.5.3.6.3.4.4. Deve suportar detecção de laço (loopback detection);
4.5.3.6.3.4.5. Deve implementar BPDU Guard/Filter e ROOT Guard; 4.5.3.6.3.4.6. Deve suportar até 8 grupos de agregação dinâmicos no padrão
LACP ou estático de até 8 portas GbE;

4.5.3.6.3.5. Gerenciamento

4.5.3.6.3.5.1. Deve possuir suporte a pilha dupla de protocolo IPv4/IPv6; 4.5.3.6.3.5.2. Deve suportar gerenciamento SNMP v1, v2c e v3; 4.5.3.6.3.5.3. Deve permitir configuração dos parâmetros IP através de
serviço DHCP Cliente;

4.5.3.6.3.5.4. Deve permitir acesso remoto a console via Telnet, SSHv2, HTTP e HTTPs;

4.5.3.6.3.5.5. Deve permitir configuração através de plataforma de gerenciamento em nuvem com suporte a OpenLan Switching (OLS) e OpenWiFi em conformidade com as especificações da Telecom Infra Project (TIP);

4.5.3.6.3.5.6. Deve permitir acesso local a console CLI;

4.5.3.6.3.5.7. Deve permitir atualização e provisionamento automáticos, podendo este ser executado por sistema de gestão externo sendo, neste caso, necessário proporcionar a solução completa;

4.5.3.6.3.5.8. Deve suportar os grupos 1, 2, 3 e 9 de RMON;

4.5.3.6.3.5.9. Deve suportar o protocolo LLDP (IEEE 802.1ab);

4.5.3.6.3.5.10. Deve permitir armazenar no mínimo duas imagens de firmware em memória flash interna;

4.5.3.6.3.5.11. Deve permitir a atualização de firmware via HTTP;

TFTP ou FTP em memória tipo flash;

4.5.3.6.3.5.12. Deve permitir armazenar no mínimo duas configurações distintas em memória flash interna;

4.5.3.6.3.5.13. Deve permitir salvar as configurações em um computador local (backup) via HTTP, TFTP ou FTP;

4.5.3.6.3.5.14. Deve suportar espelhamento de tráfego; 4.5.3.6.3.5.15. Deve suportar SNMP over IPv6; 4.5.3.6.3.5.16. Deve suportar HTTP over IPv6; 4.5.3.6.3.5.17. Deve suportar IPv6 remote ping; 4.5.3.6.3.5.18. Deve suportar NTP ou SNTP;

4.5.3.6.3.5.19. Deve implementar log de eventos em memória flash e permitir a gravação em servidor externo padrão Syslog;

4.5.3.6.3.6. Segurança

4.5.3.6.3.6.1. Deve possuir proteção a ataques Denial of Service; 4.5.3.6.3.6.2. Deve suportar autenticação local e através de servidor RADIUS e TACACS+;

4.5.3.6.3.6.3. Deve implementar segurança de acesso através do protocolo IEEE 802.1X e autenticação por MAC;

4.5.3.6.3.6.4. Deve suportar assinalamento automático de VLAN e política de QoS;

4.5.3.6.3.6.5. Deve possuir suporte à AAA (Authentication, Authorization and Account) em servidores RADIUS ou TACACS+;

4.5.3.6.3.6.6. Deve suportar implementação de VLANs para visitantes; 4.5.3.6.3.6.7. Deve permitir filtragem de pacotes identificados por cabeçalho ethernet ou IP;

4.5.3.6.3.6.8. Deve suportar DHCP snooping; 4.5.3.6.3.6.9. Deve suportar IP Source Guard;

4.5.3.6.3.6.10. Deve possuir Port Security ou funcionalidade similar; 4.5.3.6.3.6.11. Deve possuir Dynamic ARP Inspection ou funcionalidade similar;

4.5.3.6.3.6.12. Deve implementar MAC based ACL;

4.5.3.6.3.7. Desempenho

4.5.3.6.3.7.1. Deve possuir capacidade de vazão de ao menos 80 Gbps; 4.5.3.6.3.7.2. Deve chavear no mínimo 59 Mpps;

4.5.3.6.3.7.3. Tabela de endereços MAC com capacidade para no mínimo

16.000 endereços;

4.5.3.6.3.7.4. Funções camada 3

4.5.3.6.3.7.5. Deve implementar rotas estáticas; 4.5.3.6.3.7.6. Deve implementar o protocolo RIP;

4.5.3.6.3.8. Padronização

4.5.3.6.3.8.1. Deve ser compatível com os seguintes padrões:

a) IEEE 802.1D (STP)

b) IEEE 802.1p (COS)

c) IEEE 802.1Q (VLAN)

d) IEEE 802.1s (MSTP)

e) IEEE 802.1v (VLAN)

f) IEEE 802.1w (RSTP)

g) IEEE 802.1X (Security)

h) IEEE 802.3ad (Link aggregation)

i) IEEE 802.3x (Flow control)

j) IEEE 802.3z (Gigabit)

k) IEEE 802.1AB (Link Layer Discovery Protocol)

l) IEEE 802.3az (Energy Efficiency)

4.5.3.6.3.9. Gerais

4.5.3.6.3.9.1. Deve possuir fonte de alimentação interna operando em tensões de 100 a 240 V e em frequências de 50 a 60 Hz automaticamente;

4.5.3.6.3.9.2. Deve vir acompanhado do kit de suporte específico para montagem em Rack de 19;

4.5.3.6.3.9.3. O equipamento deverá ocupar uma unidade de rack; 4.5.3.6.3.9.4. Deve possuir temperatura de operação de 0° C a 50° C; 4.5.3.6.3.9.5. Deve possuir sistema operacional OpenLan Switching (OLS) em conformidade com as especificações da Telecom Infra Project (TIP);

4.6. O sistema de gerenciamento de acesso das praças deverá ser de responsabilidade da Contratada seguindo todas as normas da lei 13.709/2018 (LEI GERAL DE PROTEÇÃO DE DADOS - LGPD) e Lei Federal nº 12.965/2014, Decreto Federal nº 8.771/2016 que regulamenta o Marco Civil da Internet e demais legislações Federais ou Municipais relativas à matéria.

4.7. O caráter confidencial das informações dos usuários será garantido, não podendo ser compartilhado em nenhuma hipótese, inclusive para uso comercial, publicitário ou estatístico.

4.8. A contratada deverá fornecer acesso ao sistema de gerenciamento das Praças, quantidade de acesso, acesso para inserção de informações e ações da Prefeitura e demais secretarias, não sendo aceito propagandas da contratada.

4.9. O SSID da rede não poderá associar o nome do eventual contratante privado.

4.10. O formato do SSID será definido pela Prefeitura Municipal de Cáceres / Coordenação de Tecnologia da Informação (CTI).

4.11. A Contratada deverá fornecer o sistema de gerenciamento hotspot de fácil acesso para os visitantes, que seja feito a coleta do nome, telefone e e-mail dos visitantes.

4.12. Será obrigação contratual a armazenagem, por todo o período de vigência, do registro de conexão, de medições básicas da rede e de todas as informações de cadastro de usuários, incluindo as informações de preenchimento voluntário.

4.13. Ao pressionar o botão destinado à conexão com a internet pela primeira vez, ele será transferido para a página de cadastro definido pela Contratante;

4.14. Que os usuários não tenham acesso a equipamentos de outros usuários conectados à rede WI-FI.

4.15. A contratada deverá fornecer sistema ou API de gerenciamento de funcionamento dos Wi-Fi das praças para auxiliar a fiscalização e acompanhamento do funcionamento das conexões, além de identificar cada Wi-Fi com o nome das respectivas Praças.

4.16. A Contratada deverá apresentar junto à emissão de Nota Fiscal, os respectivos relatórios de funcionamento, login acessos dos visitantes e consumo de banda por aparelho de rádio, identificando cada praça conforme mês referência da Nota Fiscal.

4.17. A contratada, se achar necessário, poderá fazer uma visita técnica aos pontos das possíveis praças que receberão a internet, para mensurar o custo de cada praça, para a montagem da proposta do preço médio total.

4.18. A contratada deverá fornecer os aparelhos que sejam capazes de abranger geograficamente toda a área da praça ofertada, podendo ser de 1(um) ou mais aparelhos para cada praça.

4.19. Deverão ser previstos todos os equipamentos ativos e passivos de rede, infraestrutura e insumos necessários ao bom funcionamento do sistema, tais como, mas não exclusivamente: postes, fios, cabos, conectores, amplificadores, racks, pontos de conexão (access points), no- breaks, wireless controllers, watch dogs, software e suprimentos complementares de energia elétrica, conforme o caso.

4.20. Cada aparelho de acesso das Praças deverá aceitar até 500 conexões simultâneas, dividindo assim a banda de internet 100mbs igualmente para os visitantes.

4.21. Internets Wi-Fi instaladas deverão ser capazes de garantir a qualidade e estabilidade do sinal aos usuários, evitando jitters e latências, sendo compatíveis com notebooks, celulares, smartphones, netbooks, tablets e outros dispositivos comumente utilizados para acesso à internet, dentro dos padrões mínimos: 802.11b, 802.11g, 802.11n e 802.11ac.

4.22. A contratada deverá garantir o nível de sinal de pelo menos -65 dBm na área de cobertura em todas as localidades e em ambas as faixas de frequência (2,4 GHz e 5 GHz).

4.23. CONTRATADA deverá dispor de ferramentas e recursos de monitoramento e controles de hardware e/ou software que possam ser operados por seus técnicos, e que possibilitem a imediata identificação de anormalidades na operação da infraestrutura de comunicação da rede Wi-Fi

4.24. A Contratada deverá fornecer uma banda de internet de 150 Mbs dedicada para cada ponto instalado.

4.25. O funcionamento de cada praça ofertada será por 24 (vinte e quatro) horas por dia, durante 7 (sete) dias da semana.

4.26. A combinação dessas tecnologias resulta em uma infraestrutura altamente disponível, segura e escalável, proporcionando continuidade operacional, proteção avançada contra ameaças cibernéticas e eficiência na comunicação entre as unidades municipais.

4.27. A solução foi desenhada para assegurar a proteção e a disponibilidade dos serviços municipais ao longo de todo o ciclo de vida do contrato, abrangendo desde a implantação inicial até a gestão contínua da infraestrutura de segurança e conectividade. A abordagem adotada permite que o município de Cáceres modernize sua infraestrutura

digital, proteja seus ativos de TI e garanta a prestação eficiente de serviços à população, sempre com segurança, confiabilidade e alta performance.

5. REQUISITOS DA CONTRATAÇÃO

5.1. Requisitos De Negócio

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

5.1.1.1. Implementação de tecnologia Next Generation Firewall (NGFW) para garantir proteção robusta contra ameaças cibernéticas e manutenção da integridade das operações de rede.

5.1.1.2. Implementação de sistema baseado em Inteligência Artificial Preditiva capaz de analisar padrões de comportamento na rede, identificar e neutralizar automaticamente ameaças sem necessidade de intervenção humana.

5.1.1.3. Disponibilização de equipamentos de hardware necessários à proteção da rede, sem a necessidade de aquisição direta, com manutenção e suporte garantidos pelo fornecedor, promovendo economicidade e flexibilidade.

5.1.1.4. Proteção eficaz contra ataques de “Zero Day”.

5.1.1.5. Atuação direta no tráfego de entrada da internet, identificando e neutralizando instantaneamente origens maliciosas.

5.1.1.6. Proteção abrangente para toda a infraestrutura, incluindo firewalls e roteadores.

5.1.1.7. Proteção abrangente para toda a infraestrutura, incluindo firewalls e roteadores.

5.1.1.8. Inclusão de software para configuração, monitoramento e gestão centralizada das políticas de segurança da rede de forma integrada e eficiente, permitindo maior controle e visibilidade.

5.1.1.9. Garantia de licenças válidas durante todo o período contratual, permitindo o pleno uso das funcionalidades da solução contratada.

5.1.1.10. Provisão de link dedicado de acesso à internet, bloco /29 e banda mínima de acesso garantida de 500Mbps para a solução NGFW SEDE (Dois Link de ASN e Rota Diferentes), essa configuração garante alta disponibilidade, resiliência a falhas e suporte eficiente às operações críticas.

5.1.1.11. Configuração e integração dos links diretamente com a solução NGFW, permitindo a gestão eficiente do tráfego e a aplicação das políticas de segurança.

5.1.1.12. Implementação de soluções SD-WAN integradas ao NGFW para conectar unidades externas vinculadas às secretarias municipais, promovendo segurança, desempenho e centralização na gestão de tráfego entre os locais.

5.1.1.13. Provisão de link primário de acesso à internet banda mínima de acesso garantida de 150Mbps Sites Remotos (Fibra Óptica), e link secundário de acesso à internet banda mínima de acesso garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G), link de ASN e rota diferentes, específicos para cada unidade externa e praças municipais, assegurando a continuidade das operações e a resiliência da rede em caso de falhas.

5.1.1.14. Realização de serviços especializados para instalação, configuração inicial e adequação às necessidades específicas do contratante e das unidades externas.

5.1.1.15. Implantação nas unidades externas de redes Wi-Fi seguras e segregadas para uso exclusivo dos servidores municipais, otimizando a conectividade e produtividade.

5.1.1.16. Garantia de autenticação por usuário e integração com políticas de segurança baseadas no NGFW.

5.1.1.17. Oferta de internet Wi-Fi gratuita nas unidades externas e nas praças municipais, com políticas de acesso baseadas no NGFW, assegurando privacidade e controle de navegação.

5.1.1.18. Implementação de mecanismos de limitação de banda e monitoramento para manter a qualidade do serviço e evitar o uso inadequado.

5.1.1.19. Atualizações regulares de firmware e assinaturas de segurança e patches, assegurando proteção contra ameaças emergentes e melhorias contínuas no desempenho da solução.

5.1.1.20. Capacitação especializada para a equipe do contratante, com emissão de certificação que ateste o domínio das funcionalidades e a capacidade de operação e manutenção da solução.

5.1.1.21. Oferta de suporte técnico com níveis de serviço bem definidos (SLA), cobrindo atendimento remoto e presencial, para resolução de incidentes e dúvidas operacionais.

5.1.1.22. Expansibilidade da solução para atender a demandas futuras de crescimento em tráfego, usuários e funcionalidades.

5.1.1.23. Ferramentas para supervisão em tempo real e geração de relatórios detalhados para análise de desempenho, auditorias e conformidade.

5.1.1.24. Garantia de aderência às regulamentações aplicáveis à proteção de dados e segurança da informação, incluindo requisitos legais e normativos vigentes.

5.1.1.25. Solução projetada para assegurar operação ininterrupta, com mecanismos de failover, redundância e backup que minimizem o impacto de falhas ou interrupções.

5.1.1.26. Redução da complexidade operacional, proporcionando maior eficiência no gerenciamento da segurança da rede e otimização de recursos técnicos e financeiros.

5.1.1.27. Configuração de políticas de tráfego e priorização de dados para garantir a performance ideal em aplicações críticas.

5.2. **Requisitos De Capacitação**

5.2.1. Deverá ser incluído na contratação capacitação técnica para a operação da solução, a serem conduzidos diretamente pelo fabricante ou por parceiro nacional devidamente capacitado, certificado e autorizado pelo fabricante para ministrar capacitações oficiais.

5.2.2. Deverá ser ministrado em Língua Portuguesa/Brasil.

5.2.3. Realização de capacitação básica com duração de 40 horas, abrangendo os conhecimentos essenciais para operar e gerenciar a solução implantada.

5.2.4. Deverá ser realizada uma reunião prévia entre o contratante e a empresa contratada para definição do calendário da capacitação básica que trata o item 5.2.3.

5.2.4.1. O cronograma deverá ser ajustado às necessidades da equipe da Coordenação de TI e compatível com a disponibilidade operacional, garantindo a participação integral dos envolvidos e a eficácia do processo de aprendizado.

5.2.5. Capacitação destinada a uma equipe de até 10 participantes da Coordenação de TI, garantindo maior interação com os instrutores e personalização do aprendizado.

5.2.6. Emissão de certificação oficial reconhecida pelo fabricante da solução ou por entidades de referência na área de segurança de rede, atestando a qualificação da equipe.

5.2.7. Capacitação presencial, realizado na sede da Prefeitura Municipal de Cáceres, para otimizar o tempo e garantir a participação efetiva da equipe.

5.2.8. Divisão do conteúdo em módulos, facilitando o aprendizado progressivo:

- Módulo 1: Introdução ao NGFW, IA Preditiva e princípios de segurança de rede.
- Módulo 2: Configuração inicial e operação básica dos equipamentos e software.
- Módulo 3: Gerenciamento de políticas de segurança e monitoramento da rede.
- Módulo 4: Configuração de links dedicados (redundância e backup).
- Módulo 5: Resolução de problemas e resposta a incidentes.

5.2.9. A divisão de conteúdo que trata o item 5.2.8 poderá ser alterado mediante reunião prévia entre o contratante e a empresa contratada.

5.2.10. Inclusão de laboratórios práticos para simulação de cenários reais, como aplicação de políticas de segurança, monitoramento de tráfego e configuração de redundância e backup.

5.2.11. Disponibilização de apostilas, guias de configuração, tutoriais e acesso a uma base de conhecimento técnico para consulta pós-capacitação.

5.2.12. Instruções específicas sobre a configuração, gerenciamento e monitoramento dos links de redundância e backup, incluindo a utilização de IPs fixos.

5.2.13. Aplicação de avaliação ao final da capacitação para validação do conhecimento adquirido.

seguido da entrega de certificados aos aprovados.

5.2.14. Abordagem de procedimentos para garantir a continuidade operacional da solução, como atualizações, backup de configurações e gerenciamento de logs.

5.2.15. Disponibilização de suporte técnico após a capacitação, para auxiliar na aplicação prática dos conhecimentos adquiridos.

5.2.16. Orientação sobre as melhores práticas para gestão segura da rede, incluindo conformidade com normas e regulamentações aplicáveis, como a LGPD.

5.2.17. Previsão de um workshop complementar, podendo este ser por vídeo conferencia, a ser realizado após a conclusão da capacitação, para reforçar conteúdos e sanar dúvidas remanescentes.

5.2.18. Elaboração de relatórios detalhados com informações sobre a participação, desempenho e certificação da equipe, para acompanhamento da gestão de competências.

5.3. **Requisitos Legais**

5.3.1. **Conformidade Legal e Normativa:**

5.3.1.1. A contratação deve obedecer à Constituição Federal, garantindo os princípios da legalidade, moralidade, publicidade, eficiência e economicidade.

5.3.1.2. Estar em conformidade com a Lei nº 14.133/2021, que regula as normas gerais de licitação e contratação pública.

5.3.1.3. Atender à Instrução Normativa SGD/ME nº 94, de 2022, que disciplina contratações de TIC no setor público.

5.3.1.4. Respeitar a Instrução Normativa SEGES/ME nº 65, de 2021, que trata da governança em aquisições de TIC.

5.3.1.5. Observar a Lei nº 13.709, de 2018 (LGPD), garantindo a proteção de dados pessoais.

5.3.1.6. Aplicar as disposições da Lei nº 10.520, de 2001, e do Decreto nº 10.024, de 2019, referentes ao pregão eletrônico.

5.3.1.7. Cumprir o Decreto Municipal nº 665, de 09 de outubro de 2024, que regulamenta contratações de TIC no âmbito municipal.

5.3.2. **Proteção de Dados e Privacidade:**

5.3.2.1. Garantir conformidade integral com a LGPD, implementando medidas para prevenir acessos não autorizados e vazamentos de dados pessoais.

5.3.2.2. O contratado deve demonstrar, quando solicitado, os mecanismos e políticas utilizados para assegurar a proteção de dados, sujeitos à auditoria da contratante.

5.3.3. **Transparência e Publicidade:**

5.3.3.1. Todos os atos do processo licitatório e de execução contratual deverão ser registrados e divulgados nos meios oficiais, conforme exigido por lei.

5.3.3.2. Relatórios e informações sobre a execução do contrato deverão ser disponibilizados periodicamente para consulta pública, garantindo transparência no uso dos recursos.

5.3.4. **Responsabilidade do Contratado:**

5.3.4.1. O contratado é responsável por cumprir integralmente as obrigações legais aplicáveis, incluindo as previstas na Lei nº 14.133/2021 e no Decreto Municipal nº 665/2024.

respondendo por eventuais descumprimentos com as penalidades previstas em contrato e em lei.

5.4. Requisitos De Manutenção

5.4.1. Manutenção Preventiva (Não Emergencial):

5.4.1.1. Realização de manutenções programadas para garantir o funcionamento ideal da solução NGFW, incluindo inspeções, limpeza, análise de logs, e aplicação de atualizações de firmware.

5.4.1.2. Frequência mínima semestral ou conforme cronograma estabelecido entre as partes.

5.4.2. Manutenção Corretiva (Emergencial):

5.4.2.1. Atendimento imediato para corrigir falhas ou defeitos nos equipamentos ou no software, visando a restauração do funcionamento normal da solução NGFW.

5.4.2.2. Inclui diagnóstico remoto e, quando necessário, deslocamento técnico para reparos ou substituição de componentes.

5.4.3. Manutenção Adaptativa (Não Emergencial):

5.4.3.1. Adequação da solução NGFW às mudanças no ambiente operacional ou aos requisitos específicos do contratante, como ajustes de configuração ou implementação de novas políticas de segurança.

5.4.4. Manutenção Evolutiva (Não Emergencial):

5.4.4.1. Implementação de melhorias na solução, incluindo a integração de novas funcionalidades, suporte a tecnologias emergentes e expansão da capacidade para atender a demandas crescentes.

5.4.5. Monitoramento Proativo (Não Emergencial):

5.4.5.1. Serviço contínuo de monitoramento da solução, com análise de logs e detecção antecipada de falhas ou ameaças que exijam intervenção.

5.4.6. Substituição de Equipamentos (Emergencial):

5.4.6.1. Garantia de substituição rápida e sem custos adicionais de equipamentos defeituosos durante a vigência contratual, minimizando interrupções.

5.4.7. Relatórios Periódicos (Não Emergencial):

5.4.7.1. Emissão de relatórios detalhados sobre intervenções realizadas, estado dos equipamentos, atualizações aplicadas e resultados das manutenções.

5.4.8. Classificação de Ocorrências:

5.4.8.1. Critérios claros para categorizar os atendimentos em emergenciais e não emergenciais, com tratamento prioritário para problemas críticos.

5.4.9. Tabela de atendimento:

TIPO DE ATENDIMENTO	**DESCRIÇÃO**	**EMERGENCIAL/NÃO EMERGENCIAL**	**TEMPO DE RESPOSTA**	**TEMPO DE SOLUÇÃO**	**MEIO DE ATENDIMENTO**
Emergencial	Ocorrências críticas que impactem diretamente a operação da rede, como falhas graves nos equipamentos NGFW, links de redundância ou brechas de segurança.	Emergencial	Até 1 hora	Até 4 horas	Suporte remoto e, se necessário, presencial.
Corretiva	Problemas pontuais ou defeitos que não sejam de natureza crítica, mas que exijam reparo técnico para evitar impactos futuros.	Emergencial	Até 4 horas	Até 8 horas	Suporte remoto ou presencial agendado.
Preventiva	Ações periódicas de inspeção e manutenção para prevenir falhas e garantir o desempenho ideal da solução.	Não Emergencial	Agendamento prévio	Conforme cronograma	Suporte presencial planejado.
Adaptativa	Ajustes para adequação da solução a novas necessidades operacionais ou mudanças no ambiente do contratante.	Não Emergencial	Até 2 dias úteis	Até 7 dias úteis	Suporte remoto ou presencial agendado.

Evolutiva	Melhorias e implementações que ampliem as funcionalidades ou capacidades da solução NGFW.	Não Emergencial	Até 5 dias úteis	Conforme projeto	Suporte remoto ou presencial planejado.
Substituição de Equipamentos	Substituição de equipamentos defeituosos ou que apresentem falhas que afetem a continuidade do serviço.	Emergencial	Até 1 hora	Até 4 horas	Suporte remoto e, se necessário, presencial.
Monitoramento Proativo	Monitoramento contínuo da solução para antecipar problemas, com o detecção de falhas ou anomalias.	Não Emergencial	Até 4 horas	Contínuo	Suporte remoto.
Relatórios Periódicos	Emissão de relatórios detalhados sobre o status da solução NGFW, ações realizadas e estado dos equipamentos.	Não Emergencial	Até 24 horas	Conforme cronograma	Suporte remoto ou presencial agendado.

5.5. **Requisitos Temporais**

5.5.1. **Prazos de Entrega dos Equipamentos e Solução:**

5.5.1.1. O fornecimento dos equipamentos necessários para a implementação da solução, incluindo hardware, licenças e software de gerenciamento, deverá ser realizado no prazo máximo de 30 dias corridos a partir da assinatura do contrato.

5.5.1.2. A instalação, configuração e ativação completa da solução, incluindo os links de internet e redundância, deverá ser concluída no prazo máximo de 45 dias corridos após a entrega dos equipamentos.

5.5.1.3. O treinamento básico com carga horária de 40 horas para a equipe técnica da Prefeitura Municipal de Cáceres deverá ser realizada uma reunião prévia entre o contratante e a empresa contratada para definição do calendário da capacitação básica.

5.5.2. **Prazos de Atendimento para Suporte Técnico:**

5.5.2.1. **Atendimento Emergencial:**

5.5.2.1.1. Chamados emergenciais, que incluem falhas críticas que afetam diretamente a operação da rede ou a disponibilidade de serviços essenciais, deverão ser atendidos no prazo máximo de 4 horas após a abertura do chamado.

5.5.2.1.2. A solução completa para o problema deverá ser implementada no prazo máximo de 8 horas, salvo situações excepcionais que exijam medidas corretivas complexas.

5.5.2.2. **Atendimento Não Emergencial:**

5.5.2.2.1. Chamados de manutenção corretiva, preventiva, adaptativa ou evolutiva que não impactem diretamente a operação da rede deverão ser atendidos no prazo máximo de 24 horas úteis após a abertura do chamado.

5.5.2.2.2. A resolução deverá ocorrer no prazo de até 5 dias úteis, salvo a necessidade de ajustes ou implementações que exijam maior prazo, o qual será acordado previamente.

5.5.3. **Forma de Atendimento do Suporte Técnico:**

5.5.3.1. **Atendimento Remoto:**

5.5.3.1.1. O suporte técnico deverá ser disponibilizado remotamente como primeira opção para resolução de problemas, utilizando ferramentas seguras para acesso remoto e diagnóstico.

5.5.3.1.2. O suporte remoto deverá estar disponível 24x7 (24 horas por dia, 7 dias por semana) para incidentes emergenciais.

5.5.3.2. **Atendimento Presencial:**

5.5.3.2.1. Quando a resolução do problema não for possível de forma remota, será realizado atendimento presencial por técnicos especializados.

5.5.3.2.2. O prazo para deslocamento e início do atendimento no local para casos emergenciais será de até 4 horas úteis a partir da solicitação.

5.5.3.2.3. Para casos não emergenciais, o atendimento presencial será agendado com a equipe de TI da Prefeitura, respeitando o prazo máximo de 2 dias úteis.

5.5.4. **Monitoramento e Relatórios de SLA:**

5.5.4.1. A empresa contratada deverá monitorar e registrar os tempos de atendimento e resolução de chamados, emitindo relatórios mensais que comprovem o cumprimento dos SLAs estabelecidos.

5.5.4.2. O descumprimento dos prazos estabelecidos implicará penalidades contratuais conforme especificado nos termos do contrato.

5.5.5. **Atendimento de Manutenção Preventiva e Evolutiva:**

5.5.5.1. Manutenções preventivas deverão ser realizadas trimestralmente, com agendamento prévio com a equipe de TI da Prefeitura Municipal de Cáceres.

5.5.5.2. Manutenções evolutivas, que envolvam atualizações ou melhorias significativas na solução, deverão ser realizadas mediante planejamento e acordo prévio, com prazo máximo de implementação em 30 dias úteis após a aprovação.

5.6. Requisitos de Segurança e Privacidade

5.6.1. Políticas de Segurança Baseadas no NGFW

5.6.1.1. Permitir a configuração de políticas robustas de segurança para controle e monitoramento do tráfego de rede, assegurando proteção contra ataques cibernéticos, intrusões, malwares e acessos não autorizados.

5.6.1.2. Definir regras personalizadas para bloquear tráfego malicioso e permitir apenas conexões seguras e autorizadas.

5.6.1.3. Configuração de proteção contra ataques de negação de serviço (DoS), com a opção de habilitação global ou por política específica.

5.6.1.4. Disponibilizar uma interface única para configuração de políticas, integrando perfis de segurança como Proxy Web, IPS, Controle de Aplicações, SD-WAN e Proteção contra Ameaças Avançadas (ATP).

5.6.1.5. Implementar validação automatizada das políticas de segurança para identificar e resolver regras duplicadas ou conflitantes.

5.6.2. Segmentação e Isolamento de Redes

5.6.2.1. Segmentação lógica da rede principal e das redes das unidades externas, garantindo o isolamento entre setores e usuários, reduzindo os riscos de propagação de ataques.

5.6.2.2. Configuração de SD-WAN para roteamento dinâmico de tráfego entre diferentes unidades e praças municipais, assegurando desempenho e segurança.

5.6.3. Proteção Avançada Contra Ameaças

5.6.3.1. Ativação de funcionalidades como inspeção profunda de pacotes (DPI), prevenção contra intrusões (IPS) e detecção de anomalias baseadas em inteligência artificial.

5.6.3.2. Integração com serviços de inteligência de ameaças para identificação e mitigação de ataques emergentes.

5.6.4. Criptografia de Dados e Segurança em Trânsito

5.6.4.1. Garantir que todas as comunicações de dados entre firewall principal, unidades externas e dispositivos sejam protegidas por protocolos de criptografia avançados, como TLS/SSL.

5.6.4.2. Implementação de inspeção de tráfego criptografado (SSL Inspection) para detecção de ameaças em comunicações seguras.

5.6.5. Controle de Acessos e Gerenciamento Centralizado

5.6.5.1. Adotar autenticação multifator (MFA) para acesso ao sistema de gerenciamento do NGFW e a serviços críticos.

5.6.5.2. Realizar o gerenciamento centralizado de permissões, com auditoria detalhada de acessos e atividades realizadas na rede.

5.6.6. Monitoramento, Logs e Alertas de Segurança

5.6.6.1. Configuração de logs detalhados de eventos e atividades, com centralização das informações em uma solução de SIEM (Gestão de Informações e Eventos de Segurança).

5.6.6.2. Geração de alertas em tempo real para eventos críticos, como tentativas de intrusão ou anomalias de tráfego.

5.6.6.3. Emissão de relatórios periódicos sobre segurança da rede, destacando vulnerabilidades detectadas e ações tomadas.

5.6.7. **Conformidade com Normas de Segurança e Privacidade**

5.6.7.1. Garantir que a solução NGFW esteja em conformidade com a LGPD e outras legislações aplicáveis, assegurando a proteção e privacidade dos dados pessoais.

5.6.7.2. Disponibilizar recursos para anonimização ou pseudonimização de dados, conforme exigido pelas normas.

5.6.8. **Testes e Avaliações Periódicas de Segurança**

5.6.8.1. Realização de testes de penetração (pentests) regulares para avaliar a eficácia das medidas de segurança.

5.6.8.2. Simulações de incidentes de segurança para treinar equipes e validar os planos de resposta a incidentes.

5.6.9. **Backup e Recuperação Segura**

5.6.9.1. Implementar backups automáticos e criptografados das configurações do NGFW e de dados críticos, com armazenamento em locais seguros.

5.6.9.2. Garantir processos rápidos de recuperação em caso de falha ou desastre, assegurando a continuidade operacional.

5.6.10. **Conscientização e Educação de Usuários**

5.6.10.1. Desenvolver programas regulares de conscientização sobre segurança da informação para servidores municipais, abordando práticas seguras de uso da internet.

5.6.10.2. Orientar os cidadãos sobre o uso responsável das redes Wi-Fi públicas disponibilizadas nas praças e unidades municipais.

5.7. **Requisitos de Metodologia de Trabalho**

5.7.1. Emissão de Ordem de Serviço (OS):

5.7.1.1. A execução de qualquer serviço contratado está condicionada ao recebimento pelo contratado de uma Ordem de Serviço (OS) emitida pela contratante.

5.7.1.2. A Ordem de Serviço deverá especificar, de forma clara:

- O serviço a ser executado.
- A quantidade de serviços.
- A localidade onde o serviço deverá ser prestado.

5.7.2. **Meios de Contato e Registro de Ocorrências:**

5.7.2.1. O contratado deve fornecer canais de comunicação para contato e registro de ocorrências, conforme as seguintes especificações:

- Atendimento eletrônico (e-mail, sistema de chamados ou aplicativo): 24 horas por dia, 7 dias por semana.
- Atendimento telefônico: 12 horas por dia, 5 dias por semana, garantindo resposta ágil a chamados emergenciais.

5.7.3. **Acompanhamento e Comunicação Durante a Execução:**

5.7.3.1. A execução de todos os serviços deverá ser acompanhada diretamente pelo contratado, assegurando o cumprimento das especificações definidas na Ordem de Serviço.

5.7.3.2. Eventuais ocorrências ou desvios identificados durante a execução deverão ser imediatamente comunicados à contratante, com descrição detalhada da situação e das medidas corretivas adotadas.

5.7.4. **Prazos de Atendimento e Execução:**

5.7.4.1. O prazo para início da execução dos serviços será contado a partir do recebimento da Ordem de Serviço, respeitando os prazos definidos nos Requisitos Temporais.

5.7.4.2. Os serviços deverão ser finalizados dentro dos prazos estabelecidos, salvo justificativas formalmente apresentadas e aceitas pela contratante.

5.7.5. **Registro e Relatório de Serviços Executados:**

5.7.5.1. Ao término de cada serviço, o contratado deverá entregar à contratante um relatório detalhado contendo:

- Descrição do serviço realizado.
- Data e horário de início e conclusão do serviço.
- Identificação dos profissionais envolvidos.
- Observações sobre eventuais dificuldades ou necessidades futuras.

5.7.5.2. O relatório deverá ser aprovado pela contratante para formalizar a conclusão do serviço.

5.7.6. **Garantia de Qualidade e Conformidade:**

5.7.6.1. O contratado deverá assegurar que todos os serviços sejam executados em conformidade com as especificações técnicas, normativas e de segurança previamente acordadas.

5.7.6.2. Qualquer serviço executado em desacordo com o estabelecido será considerado não conforme, cabendo ao contratado refazê-lo sem custos adicionais para a contratante.

5.7.7. **Reuniões de Alinhamento e Planejamento:**

5.7.7.1. O contratado deverá participar de reuniões periódicas com a contratante para alinhar prioridades, revisar o cronograma e discutir ajustes necessários nos serviços prestados.

5.7.7.2. Essas reuniões ocorrerão em frequência mínima trimestral ou conforme solicitado pela contratante.

5.7.8. **Garantia de Resposta a Ocorrências:**

5.7.8.1. O contratado deverá manter equipe disponível para atender a chamados dentro dos prazos especificados nos Requisitos de Manutenção, priorizando serviços emergenciais.

5.7.8.2. As ocorrências serão classificadas conforme sua criticidade, e o atendimento será realizado de acordo com a priorização estabelecida na Ordem de Serviço.

5.8. Requisitos de Experiência Profissional

5.8.1. Experiência Comprovada no Fornecimento de Soluções NGFW:

5.8.1.1. O contratado deverá comprovar experiência na implementação e gerenciamento de soluções de Next Generation Firewall (NGFW) em instituições públicas ou privadas de grande porte, preferencialmente na administração municipal.

5.8.1.2. Será exigida a apresentação de no mínimo 3 (três) atestados de capacidade técnica, emitidos por clientes anteriores, que confirmem a execução de serviços similares ao escopo deste contrato, incluindo fornecimento de hardware, software, implantação, configuração e suporte técnico.

5.8.2. **Qualificação da Equipe Técnica:**

5.8.2.1. A equipe técnica alocada deve possuir profissionais certificados pelo fabricante da solução NGFW a ser implementada, garantindo competência técnica para execução dos serviços contratados.

5.8.2.2. Os profissionais responsáveis pela execução dos serviços devem ter experiência mínima de 2 (dois) anos em funções relacionadas à implantação, manutenção e suporte de soluções de segurança da informação.

5.8.3. **Experiência em Projetos de TIC para o Setor Público:**

5.8.3.1. O contratado deverá demonstrar experiência específica em projetos de Tecnologia da Informação e Comunicação (TIC) realizados para órgãos da administração pública, especialmente em contextos municipais.

5.8.3.2. A comprovação poderá incluir contratos anteriores, declarações ou relatórios técnicos que atestem a capacidade do contratado em atender às exigências específicas de órgãos públicos.

5.8.4. **Atendimento a Requisitos de Escalabilidade e Complexidade:**

5.8.4.1. A empresa deverá comprovar ter executado projetos que envolvam ambientes complexos, com integração de múltiplas unidades ou localidades, utilizando tecnologias como SD-WAN e links redundantes.

5.8.4.2. Será considerado diferencial a experiência em projetos que incluíram a disponibilização de internet Wi-Fi para servidores e cidadãos.

5.8.5. **Experiência em Treinamento e Capacitação:**

5.8.5.1. A empresa deve demonstrar ter conduzido treinamentos técnicos relacionados à operação de soluções NGFW, com fornecimento de certificações reconhecidas.

5.8.5.2. O contratado deverá apresentar registro de treinamentos realizados, com informações sobre a carga horária, conteúdo programático e feedback dos participantes.

5.8.6. **Critérios de Avaliação da Experiência:**

5.8.6.1. A experiência profissional será avaliada com base nos documentos apresentados, como contratos, atestados, certificados de conclusão de projetos e outros registros comprobatórios.

5.8.6.2. A ausência de comprovação adequada poderá resultar na desclassificação da proposta, conforme previsto na legislação vigente.

5.9. **Requisitos de Segurança da Informação e Privacidade**

5.9.1. **Conformidade com Normas e Padrões de Segurança:**

5.9.1.1. O contratado deve aderir às diretrizes da ISO/IEC 27001, garantindo a gestão eficiente da segurança da informação durante toda a execução do contrato.

5.9.1.2. Implementar controles técnicos e organizacionais para mitigar riscos de acessos não autorizados, vazamentos de dados e interrupções nos serviços.

5.9.2. **Proteção de Dados Sensíveis:**

5.9.2.1. A CONTRATADA deverá assegurar a proteção de todos os dados sensíveis e confidenciais trafegados, processados ou armazenados nos equipamentos fornecidos, utilizando criptografia adequada e outros mecanismos de segurança, em estrita conformidade com a Lei Geral de Proteção de Dados (LGPD).

5.9.2.2. É vedado à CONTRATADA compartilhar, divulgar ou permitir o acesso de terceiros a quaisquer dados sensíveis ou confidenciais, salvo mediante autorização expressa e formal da CONTRATANTE, observadas as disposições legais aplicáveis.

5.9.3. **Gestão de Políticas de Segurança:**

5.9.3.1. A solução fornecida deverá possibilitar a criação, gerenciamento e auditoria de políticas de segurança de forma centralizada, assegurando a rastreabilidade de todas as alterações e acessos.

5.9.3.2. As políticas deverão integrar funcionalidades de IPS (Prevenção contra Intrusões), SD-WAN, controle de aplicações, filtros de conteúdo web e inspeção de tráfego criptografado (SSL/TLS).

5.9.4. **Monitoramento e Resposta a Incidentes:**

5.9.4.1. O sistema deve realizar monitoramento contínuo para identificar e mitigar incidentes de segurança em tempo real.

5.9.4.2. Eventos críticos deverão gerar alertas automáticos e relatórios detalhados, a serem compartilhados com a CONTRATANTE conforme prazos previamente estabelecidos.

5.9.5. **Controle de Acesso:**

5.9.5.1. O acesso ao sistema de gerenciamento do NGFW e demais serviços críticos deverá ser protegido por mecanismos robustos de autenticação, incluindo autenticação multifator (MFA).

5.9.5.2. Os acessos deverão ser controlados por perfis de usuário, com registros completos (logs) de todas as atividades realizadas.

5.9.6. **Tratamento de Dados de Redes Wi-Fi:**

5.9.6.1. A solução deverá garantir a segregação lógica entre os dados trafegados por servidores municipais e cidadãos nas redes Wi-Fi disponibilizadas.

5.9.6.2. É vedada a utilização dos dados coletados ou trafegados na rede Wi-Fi para qualquer finalidade sem autorização formal da CONTRATANTE e em conformidade com a LGPD.

5.9.7. **Backup e Recuperação de Dados:**

5.9.7.1. O sistema deverá realizar backups automáticos e criptografados de todas as configurações, incluindo logs de segurança e políticas implementadas.

5.9.7.2. Deve-se garantir a recuperação rápida e segura dos dados em caso de falhas ou incidentes.

5.9.8. **Educação e Conscientização de Segurança:**

5.9.8.1. A CONTRATADA deverá fornecer materiais educativos ou treinamentos para conscientização dos servidores municipais sobre práticas seguras de navegação, uso de redes Wi-Fi e proteção contra ameaças cibernéticas.

5.9.9. **Auditorias e Testes de Segurança:**

5.9.9.1. Realizar auditorias periódicas no ambiente de segurança implementado, identificando vulnerabilidades e propondo medidas corretivas.

5.9.9.2. Realizar testes de vulnerabilidade e simulações de incidentes para avaliar a eficácia das medidas de proteção e identificar oportunidades de aprimoramento.

5.10. **Requisitos de Sustentabilidade**

5.10.1. **Uso Eficiente de Recursos Energéticos:**

5.10.1.1. Os equipamentos fornecidos, incluindo os dispositivos NGFW, deverão possuir características de eficiência energética, certificadas por padrões internacionais reconhecidos, como Energy Star ou equivalentes.

5.10.1.2. A empresa contratada deverá garantir que os equipamentos operem com consumo energético reduzido, promovendo a sustentabilidade ambiental e diminuindo os custos operacionais.

5.10.2. **Descarte Adequado de Equipamentos Obsoletos:**

5.10.2.1. Todos os equipamentos substituídos durante a vigência do contrato deverão ser descartados de forma responsável e conforme as normas ambientais vigentes, incluindo a Política Nacional de Resíduos Sólidos (PNRS).

5.10.2.2. A contratada deverá apresentar comprovantes de descarte adequado ou reciclagem dos componentes eletrônicos substituídos.

5.10.3. **Redução de Impacto Ambiental no Transporte:**

5.10.3.1. Sempre que possível, as atividades de instalação, manutenção e suporte deverão ser realizadas de forma remota, minimizando deslocamentos físicos e reduzindo a emissão de gases de efeito estufa.

5.10.3.2. Quando o atendimento presencial for indispensável, a empresa contratada deverá priorizar o uso de veículos elétricos ou de baixo consumo energético.

5.10.4. **Promoção de Práticas Digitais Sustentáveis:**

5.10.4.1. O contratado deverá implementar soluções digitais que reduzam o uso de papel, como relatórios, registros de manutenção e documentação de configuração disponibilizados exclusivamente em formato eletrônico.

5.10.4.2. Os sistemas e ferramentas utilizados deverão ser otimizados para minimizar o consumo de banda de rede, evitando desperdícios e sobrecargas desnecessárias.

5.10.5. **Gestão Responsável dos Links de Internet:**

5.10.5.1. A configuração dos links de internet deverá priorizar o uso eficiente dos recursos disponíveis, evitando sobrecargas e consumo desnecessário.

5.10.5.2. O contratado deverá implementar práticas de monitoramento contínuo para garantir que os links estejam sendo utilizados de forma sustentável e equilibrada.

5.10.6. **Capacitação com Enfoque Sustentável:**

5.10.6.1. Os treinamentos oferecidos para a equipe da Prefeitura deverão incluir orientações sobre práticas sustentáveis no uso e gerenciamento dos sistemas e dispositivos de rede.

5.10.6.2. A capacitação deverá enfatizar a importância da economia de recursos, como energia e banda, no contexto de TI sustentável.

5.10.7. **Relatórios de Sustentabilidade:**

5.10.7.1. A contratada deverá apresentar relatórios periódicos sobre ações e práticas sustentáveis implementadas, incluindo:

- Consumo energético dos equipamentos fornecidos.
- Impacto ambiental reduzido pelas operações remotas.
- Quantidade de materiais reciclados ou descartados adequadamente.

5.10.7.2. Esses relatórios deverão ser analisados em conjunto com a contratante para identificar oportunidades adicionais de sustentabilidade.

5.11. **Da Exigência de Carta de Solidariedade**

5.11.1. Será exigida a apresentação de Carta de Solidariedade, emitida pelo fabricante, como garantia da execução contratual.

5.11.2. A referida carta deverá ser apresentada juntamente com a qualificação técnica da licitante e abranger os seguintes itens da solução ofertada:

- Item 1
- Item 2
- Item 3
- Item 4

5.11.3. A exigência visa assegurar que as licitantes contratadas possuam plenas condições de fornecimento e manutenção dos equipamentos mencionados, garantindo seu pleno funcionamento durante a vigência do contrato.

5.11.4. A exigência busca resguardar a Administração contra eventuais prejuízos decorrentes da indisponibilidade de peças de reposição ou da ausência de suporte técnico necessário para ajustes e aprimoramentos dos equipamentos fornecidos.

5.12. **Subcontratação**

5.12.1. **Critérios para Subcontratação:**

5.12.1.1. A subcontratação de serviços pela empresa contratada será permitida apenas mediante autorização prévia e formal da Prefeitura Municipal de Cáceres.

5.12.1.2. A empresa contratada deverá garantir que a subcontratada possua capacidade técnica comprovada, com experiência e certificações relevantes ao escopo dos serviços a serem executados.

5.12.2. **Responsabilidades da Contratada em Caso de Subcontratação:**

5.12.2.1. A empresa contratada será responsável integralmente pelos serviços executados pela subcontratada, respondendo pelos mesmos padrões de qualidade, prazos e resultados exigidos no contrato.

5.12.2.2. A contratada deverá assegurar que os serviços realizados pela subcontratada estejam em conformidade com todos os requisitos técnicos, normativos e de segurança estabelecidos no contrato.

5.12.2.3. Qualquer prejuízo ou falha decorrente de serviços executados pela subcontratada será de total responsabilidade da empresa contratada, que deverá arcar com os custos e medidas corretivas necessárias.

5.12.3. **Obrigações Adicionais da Subcontratada:**

5.12.3.1. A subcontratada deverá seguir rigorosamente as normas de segurança e privacidade, especialmente aquelas relacionadas à Lei Geral de Proteção de Dados (LGPD).

5.12.3.2. A subcontratada deverá assinar um Termo de Confidencialidade, comprometendo-se a proteger todas as informações relacionadas ao projeto e à infraestrutura da Prefeitura Municipal de Cáceres.

5.12.4. **Limitações e Proibições:**

5.12.4.1. Não será permitido subcontratar o fornecimento de equipamentos essenciais, como os dispositivos NGFW, IA preditiva e softwares de gerenciamento, que deverão ser fornecidos diretamente pela contratada ou pelo fabricante autorizado.

5.12.4.2. Não será permitido subcontratar serviços que envolvam suporte emergencial ou atividades críticas que demandem resposta imediata.

5.12.4.3. A subcontratação de serviços especializados (ex.: treinamento oficial, suporte técnico avançado) somente será permitida se o subcontratado for certificado pelo fabricante da solução NGFW, IA preditiva e softwares de gerenciamento.

5.12.5. **Comunicação e Relatórios:**

5.12.5.1. A empresa contratada deverá notificar previamente a Prefeitura Municipal de Cáceres sobre qualquer intenção de subcontratar serviços, fornecendo informações detalhadas sobre a empresa subcontratada e os serviços a serem realizados.

5.12.5.2. Relatórios detalhados sobre a execução de serviços pela subcontratada deverão ser incluídos nos relatórios periódicos enviados pela empresa contratada.

5.12.6. **Penalidades em Caso de Irregularidades na Subcontratação:**

5.12.6.1. O não cumprimento das condições estabelecidas para subcontratação poderá implicar penalidades contratuais, incluindo advertências, multas ou até rescisão contratual.

5.12.6.2. A Prefeitura Municipal de Cáceres poderá solicitar a substituição imediata da subcontratada caso se identifiquem falhas graves ou descumprimento dos requisitos contratuais.

5.13. **Garantia Da Contratação**

5.13.1. Não se aplica ao objeto deste Termo de Referência.

5.14. Da Alteração Subjetiva

5.14.1. Não se aplica no presente processo licitatório.

6. PAPÉIS E RESPONSABILIDADES

6.1. Durante o período de vigência do contrato sem prejuízo para as obrigações mencionadas em outros dispositivos deste instrumento ou de qualquer outra obrigação imposta por lei, **serão obrigações da CONTRATANTE**:

6.1.1. Proporcionar à CONTRATADA todas as condições necessárias para a execução dos serviços e entrega dos produtos, incluindo infraestrutura, suporte técnico e informações adicionais de responsabilidade da CONTRATANTE.

6.1.2. Prestar à CONTRATADA todas as informações, esclarecimentos, elementos e dados técnicos necessários ao cumprimento do contrato.

6.1.3. Encaminhar à CONTRATADA todas as solicitações relativas à execução dos serviços e ao fornecimento de produtos, detalhando requisitos, prazos e especificações.

6.1.4. Permitir o acesso de empregados, prepostos ou representantes da CONTRATADA às dependências da Prefeitura Municipal de Cáceres, desde que previamente autorizado e em conformidade com as normas de segurança do local.

6.1.5. Acompanhar e fiscalizar a execução do contrato, designando servidor ou comissão responsável para monitoramento das atividades da CONTRATADA, conforme previsto na Lei nº 14.133/2021.

6.1.6. Garantir que os fiscais designados documentem ocorrências, elaborem relatórios e comuniquem irregularidades à CONTRATADA de forma tempestiva.

6.1.7. Verificar, no prazo fixado, a conformidade dos serviços prestados e produtos entregues, garantindo sua adequação às especificações contratuais.

6.1.8. Rejeitar, total ou parcialmente, serviços ou produtos que não atendam aos requisitos contratuais, comunicando a necessidade de correção ou substituição.

6.1.9. Aplicar as penalidades cabíveis, garantindo a prévia e ampla defesa da CONTRATADA.

6.1.10. Informar imediatamente à CONTRATADA qualquer problema ou irregularidade detectada nos serviços ou produtos fornecidos.

6.1.11. Solicitar, por escrito, a substituição dos serviços que apresentarem desconformidade com o contrato.

6.1.12. Emitir o Termo de Aceite Definitivo após a devida implantação dos serviços contratados.

6.1.13. Atestar as faturas de serviço apresentadas mensalmente pela CONTRATADA.

6.1.14. Manifestar-se, no prazo de 3 dias úteis, sobre as informações contidas na planilha de memória de cálculo fornecida pela CONTRATADA.

6.1.15. Efetuar o pagamento à CONTRATADA no prazo estipulado, desde que todas as obrigações contratuais tenham sido devidamente cumpridas e homologadas.

6.1.16. Promover reuniões periódicas com a CONTRATADA para avaliação do andamento dos serviços, apresentação de relatórios técnicos e resolução de eventuais problemas.

6.1.17. Registrar todas as interações e ocorrências relacionadas ao contrato, garantindo rastreabilidade e acompanhamento das obrigações de ambas as partes.

6.2. Durante o período de vigência do contrato, sem prejuízo para as obrigações mencionadas em outros dispositivos deste instrumento ou de qualquer outra obrigação imposta por lei, **serão obrigações da CONTRATADA**:

6.2.1. Cumprir todas as obrigações previstas no Edital, seus anexos e na proposta apresentada, assumindo integralmente os riscos e as despesas decorrentes da execução do contrato.

6.2.2. Executar o objeto do contrato em sua totalidade, em conformidade com as especificações estabelecidas no Termo de Referência e no contrato firmado.

6.2.3. Efetuar a entrega dos serviços e produtos dentro dos prazos estabelecidos, garantindo que estejam em perfeitas condições e em conformidade com as especificações contratuais.

6.2.4. Acompanhar a entrega dos produtos com a devida nota fiscal, contendo marca, fabricante, modelo, procedência, prazo de garantia ou validade e demais informações exigidas.

6.2.5. Garantir que os serviços e produtos fornecidos sejam de boa qualidade, atendendo integralmente às condições, quantidades e padrões estipulados no contrato.

6.2.6. Resolver prontamente quaisquer falhas ou não conformidades apontadas pela CONTRATANTE, incluindo a substituição ou correção dos serviços e produtos rejeitados.

6.2.7. Manter, durante toda a execução do contrato, as condições de habilitação exigidas, incluindo requisitos técnicos, fiscais, trabalhistas e sociais.

6.2.8. Assumir integralmente as despesas relacionadas à execução do contrato, incluindo tributos, encargos trabalhistas e previdenciários de seus empregados.

6.2.9. Disponibilizar equipe técnica qualificada e apta a atender às demandas durante toda a vigência do contrato.

6.2.10. Implementar práticas de sustentabilidade ambiental, social e econômica na execução dos serviços, conforme princípios legais e normativos aplicáveis.

6.2.11. Permitir à CONTRATANTE a fiscalização da execução dos serviços e fornecimento dos produtos, prestando todos os esclarecimentos solicitados.

6.2.12. Registrar todas as interações e ocorrências relacionadas ao contrato, garantindo rastreabilidade e acompanhamento das obrigações contratuais.

6.2.13. Fornecer canais de atendimento eficientes para comunicação com a CONTRATANTE, garantindo solução ágil para eventuais problemas.

6.2.14. Tomar todas as providências necessárias para implantar e manter os serviços contratados em níveis satisfatórios, de acordo com o IMR e demais disposições contratuais.

6.2.15. Fornecer, sem custo adicional, todos os equipamentos e acessórios necessários à prestação dos serviços nas condições estabelecidas no contrato.

6.2.16. Diagnosticar falhas nos serviços relatadas pela CONTRATANTE e eliminar defeitos nos componentes sob sua responsabilidade.

6.2.17. Sanar quaisquer falhas, degradações ou indisponibilidades do serviço, independentemente de notificação da CONTRATANTE ou detecção via monitoramento proativo.

6.2.18. Executar serviços que acarretem riscos aos sistemas em produção ou requeiram parada de servidores, equipamentos ou rede elétrica somente fora do expediente, incluindo finais de semana e feriados, mediante prévia autorização do Setor de Tecnologia da Informação e Comunicação.

6.2.19. Comunicar à CONTRATANTE, via e-mail e com antecedência mínima de três horas, a presença de seus colaboradores no ambiente da CONTRATANTE, informando nome completo e CPF do técnico para prestação de serviços de instalação ou manutenção.

6.2.20. Fornecer crachá de identificação a seus prepostos durante a realização das atividades no ambiente da CONTRATANTE.

6.2.21. Apresentar mensalmente relatório contendo a planilha de memória de cálculo do faturamento, detalhando:

I) Período de faturamento;

II) Discriminação dos serviços prestados e seus valores;

III) Relação dos eventos, incluindo numeração de chamado, horários de início e término;

IV) Eventos que ensejam descontos contratuais e seus respectivos valores;

V) Totais e subtotais.

6.2.22. Informar, nos relatórios fornecidos, detalhes sobre indisponibilidades ocorridas, incluindo data, período, causas, total de minutos e percentual de disponibilidade do período faturado.

6.2.23. Aplicar os devidos descontos em fatura por descumprimento do IMR, conforme previsto no contrato.

6.2.24. Apresentar mensalmente as faturas dos serviços prestados, acompanhadas da planilha de memória de cálculo definitiva validada pela CONTRATANTE.

6.2.25. Atender a reclamações ou pedidos de esclarecimento relacionados ao faturamento dos serviços contratados.

7. MODELO DE EXECUÇÃO DO OBJETO

7.1. A execução do objeto será conduzida de forma estratégica, visando garantir a plena implementação da solução contratada, conforme os requisitos previamente estabelecidos. A prestação dos serviços envolverá a implantação de um ambiente de segurança cibernética robusto, integrando tecnologias de Firewall de Nova Geração (NGFW), SD- WAN e IA Preditiva, conectividade segura e suporte técnico especializado, de modo a proporcionar alta disponibilidade, eficiência operacional e proteção integral dos ativos digitais da Prefeitura Municipal de Cáceres.

7.2. A prestação do serviço se dará em duas fases, garantindo uma implementação estruturada e um suporte contínuo para a operação da solução contratada, respeitando os prazos estipulados:

7.2.1. **Fase de Implantação** (até 60 dias após a assinatura do contrato):

7.2.1.1. Essa etapa compreende todas as atividades relacionadas à implementação física e lógica da solução. Inclui a instalação e configuração dos equipamentos, ativação dos links dedicados de internet, integração das unidades externas e praças municipais à infraestrutura de comunicação, além da capacitação técnica da equipe da Prefeitura. A fase será concluída com a entrega da documentação técnica detalhada (As Built) e a validação operacional dos serviços prestados.

7.2.1.2. A solução será implantada na sede da Prefeitura e em todas as unidades externas e praças municipais, garantindo conectividade segura e redundante para os serviços essenciais. Para viabilizar a execução adequada, serão instalados e configurados equipamentos de última geração, com capacidade para gerenciar múltiplas conexões simultâneas e otimizar o fluxo de dados.

7.2.1.3. A distribuição dos serviços seguirá a estrutura administrativa do município, contemplando unidades estratégicas vinculadas a diversas secretarias. O quantitativo necessário foi dimensionado considerando a demanda operacional de cada local, garantindo que todos os pontos críticos estejam devidamente atendidos. Entre as unidades contempladas, incluem-se:

7.2.1.3.1. Unidades Centralizadas

SECRETARIA	UNIDADE	LOCALIZAÇÃO	QUANTIDADE
SMEAE	SMEAE - PREFEITURA SEDE (COC)	https://maps.app.goo.gl/qTzbhDM8NCAEBxBf7	1
	UNIDADE CENTRALIZADA 1		1
	UNIDADE CENTRALIZADA 2		1
SMA	SMA - ALMOXARIFADO	https://maps.app.goo.gl/NiAhRcuDi3oF6Qvn9	1
	SMA - GUARDA MUNICIPAL	https://maps.app.goo.gl/hoMkt4EuyDL3BrFKA	1
SMAGRI	SMAGRI	https://maps.app.goo.gl/J1rDH3pp4oPSEfsj7	1
SMASC	SMASC - CCI	https://maps.app.goo.gl/j8UjTvfKLx4ypbPs5	1
SME	SME - CMEC	https://maps.app.goo.gl/ZUD6oU9HeMvLqXe89	1
SMIL	SMIL - GUARITA OBRAS	https://maps.app.goo.gl/PTWC8Lr3aGwXPxnP9	1
	SMIL - GUARITA PORTICO	https://maps.app.goo.gl/u39WX2UzVeVQQWS28	1
	SMIL - OFICINA	https://maps.app.goo.gl/wQmT4CxnPbdKZUYC9	1

TOTAL	**11**

7.2.1.3.2. Unidades Descentralizadas

SECRETARIA	UNIDADE	LOCALIZAÇÃO	QUANTIDADE
SMEAE	SMEAE - DEFESA CIVIL	https://maps.app.goo.gl/zYaMoX5jtfJ1VQ2h8	1
	UNIDADE DESCENTRALIZADA 1	-	1
SMA	SMA - ARQUIVO	https://maps.app.goo.gl/n6Jj6YzpqNfS8cHF7	1
	UNIDADE DESCENTRALIZADA 2	-	1
SMASC	SMASC - ALMOXARIFADO	https://maps.app.goo.gl/CZV2nUAkbYMhY6uq9	1
	SMASC - CASA BELBELITA	https://maps.app.goo.gl/DxddTbATc7X73Bns5	1
	SMASC - CASA DE PASSAGEM	https://maps.app.goo.gl/WrVThbciHZooSfgX6	1
	SMASC - CENTRO DE MULTIPLO USO	https://maps.app.goo.gl/Lz5UoPyGg42jrnUn8	1
	SMASC - CONSELHO TUTELAR	https://maps.app.goo.gl/tyQnNc8nTmMfQ3MW7	1
	SMASC - CRAS I	https://maps.app.goo.gl/xPiY5KnmduNnBgK49	1
	SMASC - CRAS II	https://maps.app.goo.gl/HPNPDMJ2U98R5tRm8	1
	SMASC - CREAS	https://maps.app.goo.gl/xoJqeaMyfF9Ds6g19	1
	SMASC - SAICA	https://maps.app.goo.gl/CCwLfifR6sWyhhdm7	1
	SMASC - GANHA TEMPO	https://maps.app.goo.gl/5AXCG6MYtbiF1gwV7	1
	UNIDADE DESCENTRALIZADA 3	-	1

SME	SME - SECRETARIA DE EDUCAÇÃO	https://maps.app.goo.gl/WbNKuCbpt1rDS5TE7	1
	SME - MERENDA	https://maps.app.goo.gl/byhFeQxucnAjkWfH8	1
	SME - CENTRO MUNICIPAL DE EDUCAÇÃO INFANTIL	https://maps.app.goo.gl/r9P3FHMDnqK3KTGUA	1
	SME - EM 16 DE MARÇO	https://goo.gl/maps/irEBgMynkLFUVdqDA	1

	SME - EM BRINCANDO E APRENDENDO	https://goo.gl/maps/qUYuASgJv5KN9z9v6	1
	SME - EM BURITI	https://goo.gl/maps/oJLMV4MMGaWkxdi7A	1
	SME - EM BUSCANDO O SABER	https://maps.app.goo.gl/52UwvjnQcLHDWQ7k6	1
	SME - EM CENTRO EDUCACIONAL DOM MÁXIMO BIENNÉS	https://goo.gl/maps/BDNwB6uZWrEapfWx5	1
	SME - EM DES. GABRIEL PINTO DE ARRUDA	https://goo.gl/maps/BDCMfHEfwrEELscN9	1
	SME - EM DR. JOSÉ RODRIGUES FONTES	https://maps.app.goo.gl/gN8iVN15FtGRnxbB9	1
	SME - EM DUQUE DE CAXIAS	https://goo.gl/maps/s5PAoUDUNHedzdks6	1
	SME - EM FAZENDO ARTE	https://maps.app.goo.gl/kTP6RNoQeYxuAfPNA	1
	SME - EM GARCÊS	https://goo.gl/maps/3J1HfZuFZ9v5WEcj9	1
	SME - EM GOTINHAS DO SABER	https://goo.gl/maps/mYM52pa2QkFA2j2C9	1
	SME - EM JARDIM GUANABARA	https://goo.gl/maps/Rfg8wh2T7iw4NrbP6	1
	SME - EM JARDIM PARAÍSO	https://goo.gl/maps/kkyMp6LAXieSyvPW9	1
	SME - EM NOVO ORIENTE	https://maps.app.goo.gl/4gacByZXhJ48UMvt5	1
	SME - EM PEQUENO SÁBIO	https://goo.gl/maps/EMEBFPffRm6Tb62a8	1
	SME - EM PROF. EDUARDO BENEVIDES LINDOTE	https://goo.gl/maps/Y43ifBkKTAwNN1U86	1
	SME - EM PROFª ISABEL CAMPOS	https://goo.gl/maps/1MgqjESG46yCxwe88	1

	SME - EM PROFA. ERENICE SIMÃO ALVARENGA	https://goo.gl/maps/yo4E1htCJ5EJYWE48	1
	SME - EM RAQUEL RAMÃO DA SILVA	https://goo.gl/maps/ke1dUMYCGWqwve6P8	1
	SME - EM SANTOS DUMONT	https://goo.gl/maps/uyBXsZNDDszodCxk6	1
	SME - EM TANCREDO NEVES	https://goo.gl/maps/fKVomd6j3LZtfjkS8	1
	SME - EM VILA IRENE	https://goo.gl/maps/aGdb2PV6NF3Yoxhe7	1
	SME - EM VILA REAL	https://goo.gl/maps/dfKNaDkEfK2V8YiJ8	1
	SME - EM VITÓRIA RÉGIA	https://goo.gl/maps/vP5EUrdTiHhhw13y6	1
	SME - EMEI FREI GRIGNION	https://goo.gl/maps/LmB1VSuePV8FtSXHA	1
	SME - EMEI IRENE COELHO CRUZ	https://goo.gl/maps/BiLhvdeg1tRmiuR37	1
	SME - EMEI MADRE MARIA ESTEVÃO	https://goo.gl/maps/kRXo9FN7eFvufAaV8	1
	SME - EMEI PROFESSORA DULSÂNGELA DE ALMEIDA SOUZA	https://maps.app.goo.gl/QZKQCN7SU9D2qwgd8	1
	SME- LIMOEIRO	https://goo.gl/maps/nrqaUDmiZV3xDpUN9	1
	SME - NOSSA SENHORA APARECIDA	https://goo.gl/maps/uYpxYHJzCmm6Qo1w8	1
	SME - PAULO FREIRE	https://maps.app.goo.gl/DE7sbzdMQVbaQXS77	1
	SME - PROFª LÉA MARIA LARA SILVA	https://maps.app.goo.gl/pjrMdwiU6wSSn3Uf7	1

	SME - PROVÍNCIA DE AREZZO	https://goo.gl/maps/NSNEbdrq1cjknywX8	1
	SME - ROÇA VELHA	https://goo.gl/maps/fGfEoY7trAGZhmS9A	1
	SME - SANTA CATARINA	https://goo.gl/maps/VzU6r8C8TVQJc3RM7	1
	SME - SANTO ANTÔNIO DO CARAMUJO	https://goo.gl/maps/ducAKNjzSQXECMHj9	1
	SME - SOTECO	https://maps.app.goo.gl/P32RY2iPJR7VLC9p7	1
	SME - TRANSPORTE EDUCAÇÃO	https://maps.app.goo.gl/cQumZ9jvaygvLQ159	1
	SME - EM UNIÃO	https://goo.gl/maps/zxtNZfD4YSyKrDVk8	1
	SME - CLARINÓPOLIS	https://goo.gl/maps/ducAKNjzSQXECMHj9	1
	SME - INFRAESTRUTURA EDUCAÇÃO	https://maps.app.goo.gl/b3bCUzB8qwz7vRd77	1
	SME - LARANJEIRA I	https://goo.gl/maps/jB1SZ3za3cdYev4a6	1
	SME - SÃO FRANCISCO	https://maps.app.goo.gl/sxzj1LsfxkFEX7Zy6	1
	UNIDADE DESCENTRALIZADA 4	-	1
	UNIDADE DESCENTRALIZADA 5	-	1
	UNIDADE DESCENTRALIZADA 6	-	1
	UNIDADE DESCENTRALIZADA 7	-	1
SMMADE	SMMADE	https://maps.app.goo.gl/zYaMoX5jtfJ1VQ2h8	1
	UNIDADE DESCENTRALIZADA 8	-	1
	SMEL - CIE	https://maps.app.goo.gl/Kkk4g4zUipLG7RDw6	1

SMEL	SMEL - DIDI PROFETA	https://maps.app.goo.gl/wUmbU83AgrRCFAjy6	1
	UNIDADE DESCENTRALIZADA 9		1
SMIL	SMIL - AEROPORTO	https://maps.app.goo.gl/N6nKAp5k4TpbGE1n6	1
	UNIDADE DESCENTRALIZADA 10		1
SMS	SMS - SECRETARIA DE SAUDE	https://maps.app.goo.gl/VWf4EYS5mnNdMk85A	1
	SMS - CAPS, AMBULATÓRIO DERMATOLÓGICO, LABORATORIO MUNICIPAL, ALMOXARIFADO, CMS	https://maps.app.goo.gl/3YsQdJ4PJUVqd6nG7	1
	SMS - CAPSI INFANTO JUVENIL	https://maps.app.goo.gl/NRE6n76fGEMAzeyy9	1
	SMS - CENTRO DE ESPECIALIDADES MEDICAS CEM	https://maps.app.goo.gl/zkjGjchEE1wsL14r8	1
	SMS - CENTRO DE SAUDE REFERENCIAL	https://maps.app.goo.gl/Z5MEaMJi68dU5hrG6	1
	SMS - CENTRO REAB DOM AQUINO CORREA CACERES CER II	https://maps.app.goo.gl/VhCQc4YayPyXp7sj8	1
	SMS - CEO	https://maps.app.goo.gl/wZMwZd1mfqVrkuRW6	1
	SMS - CTA CENTRO DE TESTAGEM E ACONSELHAMENTO SAE CACERES	https://maps.app.goo.gl/QPC3oTbJjodwapDV7	1

	SMS - FARMACIA BASICA DA SMS	https://maps.app.goo.gl/YwUSzHzPiKE5h3Vy8	1
	SMS - FROTAS	https://maps.app.goo.gl/UQZEQZxDpudbq1wH7	1
	SMS - POSTO DE SAUDE DA PAIOL	https://maps.app.goo.gl/PHsDSTgdLW1CdkacA	1
	SMS - POSTO DE SAUDE DE VILA APARECIDA	https://maps.app.goo.gl/uGRnxEjReD6jHpJ9A	1
	SMS - POSTO DE SAUDE DO LIMAO	https://maps.app.goo.gl/CfPip6ysDGqhiWmT6	1
	SMS - POSTO DE SAUDE HORIZONTE DOESTE	https://maps.app.goo.gl/6bkzEYMH7wQsigL49	1
	SMS - POSTO DE SAUDE LARANJEIRAS	https://maps.app.goo.gl/XpkQdasWsWE86U9q6?g_st=aw	1
	SMS - POSTO DE SAUDE PROF VERA LYGIA BALDO FACAO	https://maps.app.goo.gl/f6PfkXjMQjTudKqZ8	1
	SMS - POSTO DE SAUDE SADIA	https://maps.app.goo.gl/H29oLsoimParvAwv8	1
	SMS - UNID DE SAUDE DA FAMILIA VISTA ALEGRE	https://maps.app.goo.gl/FirXbqEx2srZf787A	1
	SMS - UNID SAUDE DA FAMILIA VITORIA REGIA	https://maps.app.goo.gl/mZmvrRyEijHAnTFY7	1
	SMS - UNIDADE BASICA DE SAUDE DR ADEMAR ROCHA DE OLIVEIRA CAVALHADA	https://maps.app.goo.gl/8gjpYWP87HBqcoZ46	1
	SMS - UNIDADE BASICA DE SAUDE JARDIM DAS	https://maps.app.goo.gl/tT5o6Y7N38AVLUkZ9	1

	OLIVEIRAS		
	SMS - UNIDADE BASICA DE SAUDE SANTA ISABEL	https://maps.app.goo.gl/kUwep6ZQ8h7MucdX7	1
	SMS - UNIDADE DE SAUDE DA FAMILIA COHAB NOVA	https://maps.app.goo.gl/2dwof9LpsMAPALtM7	1
	SMS - UNIDADE DE SAUDE DA FAMILIA DO CAIC	https://maps.app.goo.gl/oJAf3xrRqWLe5Jev8	1
	SMS - UNIDADE DE SAUDE DA FAMILIA DO RODEIO	https://maps.app.goo.gl/2jADTBF6EXEvx9Ew6	1
	SMS - UNIDADE DE SAUDE DA FAMILIA JD PARAISO	https://maps.app.goo.gl/TdhriFPJ8nPUpFVx6	1
	SMS - UNIDADE DE SAUDE DA FAMILIA VILA REAL	https://maps.app.goo.gl/E1nPn9mTybVmcB267	1
	SMS - UNIDADE DE SAUDE SANTOS DUMONT	https://maps.app.goo.gl/oZuia8p4RaSbPKzP7	1
	SMS - UNIDADE DE SAUDE UNIVERSITÁRIO	https://maps.app.goo.gl/vYJEuN1ufGKzoEeK7	1
	SMS - UNIDADE SAUDE FAMILIA DO CARAMUJO	https://maps.app.goo.gl/zhXa1oX3UQzTwcHj9	1
	SMS - UNIDADE SAUDE FAMILIA JARDIM GUANABARA	https://maps.app.goo.gl/bRE93W32464phEPJ7	1

	SMS - UPA PRONTO ATENDIMENTO JOSE SOUTO FARIAS	https://maps.app.goo.gl/mgaRTmkRznLoMFrY7	1
	SMS - VIGILANCIA EM SAÚDE	https://maps.app.goo.gl/YJFGaUT4mc3VeFoV6	1
	UNIDADE DESCENTRALIZADA 11	-	1
	UNIDADE DESCENTRALIZADA 12	-	1
	UNIDADE DESCENTRALIZADA 13	-	1
	UNIDADE DESCENTRALIZADA 14	-	1
SMTC	SMTC	https://maps.app.goo.gl/sMPDMtU3poAP51LF7	1
	SMTC - CASA DAVERON	https://maps.app.goo.gl/fHqLcuW2X5nJCHBv6	1
	SMTC - BIBLIOTECA	https://maps.app.goo.gl/6cGeYMDAR1YMQXTX 6	1
	SMTC - CLUBINHO 2000	https://maps.app.goo.gl/vaUxdTdcihpHVacH9	1
	SMTC - MUSEU	https://maps.app.goo.gl/kKvwGsx58CZmAqDfA	1
	UNIDADE DESCENTRALIZADA 15	-	1
TOTAL			**115**

7.2.1.3.3. Praças Públicas

SECRETARIA	**PRAÇA**	**LOCALIZAÇÃO**	**QUANTIDADE**
	SMEAE - AROLDO FANAIA	https://maps.app.goo.gl/8J86ycmMgagCRjCb6	1
	SMEAE - COHAB VELHA	https://maps.app.goo.gl/ExPmvCxJtbZ6Tsxk6	1

SMEAE	SMEAE - PRAÇA BENJAMIN CONSTANT	https://goo.gl/maps/Bp9fHEKnFKQ4shkB7	1
	SMEAE - PRAÇA CARAMUJO	https://maps.app.goo.gl/7h6GapqJ9cnAkc8T7	1
	SMEAE - PRAÇA CIDADE ALTA	https://goo.gl/maps/MxXmDgoFqVtZdNex8	1
	SMEAE - PRAÇA CIDADE NOVA	https://maps.app.goo.gl/W8wgiTyN45SChQ9d8	1
	SMEAE - PRAÇA COHAB NOVA	https://goo.gl/maps/7xNnbDpDas9VePnN9	1
	SMEAE - PRAÇA DA FEIRA - CENTRO	https://goo.gl/maps/sjqGYtg7KatQcwcZ8	1
	SMEAE - PRAÇA DNER - BOMBEIROS	https://goo.gl/maps/3tgxS4Uz2pnsdPxH9	1
	SMEAE - PRAÇA DO GERALDÃO	https://goo.gl/maps/iGDeEFGjFZqQ3ct79	1
	SMEAE - PRAÇA DO MONTE VERDE	https://goo.gl/maps/VDYK2HWXctL7tgmV6	1
	SMEAE - PRAÇA DOM MÁXIMO	https://goo.gl/maps/om21uh8nLLWQdJs1A	1
	SMEAE - PRAÇA DUQUE DE CAXIAS - CENTRO	https://goo.gl/maps/sjqGYtg7KatQcwcZ8	1
	SMEAE - PRAÇA HORIZONTE D'OESTE	https://maps.app.goo.gl/yNFf1xADWNWK6NkZ6	1
	SMEAE - PRAÇA JARDIM AEROPORTO	https://goo.gl/maps/W6oEg6qd6pwi7MwF9	1
	SMEAE - PRAÇA JARDIM DA OLIVEIRA (EMPA)	https://maps.app.goo.gl/Z1yuZWjrLsYP5jwP7	1

	SMEAE - PRAÇA JARDIM PARAISO	https://maps.app.goo.gl/pYiSUbjpqciUhE3N9	1
	SMEAE - PRAÇA JARDIM SÃO LUIZ	https://maps.app.goo.gl/nBF5xryfXZoMWjUQ9	1
	SMEAE - PRAÇA JARDIM UNIVERSITÁRIO III	https://goo.gl/maps/ofActSaScSGdXz4R6	1
	SMEAE - PRAÇA JOSÉ DE ANCHIETA	https://goo.gl/maps/A8WHwD7BX6NUWhJT6	1
	SMEAE - PRAÇA JUNCO	https://maps.app.goo.gl/qXAReBWJ7BQRPpkM9	1
	SMEAE - PRAÇA MAJOR JOÃO CARLOS	https://goo.gl/maps/Qcwdn4CXJdT5VCWQ6	1
	SMEAE - PRAÇA MEDEIROS	https://goo.gl/maps/HUThKqHzuPa6ABpEA	1
	SMEAE - PRAÇA NOVA ERA (CAMPO)	https://maps.app.goo.gl/YQKX7SBhzB9dcjcj9	1
	SMEAE - PRAÇA PANTANAL	https://goo.gl/maps/AUKWENW5iR2gENDT7	1
	SMEAE - PRAÇA RESIDENCIAL ANA PAULA	https://goo.gl/maps/pA2tyTfhq8jqo5Fk7	1
	SMEAE - PRAÇA SANTA CRUZ	https://maps.app.goo.gl/KFsn7XrjbpDGFV1X9	1
	SMEAE - PRAÇA SANTA ISABEL	https://maps.app.goo.gl/TBJYXELoqvGd7Lkm9	1
	SMEAE - PRAÇA SANTO ANTONIO	https://maps.app.goo.gl/Tu2hhrXUFw4rSABn6	1
	SMEAE - PRAÇA SÃO JORGE	https://goo.gl/maps/MxXmDgoFqVtZdNex8	1
	SMEAE - PRAÇA SÃO LOURENÇO (CAMPO)	https://maps.app.goo.gl/bouowePQbhfCzuRm7	1
	SMEAE - PRAÇA	https://goo.gl/maps/TeYnV6RyQdD3d4Zo8	1

	SÃO MIGUEL		
	SMEAE - PRAÇA VALTER FIDELIS - VILA REAL	https://maps.app.goo.gl/PyeiqkA6niDZH3hE9	1
	SMEAE - PRAÇA VILA APARECIDA	https://maps.app.goo.gl/Cjpoxp8VnhRTkBMa9	1
	SMEAE - PRAÇA VILA REAL	https://maps.app.goo.gl/Yp8X21VytfkPPvgw6	1
	SMEAE - PRAÇA VITÓRIA RÉGIA	https://goo.gl/maps/mJXKjDVQASbukgY37	1
	SMEAE - RODOVIÁRIA	https://maps.app.goo.gl/8LyQniCzZ74f3oCC7	1
	SMEAE - SADIA	https://maps.app.goo.gl/tc1GB5cCztjYFNtm9	1
	PRAÇA MUNICIPAL 1		1
	PRAÇA MUNICIPAL 2		1
	PRAÇA MUNICIPAL 3		1
	PRAÇA MUNICIPAL 4		1
SMTC	SMTC - PALCO DE EVENTOS SEMATUR	https://maps.app.goo.gl/WsUtv8cTtAgazbeP9	1
	SMTC - PRAÇA BARÃO	https://maps.app.goo.gl/vP3qT3xGyzzbTkVf8	1
	PRAÇA MUNICIPAL 5		1
	PRAÇA MUNICIPAL 6		1
TOTAL			**46**

7.2.2. **Fase de Prestação de Serviço Mensal** (até 180 meses após a assinatura do contrato):

7.2.2.1. Após a implantação, será iniciada a fase de operação contínua da solução, garantindo a manutenção preventiva e corretiva dos equipamentos, suporte técnico especializado, monitoramento em tempo real da infraestrutura de segurança cibernética e otimização do tráfego de rede com tecnologia SD- WAN. Essa fase inclui a prestação de serviços de segurança cibernética baseada em Inteligência Artificial Preditiva, bem como a consultoria contínua para aprimoramento da política de segurança da informação do município.

7.3. Além da estruturação física, a execução do contrato incluirá a implantação de links dedicados de internet para garantir alta disponibilidade, com redundância de ASN e rotas distintas, estabilidade para os serviços administrativos e operacionais e alternativa de contingência para evitar interrupções.

nos serviços

7.4. O serviço de Link de Internet para as localidades que serão contempladas com WI-FI Social deverá ser implantado impreterivelmente em até 30 (trinta) dias a partir da ordem de serviço emitida pelo Gestor do Contrato.

7.5. Para o Lote único a CONTRATADA deverá cumprir os eventos descritos na tabela a seguir, respeitando os prazos máximos estabelecidos

MARCOS DIA	**PRAZOS MÁXIMOS (EM DIAS)**	**EVENTO**	**RESPONSÁVEL**
D0		Assinatura do contrato entre o CONTRATANTE e a empresa licitante vencedora.	CONTRATANTE e a CONTRATADA
D1		Emissão da Ordem de Serviço pelo CONTRATANTE	CONTRATANTE
D2	D1+2	Entrega do projeto executivo	CONTRATADA
D3	D2+2	Aprovação do projeto executivo	CONTRATANTE
D4	D1+15	Entrega dos link de Internet e WI-FI nas praças, contemplando toda a solução de segurança de SDWAN e NGFW	CONTRATADA
D5	D4+3	Emissão do Termo de Recebimento provisório, para início da conferência do serviço entregue dos Links de Internet das praças	CONTRATANTE
D6	D5+5	Emissão do Termo de Recebimento Definitivo, autorização para emissão de faturamento e início do período de execução dos serviços dos Links de Internet das praças	CONTRATANTE
D7	D1+60	Conclusão da entrega, instalação e configuração dos equipamentos, capacitação e operacionalização de todos os links de comunicação, Firewall, IA Preditiva, sensores de cibersegurança, SDWAN, NGFW	CONTRATADA
D8	D7+3	Emissão do Termo de Recebimento provisório, para início da conferência do serviço entregue.	CONTRATANTE
D9	D8+5	Emissão do Termo de Recebimento Definitivo, autorização para emissão de faturamento e início do período de execução dos serviços de links de comunicação, Firewall, Sensores de Cibersegurança, SDWAN, NGFW	CONTRATANTE

7.6. A instalação da solução será realizada por uma empresa homologada e credenciada, com compromisso

rio - 029/2025

solidário ao fabricante, garantindo a fluidez da implantação dentro do prazo estipulado no edital. Para assegurar a operacionalidade da solução, serão promovidas capacitações técnicas para a equipe da Prefeitura, visando aprimorar a gestão e monitoramento dos sistemas implementados.

7.7. O modelo de execução do objeto visa garantir não apenas a segurança cibernética e a conectividade da administração pública municipal, mas também a eficiência na prestação de serviços essenciais à população, promovendo inovação, resiliência e modernização tecnológica.

8. MODELO DE GESTÃO DO CONTRATO

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

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

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

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

8.5. Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

8.6. **Fiscalização**

8.6.1. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput), nos termos do Decreto nº 665 de 09 de outubro de 2024.

8.6.2. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

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

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

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

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

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

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

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

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

8.6.5. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

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

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

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

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

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

9. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

9.1. **Forma de Acompanhamento da Garantia e Níveis de Serviço**

9.1.1. Para cumprir com os níveis de disponibilidade a prestadora de serviços deve trabalhar com duas variáveis principais: o MTBF (Tempo médio entre falhas) da solução, e o MTTR (Tempo médio de reparação de falhas). Para aumentar a disponibilidade deve-se aumentar o MTBF e diminuir o MTTR, de forma que o sistema apresente falhas com menor frequência e que estas sejam recuperadas mais rapidamente.

Abaixo estão listados os valores de disponibilidade mensal para cada Item deste Termo:

ITEM	SERVIÇO	DISPONIBILIDADE
1	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)	99,8%
2	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	99,8%
3	Serviço de Link dedicado de Acesso à internet, bloco /29 e Banda Mínima de Acesso Garantida de 500Mbps (Alta Disponibilidade) SEDE (Dois Link de ASN e Rota Diferentes)	99,8%
4 5	Serviço de Link de acesso à Internet Sites Remotos, aplica-se ao WIFI Social	99,2%

9.2. Nas planilhas abaixo estão detalhados todos os indicadores destinados à aferição dos níveis mínimos de serviço da contratação pretendida. Na apuração dos indicadores poderão ser confrontados os dados da solução de gerenciamento da CONTRATADA e do sistema de monitoramento da CONTRATANTE.

MÉTRICA 1 - DISPONIBILIDADE (IMR-01)	
Indicador de Qualidade	Índice de Disponibilidade.

Métrica	Indicador é calculado com a seguinte forma: **IDM=[(To - Ti)/To]*100** Onde: IDM = índice de disponibilidade mensal do LINK em % To = período de operação (um mês) em minutos. Ti = somatório dos tempos de inoperância durante o período de operação (1 mês) em minutos. No caso de inoperância reincidente num período inferior a 3 horas, contado a partir do restabelecimento do link da última inoperância, considerar-se-á como tempo de indisponibilidade do enlace o início da primeira inoperância até o final da última inoperância, quando o link estiver totalmente operacional. Os tempos de inoperância serão os tempos em que os links apresentarem problemas que serão obtidos dos chamados abertos no sistema de abertura de chamados técnicos (Trouble Ticket) e os tempos de indisponibilidade computados pela violação do indicador de Retardo. Somente serão desconsiderados os tempos de inoperância causados por manutenções programadas com o CONTRATANTE, ressalvados, contudo, os casos fortuitos e de força maior.
Periodicidade de Aferição	Mensal
Limiar de Qualidade	Vide Item 9.1 - Forma de Acompanhamento da Garantia e Níveis de Serviço
Pontos de Controle	A CONTRATADA realizará, por meio da sua solução de gerenciamento, a coleta e armazenamento de

	informações a respeito de todos os serviços pelo tempo de duração do contrato.
Relatórios de Níveis de Serviço	A CONTRATADA deverá disponibilizar mensalmente à CONTRATANTE, relatórios com os índices apurados, totalizados e apresentados mensalmente por serviço. Nos relatórios citados deverão ser apresentados: o número do ticket, tempo de indisponibilidade (horas e minutos), o tempo de interrupções programadas, o tempo de interrupções de responsabilidade da CONTRATANTE. A CONTRATADA deverá disponibilizar, quando demandada pelo CONTRATANTE, relatório detalhando os tempos de falhas (com hora de início e fim da inoperância), minutos excedentes ao prazo máximo para reparo e disponibilidade no período (mês) e motivo(s) da(s) indisponibilidade(s) apurada(s). Após análise do fiscal técnico, poderá ser desconsiderado do período de inoperância, o tempo decorrente da impossibilidade da CONTRATADA acessar os equipamentos nas instalações da CONTRATANTE, comprovando a CONTRATADA que o problema estava nas dependências da CONTRATANTE.

MÉTRICA 2 - TAXA DE ERRO (IMR-02)	
Indicador de Qualidade	Percentual de erros nos enlaces.
Métrica	Indicador é calculado com a seguinte fórmula: **TER = (QEQ / TTQ)* 100** Sendo: TER = Indicador de taxa de erro; TTQ = Quantidade total de quadros enviados ou recebidos em um determinado período; QEQ = Quantidade de erros identificados em um determinado período. Para efeito de mensuração desta métrica utiliza-se as seguintes considerações: • Quadro é a unidade de transferência de dados na camada de enlace do modelo OSI, ou seja, o frame Ethernet; • Os erros devem ser reportados pelo roteador da CONTRATADA utilizado na conexão com a rede da CONTRATANTE; • Serão considerados os erros em ambas as interfaces de ingresso e egresso no roteador da CONTRATADA.
Periodicidade de Aferição	Esta métrica deverá ser aferida, ininterruptamente, em intervalos de 5 minutos.
Limiar de Qualidade	0,5%
Pontos de Controle	O período utilizado no cálculo da métrica e, quando for o caso, o período considerado como indisponível será o do intervalo entre as aferições

MÉTRICA 3 - LATÊNCIA (IMR-03)	
Indicador de Qualidade	Tempo de latência de ida e volta do pacote através do link contratado
Métrica	A latência deve mensurar o tempo do trajeto de ida-e-volta (RTT - round trip time) de um pacote do tipo ICMP com tamanho de 1000 bytes. Para efeito de mensuração desta métrica utiliza-se as seguintes considerações: • Para os links Internet, as medições de latência devem ser feitas entre o Roteador Internet ou Appliance SD-WAN e o primeiro roteador da CONTATADA na Internet. • Pacote é a unidade de transferência de dados na camada de redes do modelo OSI, ou seja os datagramas TCP, UDP, ICMP e ARP; • O envio de pacotes para obtenção dos quantitativos utilizados no cálculo desta métrica deve ocorrer entre dois pontos distintos e remotos, um localizado no segmento de rede da CONTRATANTE onde estiver conectado o roteador da CONTRATADA, e outro localizado em segmento de rede de terceiros que estejam ligados a Internet por meio da rede da mesma CONTRATADA, ou em segmento de rede utilizado para troca de tráfego entre de operadoras de acesso a Internet (Pontos

	de Troca de Tráfego), podendo inclusive, tratar-se dos roteadores de borda da CONTRATADA conectados aos segmentos aqui mencionados. Serão desconsiderados os períodos em que os valores mensurados ultrapassem o limite aceitável desta métrica, caso a volume médio de utilização do link no mesmo período seja superior a 80% da velocidade do respectivo enlace.
Mínimo aceitável	Links de Internet: 65 ms
Periodicidade Aferição	Esta métrica deverá ser aferida, ininterruptamente, em intervalos de 5 minutos. O período utilizado no cálculo da métrica será o período do intervalo entre as aferições

MÉTRICA 4 – PERDA DE PACOTES (IMR-04)	
Indicador de Qualidade	Percentual de perda de pacotes IP ao longo da rede da CONTRATADA em um determinado período.
Métrica	Indicador é calculado com a seguinte forma: **TPP = (QPP / QTP)* 100** Sendo: TPP = Indicador de perda de pacotes QTP = Quantidade total de pacotes enviados ou recebidos em um determinado período QPP = Quantidade de pacotes perdidos em um determinado período Para efeito de mensuração desta métrica utiliza-se as seguintes considerações: • Pacote é a unidade de transferência de dados na camada de redes do modelo OSI, ou seja os datagramas TCP, UDP, ICMP e ARP; • O envio de pacotes para obtenção dos quantitativos utilizados no cálculo desta métrica deve ocorrer entre dois pontos distintos e remotos, um localizado no segmento de rede da CONTRATANTE onde estiver conectado o roteador da CONTRATADA, e outro localizado em segmento de rede de terceiros que estejam ligados a Internet por meio da rede da mesma CONTRATADA, ou em segmento de rede utilizado para troca de tráfego entre de operadoras de acesso à Internet (Pontos de Troca de Tráfego), podendo inclusive, tratar-se dos roteadores de borda da CONTRATADA conectados aos segmentos aqui mencionados. Serão desconsiderados os períodos em que os valores mensurados ultrapassem o limite aceitável desta métrica, caso a volume médio de utilização do link no mesmo período seja superior a 80% da velocidade do respectivo enlace.
Máximo	3% de perda

aceitável	
Periodicidade	Esta métrica deverá ser aferida, ininterruptamente, em intervalos de 5 minutos.
Aferição	O período utilizado no cálculo da métrica será o período do intervalo entre as aferições.

MÉTRICA 5 – PRAZO PARA ALTERAÇÃO DE CONFIGURAÇÃO DOS EQUIPAMENTOS SOLICITADOS PELO CONTRATANTE	
Indicador de Qualidade	Prazo, em horas, para a contratada alterar a configuração dos equipamentos solicitada pelo CONTRATANTE.
Métrica	Apuração mensal do tempo que a contratada executa e apresente uma alteração na configuração de equipamentos, a partir do momento do registro da solicitação de alteração da configuração na base de dados relativa à solução de gerenciamento do Provedor e de comparação com o valor do Limiar de Qualidade desta tabela. **PA = Taa – Tsa** onde: PA = Prazo de alteração da configuração de equipamentos Taa = Instante da aceitação pela da alteração Tsa = Instante da solicitação da alteração

Periodicidade de Aferição	Mensal
Limiar de Qualidade	Prazo máximo: 48 horas após a solicitação de alteração da configuração pela CONTRATANTE. Em caso de agendamento pelo CONTRATANTE este prazo ficará suspenso.
Pontos de Controle	De acordo com os registros na Central de Atendimento.
Relatórios de Níveis de Serviço	A CONTRATADA deverá disponibilizar mensalmente à CONTRATANTE, relatórios com os índices apurados, totalizados e apresentados mensalmente por serviço. Nos relatórios citados deverão ser apresentados: o número do ticket, tempo de indisponibilidade (horas e minutos), o tempo de interrupções programadas, o tempo de interrupções de responsabilidade da CONTRATANTE.
Descontos	Para cada 1 (uma) hora acima do Prazo para Alteração de Configuração de Equipamentos (PAC), será implicado à contratada desconto correspondente a 2,0% (dois por cento), calculado sobre o valor mensal do circuito afetado. O referido desconto deverá ser retratado nos relatórios de prestação dos serviços, junto ao faturamento, apresentados mensalmente por enlace.

9.3. **Recebimento do Objeto**

9.3.1. A emissão do Termo de Recebimento Definitivo é o marco inicial da efetiva prestação do serviço contratado, nas condições em que foram definidas pela CONTRATANTE neste instrumento.

9.3.2. Os serviços serão recebidos provisoriamente, no prazo de até 3 (três) dias, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. (Art. 140, I, a , da Lei nº 14.133 e Arts. 22, X e 23, X do Decreto nº 11.246, de 2022);

9.3.2.1. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda do contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga;

9.3.2.2. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico. (Art. 22, X, Decreto nº 11.246, de 2022);

9.3.2.3. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo. (Art. 23, X, Decreto nº 11.246, de 2022)

9.3.2.4. O fiscal setorial do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo.

9.3.3. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato:

9.3.3.1. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição

de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

9.3.3.2. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório. (Art. 119 c/c art. 140 da Lei nº 14133, de 2021)

9.3.3.3. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

9.3.3.4. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

9.3.4. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

9.3.5. Os serviços serão recebidos definitivamente no prazo de 7(sete) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

9.3.5.1. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento (art. 21, VIII, Decreto nº 11.246, de 2022).

9.3.5.2. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções;

9.3.5.3. Emitir Termo Circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e

9.3.5.4. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

9.3.5.5. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão

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

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

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

9.3.9. Será permitido a emissão do Termo de Recebimento Definitivo, de forma individual, para serviço de Link de Internet WI-FI nas praças.

9.4. **Sanções Administrativas e Procedimentos Para Retenção ou Glosa no Pagamento**

9.4.1. **Descontos Aplicáveis em Caso de Descumprimento do IMR**

9.4.1.1. Durante a vigência do contrato poderão ser aplicados descontos na fatura, em caso de eventual descumprimento do Instrumento de Medição de Resultado (IMR), a título de glosa, limitando-se cada um ao limite do valor mensal do contrato.

9.4.1.2. Para fins de cálculo do valor do desconto de glosa contratual serão observados os critérios do **Item**

9.1. Forma de Acompanhamento da Garantia e Níveis de Serviço, nos termos do Instrumento de Medição de Resultado - IMR, aplicando os descontos correspondentes à disponibilidade mensal aferida, conforme a tabela abaixo:

ITEM	**SERVIÇO**	**FAIXA ATÉ 24H**	**FAIXA 24H ATÉ 48H**	**FAIXA ACIMA 48 H**
1	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN Sede (Alta Disponibilidade)	0,01% /min	0,02% /min	0,02% /min multa moratória prevista no subitem 9.4.3.1
2	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	0,01% /min	0,02% /min	0,02% /min multa moratória prevista no subitem 9.4.3.1
3	Serviço de Link dedicado de Acesso à internet, bloco /29 e Banda Mínima de Acesso Garantida de 500Mbps (Alta Disponibilidade) SEDE (Dois Link de ASN e Rota Diferentes)	0,01% /min	0,02% /min	0,02% /min multa moratória prevista no subitem 9.4.3.1
4 5	Serviço de Link de acesso à Internet Sites Remotos, aplica-se ao WIFI Social	0,009% /min	0,025% /min	0,025% /min

9.4.1.3. Em caso do não cumprimento da Métrica 5 do IMR o desconto será aplicado conforme abaixo:

MÉTRICA	**FAIXA ATÉ 48H**	**FAIXA 48H ATÉ 72H**	**FAIXA ACIMA 72H**

MÉTRICA 5 - Solicitação de alteração de configuração dos equipamentos - Prazo 48 horas	2,0% /hora	2,5% /hora	2,5% /hora + multa moratória prevista no subitem 9.4.3.1

9.4.1.4. Nos cálculos de desconto, em que a faixa for ultrapassada, todo o cálculo deverá ser feito na faixa posterior.

9.4.1.5. O valor do desconto será aplicado no mês imediatamente subsequente ao mês em que ocorreram os fatos causadores dos descontos, tendo como base o valor vigente do acesso do mês da ocorrência da interrupção.

9.4.1.6. Os descontos não poderão ultrapassar o valor do item do serviço prestado.

9.4.2. **Sanções Aplicáveis Fase de Instalação**

9.4.2.1. O atraso injustificado no cumprimento do objeto sujeitará a CONTRATADA às seguintes penalidades:

- Advertência;
- Multa moratória no valor de 1% do valor anual do contrato para o enlace, por dia de atraso, limitado a 10 dias, pelo atraso injustificado na entrega do projeto executivo, podendo ser adotadas medidas administrativas para rescisão contratual por inexecução total da obrigação. Entende-se por enlace/circuito como qualquer link Internet nos Sites Remotos e na Sede do CONTRATANTE;
- Multa moratória no valor de 1% do valor anual do contrato para o enlace, por dia de atraso, limitado a 30 dias, pelo atraso injustificado na instalação e configuração dos enlaces contratados, podendo ser adotadas medidas administrativas para rescisão contratual por inexecução total da obrigação. Entende-se por enlace/circuito como qualquer link Internet nos Sites Remotos e na Sede do CONTRATANTE.

9.4.3. **Sanções Aplicáveis Fase de Operação**

9.4.3.1. Caso a CONTRATADA ultrapasse a última faixa dos descontos aplicáveis, além da aplicação dos descontos, será imposta multa moratória de 1% do valor mensal do serviço não atendido no IMR, limitada a 10 dias.

9.4.3.2. A não manutenção das condiç 9.4.3.3.

9.4.3.4. ões de habilitação da empresa ao longo da execução do contrato poderá ensejar sua rescisão unilateral pelo CONTRATANTE, após devido processo administrativo, assegurados o contraditório e a ampla defesa, além da aplicação de multa de 30% sobre o valor da parcela inadimplida.

9.4.3.5. A multa poderá ser aplicada cumulativamente com outras penalidades previstas no contrato ou na legislação vigente.

9.4.3.6. A inexecução total ou parcial do contrato poderá resultar em rescisão, nos termos deste instrumento e dos arts. 155 e 156 da Lei nº 14.133/21, incluindo indenização por eventuais prejuízos causados ao CONTRATANTE.

9.4.3.7. A aplicação das sanções será realizada mediante processo administrativo específico, assegurados o contraditório e a ampla defesa, com comunicação formal da penalidade à CONTRATADA.

9.4.3.7.1. A critério da autoridade competente, com base nos princípios da proporcionalidade e razoabilidade, as penalidades poderão ser atenuadas ou relevadas mediante comprovação fundamentada, desde que requeridas por escrito no prazo de 5 dias úteis a contar da notificação.

9.4.3.8. O atraso no pagamento de multas será corrigido pelo IPCA, divulgado pelo IBGE.

9.4.3.9. O CONTRATANTE registrará no SICAF todas as penalidades aplicadas à CONTRATADA.

9.4.4. **Sanções Administrativas**

9.4.4.1. Comete infração administrativa, nos termos da Lei nº 14.133/2021, a CONTRATADA que:

9.4.4.1.1. Der causa à inexecução parcial ou total do contrato, especialmente quando causar grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

9.4.4.1.2. Deixar de entregar documentação exigida no certame ou para a contratação;

9.4.4.1.3. Não manter a proposta, salvo por fato superveniente devidamente justificado;

9.4.4.1.4. Ensejar o retardamento injustificado da execução do objeto;

9.4.4.1.5. Apresentar declaração ou documentação falsa durante a licitação ou execução do contrato;

9.4.4.1.6. Fraudar a licitação ou praticar atos fraudulentos na execução do contrato;

9.4.4.1.7. Adotar comportamento inidôneo, praticar fraudes ou atos ilícitos visando frustrar os objetivos da licitação;

9.4.4.1.8. Praticar ato lesivo conforme o art. 5º da Lei nº 12.846/2013.

9.4.4.2. Pela inexecução total ou parcial do contrato, poderão ser aplicadas as seguintes sanções:

9.4.4.2.1. Advertência, quando não se justificar penalidade mais grave;

9.4.4.2.2. Multa, variando entre 0,5% e 30% do valor do contrato, conforme art. 155 da Lei nº 14.133/2021;

9.4.4.2.3. Impedimento de licitar e contratar, pelo prazo máximo de 3 anos, nos casos de infrações previstas nos incisos II a VII do art. 155 da Lei nº 14.133/2021, quando não for cabível penalidade mais severa;

9.4.4.2.4. Declaração de inidoneidade para licitar e contratar, pelo prazo de 3 a 6 anos, nos casos das infrações previstas nos incisos VIII a XII do art. 155 da Lei nº 14.133/2021, bem como naquelas previstas nos incisos II a VII que justifiquem penalidade mais grave.

9.4.4.3. Na aplicação das sanções, serão considerados:

9.4.4.3.1. A natureza e a gravidade da infração;

9.4.4.3.2. As peculiaridades do caso concreto;

9.4.4.3.3. Circunstâncias agravantes ou atenuantes;

9.4.4.3.4. Os danos causados à Administração Pública;

9.4.4.3.5. A existência de programa de integridade na empresa.

9.4.4.4. A sanção prevista no item 9.4.4.2.4. será precedida de análise jurídica observando as seguintes regras:

9.4.4.4.1. Quando aplicada por órgão do Poder Executivo, será de competência exclusiva de Ministro de Estado, Secretário Estadual ou Municipal, ou da autoridade máxima da autarquia ou fundação responsável;

9.4.4.4.2. Quando aplicada por órgãos dos Poderes Legislativo e Judiciário, Ministério Público ou Defensoria Pública, será de competência exclusiva de autoridade equivalente às referidas no item 9.4.4.4.1, conforme regulamento.

9.4.4.5. As sanções previstas nos itens 9.4.4.2.1., 9.4.4.2.3. e 9.4.4.2.4. poderão ser aplicadas cumulativamente com a prevista no item 9.4.4.2.2.

9.4.4.6. Se o valor das multas e indenizações exceder eventuais créditos da CONTRATADA junto à Administração, a diferença será descontada da garantia prestada ou cobrada judicialmente.

9.4.4.7. A aplicação das sanções previstas nos itens 9.4.4.2.1., 9.4.4.2.2., 9.4.4.2.3. e 9.4.4.2.4. não exclui a obrigação de reparação integral dos danos causados à Administração.

9.4.4.8. A defesa quanto à aplicação das sanções previstas no item 9.4.4.2.2., poderá ser apresentada no prazo de 15 dias úteis a contar da intimação.

9.4.4.9. Para a aplicação das sanções previstas nos itens 9.4.4.2.3. e 9.4.4.2.4. será instaurado processo de responsabilização conduzido por comissão composta por, no mínimo, dois servidores estáveis, garantindo-se o direito à defesa no prazo de 15 dias úteis, nos termos do art. 158 da Lei nº 14.133/2021.

9.5. **Liquidação**

9.5.1. O faturamento mensal terá início somente após a emissão do Termo de Recebimento Definitivo, não sendo contada a fase de implantação do Item.

9.5.2. Para o serviço de Link de Internet nas localidades praças será permitido o faturamento após o Termo de Recebimento Definitivo de cada uma das unidades.

9.5.3. Durante a fase de prestação mensal a CONTRATANTE deverá validar minuciosamente as planilhas de memória de cálculo fornecidas pela CONTRATADA a fim de apurar os valores a serem faturados e os descontos aplicados, às planilhas de memória de cálculo deverão ser enviadas até o quinto dia após o fechamento do período de apuração.

9.5.4. CONTRATADA poderá optar por emitir a nota fiscal/fatura após a validação da memória de cálculo pela CONTRATANTE que terá prazo de 5 dias úteis para validação.

9.5.5. A CONTRATADA poderá emitir a nota fiscal/fatura com descontos apurados pela CONTRATADA e em caso de discordância dos descontos apurados por parte da CONTRATANTE, os descontos poderão ser aplicados na fatura do mês posterior.

9.5.6. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de 5 dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 6º, §1º do Decreto nº089/2024 .

9.5.6.1. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

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

a) o prazo de validade;

b) a data da emissão;

c) os dados do contrato e do órgão contratante;

d) o período respectivo de execução do contrato;

e) os descontos com mês referência;

f) o valor a pagar;

g) dados bancários para o recebimento do montante; e

h) eventual destaque do valor de retenções tributárias cabíveis.

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

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

9.5.10. A Administração deverá realizar consulta ao SICAF para:

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

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

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

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

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

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

9.6. **Prazo de pagamento**

9.6.1. O pagamento será efetuado no prazo de até 15 (quinze) dias úteis contados da finalização da liquidação da despesa, nos termos do art. 6º, §1º do Decreto nº089/2024.

9.7. **Forma de pagamento**

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

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

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

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

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

10. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

10.1. **Forma de seleção e critério de julgamento da proposta**

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

10.1.2. A presente aquisição adotará como regime de execução por preço unitário, a ser contratado mediante licitação, na modalidade Pregão Eletrônico, com lances abertos com intervalos mínimos entre lances de R$ 0,01(um centavo) com valor de referência sigilos, levando em conta o objetivo da promoção de uma maior disputa entre os licitantes, com resultados satisfatórios para as empresas e o órgão público, considerando que o valor ultimado pelo mercado é variável, já que o referido objeto depende de tecnologias cada vez mais avançadas.

10.2. **Exigências de habilitação**

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

10.2.1.1.Habilitação jurídica

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

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

10.2.1.1.3. **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;

10.2.1.1.4. **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;

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

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

10.2.1.1.7. **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

10.2.1.1.8. **Sociedade cooperativa:** ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

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

10.2.1.2.Habilitação fiscal, social e trabalhista

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

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

do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

10.2.1.2.3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS); 10.2.1.2.4. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a

apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

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

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

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

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

10.2.1.3. Qualificação Econômico-Financeira

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

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

10.2.1.3.3. Índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), comprovados mediante a apresentação pelo licitante de balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais e obtidos pela aplicação das seguintes fórmulas:

I) Liquidez Geral (LG) = (Ativo Circulante + Realizável a Longo Prazo) / (Passivo Circulante + Passivo Não Circulante);
II) Solvência Geral (SG)= (Ativo Total) / (Passivo Circulante +Passivo não Circulante); e
III) Liquidez Corrente (LC) = (Ativo Circulante) / (Passivo Circulante).

10.2.1.3.4. 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

OU [patrimônio líquido mínimo] de 5% do valor total estimado do item.

10.2.1.4. Qualificação Econômico-Financeira. (Justificativa)

10.2.1.4.1. Ressalta-se que as exigências de habilitação relativas à qualificação econômico- financeira acima previstas e de acordo com o artigo 69 da Lei nº 14.133/21, têm a finalidade de viabilizar a aferição da situação financeira dos licitantes pela Administração. Dessa forma, será possível verificar se o interessado reúne condições indispensáveis para suportar as despesas relativas à satisfatória execução do objeto contratual, como dado objetivo de comprovação da qualificação econômico-financeira dos licitantes e para efeito de garantia ao adimplemento do contrato a ser ulteriormente celebrado, visando assegurar que a empresa contratada possa cumprir suas obrigações de curto e longo prazo, cumprindo as obrigações previstas no Edital e contrato, por se tratar de registro de preço o índice de 5% do valor de cada item, a Administração escolheu este valor por entender ser o mínimo a exigir de uma empresa para se manter um contrato, dentro de um nível de segurança e equilíbrio. Ademais, com o objetivo de não restringir o universo de concorrentes, resolveu não exigir valor acima da unidade. Ante o exposto, a exigência do Edital nada mais fez que traduzir em critérios objetivos o disposto no art. 37, XXI, da Constituição Federal, ademais, os índices escolhidos foram democráticos, na medida em que estabelecem um "mínimo" de segurança na contratação. Desta forma, atende plenamente a Lei Federal nº 14.133/21 limitando-se a exigir índices que demonstrem a capacidade financeira dos licitantes com vistas ao compromisso a ser assumido para plena execução do contrato.

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

10.2.1.4.3. O balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos. (Lei nº 14.133, de 2021, art. 69, §6º)

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

10.2.1.5. **Qualificação Técnica**

10.2.1.5.1. Apresentação de no mínimo 3 (três) Atestados de Capacidade Técnica, em nome da licitante, emitido por pessoa jurídica de direito público ou privado que comprove a realização de fornecimento e instalação de equipamentos similares aos ofertados, bem como serviços de instalação, configuração e suporte técnico.

10.2.1.5.2. Os atestados devem especificar explicitamente a marca, os modelos e as quantidades fornecidas, comprovando a experiência da licitante em projetos de porte e natureza semelhantes.

10.2.1.5.3. A licitante deve comprovar que dispõe de, no mínimo, dois (02) técnicos certificados pelo fabricante da solução proposta, os quais participarão diretamente da execução dos serviços previstos.

10.2.1.5.4. As certificações devem ser reconhecidas pelo fabricante e estar atualizadas, garantindo conhecimento técnico adequado às demandas do projeto.

10.2.1.5.5. O fornecedor deve fornecer todas as informações e documentos necessários para validar a legitimidade dos atestados apresentados, incluindo:

- Cópia do contrato que deu origem à prestação dos serviços mencionados nos atestados;
- Endereço atual da contratante que emitiu o atestado;
- Local onde os serviços foram executados;
- Outros documentos complementares, se solicitados pela Administração.

10.2.1.5.6. A licitante deve comprovar experiência em projetos de complexidade e escopo semelhantes, preferencialmente na área pública ou em ambientes corporativos de grande porte, apresentando histórico de projetos realizados com soluções NGFW, SD-WAN e links de redundância.

10.2.1.5.7. A licitante deverá demonstrar a capacidade técnica necessária para atender aos requisitos específicos do projeto, incluindo:

- Disponibilidade de suporte técnico especializado durante todo o período contratual;
- Experiência em integrar soluções de segurança em redes heterogêneas e complexas;
- Conhecimento comprovado em tecnologias de alta disponibilidade, criptografia e gestão de redes com políticas de segurança.

10.2.1.5.8. Sempre que solicitado pela Administração, a licitante deverá apresentar documentação adicional que comprove a qualificação técnica e a capacidade operacional para executar o objeto contratado, garantindo transparência e segurança no processo de contratação.

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

11.1. O custo estimado da contratação possui caráter sigiloso e será tornado público apenas e imediatamente após o julgamento das propostas nos termos do Art. 9º do Decreto municipal 240/23.

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

12. DA PARTICIPAÇÃO DE CONSORCIO

12.1. Trata-se da vedação da participação de consórcios quanto ao registro de preços para CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA PRESTAÇÃO DE SERVIÇOS DE SEGURANÇA CIBERNÉTICA COM INTELIGÊNCIA ARTIFICIAL PREDITIVA, FORNECIMENTO, EM REGIME DE COMODATO, INSTALAÇÃO E CONFIGURAÇÃO DE NEXT GENERATION FIREWALL (NGFW) E SD-WAN, REDUNDÂNCIA COMPOSTA POR LINKS PRIMÁRIO E SECUNDÁRIO DE ASN E ROTAS DIFERENTES, MANUTENÇÃO CONTÍNUA, SUPORTE TÉCNICO, SOFTWARE DE GERENCIAMENTO, CONECTIVIDADE SEGURA PARA UNIDADES EXTERNAS E PRAÇAS PÚBLICAS, CAPACITAÇÃO CERTIFICADA DA EQUIPE E ATENDIMENTO TÉCNICO ESPECIALIZADO, GARANTINDO ALTA DISPONIBILIDADE, SEGURANÇA, EFICIÊNCIA E SUSTENTABILIDADE NO ATENDIMENTO ÀS DEMANDAS DO MUNICÍPIO DE CÁCERES.

12.2. Art. 14 da Lei 14.133/21, conferiu a discricionaridade à Administração para permitir ou vetar a formação de consórcio em certame licitatório. É sabido que, em regra, a formação de consórcio é admitida quando o objeto a ser licitado envolve questões de alta complexidade técnica ou de relevante vulto, em que, isoladamente, as empresas não teriam condições de suprir os requisitos de habilitação do edital.

12.3. Tratando-se do objeto em questão, a ausência de consórcio não trará prejuízos à competitividade do certame por se tratar de um registro de preços por item, de serviços comuns, a ser executado ao longo de 12 (doze) meses em sua totalidade ou não, que não demandam especialidades diferentes entre as empresas, as quais poderiam impedir à execução dos serviços por uma única empresa. É nítido, neste caso também que, a reunião de empesas em consórcio, ao invés de estabelecer uma disputa entre as empresas, as mesmas formalizariam acordo para eliminar a competição caso estivessem reunidas em consórcio.

12.4. Diante de todo o exposto e, considerando que existem diversas empresas com capacidade para fornecer os serviços a serem contratados facilmente comprovados através do número de cotações inseridas no processo, fica vedada à participação de consórcios na licitação.

13. ADESÃO A ATA DE REGISTRO DE PREÇO

13.1. Em conformidade com a Lei nº 14.133/2021, a Lei nº 14.770/2023 e demais regulamentos aplicáveis, a adesão à Ata de Registro de Preços (ARP) configura-se como mecanismo de cooperação interfederativa, baseado na manifestação de interesse mútuo entre os entes públicos. Tal procedimento visa proporcionar maior eficiência administrativa e econômica, especialmente diante das dificuldades enfrentadas por órgãos e entidades para realizar processos licitatórios frequentes, seja por limitações de pessoal, infraestrutura ou outras razões justificáveis.

13.2. A adesão à ARP pelos demais entes federados será viabilizada desde que respeitados os limites quantitativos previstos no instrumento convocatório e nas legislações mencionadas, bem como observadas as condições estabelecidas neste Termo de Referência. A formalização da adesão deverá ocorrer mediante solicitação formal do ente interessado, acompanhada da anuência do órgão gerenciador e da CONTRATADA, conforme exigido pela legislação vigente.

rio - 029/2025 | [illegible] (226/256) [illegible]

13.3. A adesão não poderá resultar em prejuízo ao fornecimento ou à prestação dos serviços destinados ao órgão gerenciador e demais participantes da ARP. Caso o volume decorrente das adesões comprometa o atendimento das quantidades inicialmente previstas, a CONTRATADA deverá priorizar o fornecimento ao órgão gerenciador e aos participantes originais, conforme os prazos e condições estabelecidos neste instrumento.

13.4. Os entes federados que aderirem à ARP assumem integral responsabilidade pela gestão e fiscalização dos contratos celebrados diretamente com a CONTRATADA, sem qualquer interferência ou solidariedade do órgão gerenciador. Caberá ao ente aderente zelar pelo cumprimento das obrigações pactuadas, inclusive no que se refere às condições de pagamento, prazos de entrega e demais cláusulas contratuais.

13.5. O órgão gerenciador poderá, a qualquer tempo, solicitar relatórios à CONTRATADA para acompanhar as adesões realizadas, garantindo o cumprimento dos limites quantitativos e demais disposições legais aplicáveis. Eventuais irregularidades deverão ser comunicadas ao órgão gerenciador, que adotará as providências cabíveis em conformidade com a legislação vigente.

14. ADEQUAÇÃO ORÇAMENTÁRIA

14.1. As despesas oriundas da presente aquisição correrão por conta de todas as dotações vigentes, conforme especificado pelas Secretarias no momento do empenho.

ÓRGÃO/ UNIDADE	FUNCIONAL-PROGRAMÁTICA	NATUREZA DA DESPESA	FONTE DE RECURSOS	SECRETARIA
021301	04.129.1002.2109	3.3.90.	1.1.500	SMFAZ
021201	27.122.1009.2107	3.3.90.	1.1.500	SMFAZ
020501	10.122.1003.2021	33.90.	1.1.500	SMS
020502	10.304.1003.2030	33.90.	1.600	SMS
020901	04.121.1002.2071	3.3.90.	1.1.500	SMPLAN
020901	04.127.1002.2071	3.3.90.	1.1.500	SMPLAN
021101	08.122.1008.2074	3.3.90.	1.1.500	SMAS
021102	08.244.1008.2082	3.3.90.	4.1.660	SMAS
021102	08.244.1008.2083	3.3.90.	1.1.500	SMAS
021102	08.244.1008.2083	3.3.90.	4.1.660	SMAS
021102	08.244.1008.2086	3.3.90.	4.1.660	SMAS
021102	08.244.1008.2091	3.3.90.	1.1.500	SMAS
020601	12.122.1004.2046	3.3.90.	2.1.500	SME
020401	04.123.1002.2019	3.3.90.	1.1.500	SMFIN
020701	15.122.1005.2061	3.3.90.	1.1.500	SMIL

rio - 029/2025 [illegible]

021401	18.122.1010.2111	3.3.90.	1.1.500	SMMADE
021001	20.122.1007.2072	3.3.90.	1.1.500	SMAGRI
020101	04.122.1002.2004	3.3.90.	1.1.500	GABINETE
020201	04.122.1002.2012	3.3.90.	1.1.500	SMEAE
020801	04.122.1006.2066	3.3.90.	1.1.500	SMTC
	27.122.1009.2.107	3.3.90.	1.1.500	SMEL
020201	04 126 1002 2014 0000	3.3.90	1.1.500	SMEAE
020201	04 122 1002 2012 0000	3.3.90	1.1.500	SMEAE
020301	04 122 1002 2018 0000	3.3.90	1.1.500	SMA

Cáceres-MT, 25 de fevereiro 2025.

GIRLANE VIEIRA PEREIRA
Coordenadora de Informações Sistêmicas e Tecnologia de Informação

JEREMIAS PEREIRA LEITE
Secretário Municipal Especial de Assuntos Estratégicos

CONTRATADA
Empresa: CNPJ:
Representante: CPF:
RG:

ANEXO II – TERMO DA ATA DE REGISTRO DE PREÇO

O (A). PREFEITURA MUNICIPAL DE CÁCERES, com sede no(a) na Av. Brasil,119,COC, Bairro Jardim Celeste, na cidade de Cáceres-MT, inscrito(a) no CNPJ/MF sob o nº 03214145/0001-83, neste ato representado(a) pelo(a) ...... (cargo e nome), nomeado(a) pela Portaria nº ...... de ..... de ...... de 200..., publicada no .... de ..... de .... de , portador

da matrícula funcional nº ...., considerando o julgamento da licitação na modalidade de pregão, na forma eletrônica, para REGISTRO DE PREÇOS nº ..../2024..., publicada no ...... de ...../...../200. , processo administrativo

n.º ...., RESOLVE registrar os preços da(s) empresa(s) indicada(s) e qualificada(s) nesta ATA, de acordo com a classificação por ela(s) alcançada(s) e na(s) quantidade(s) cotada(s), atendendo as condições previstas no edital, sujeitando-se as partes às normas constantes na Lei nº 14.133, de 1º de abril de 2021.

1. DO OBJETO

1.1. Registro de Preço para futura e eventual contratação de empresa especializada para prestação de serviços de segurança cibernética com Inteligência Artificial Preditiva, fornecimento, em regime de comodato, instalação e configuração de Next Generation Firewall (NGFW) e SD-WAN, redundância composta por links primário e secundário de ASN e rotas diferentes, manutenção contínua, suporte técnico, software de gerenciamento, conectividade segura para unidades externas e praças públicas, capacitação certificada da equipe e atendimento técnico especializado, garantindo alta disponibilidade, segurança, eficiência e sustentabilidade no atendimento às demandas do Município de Cáceres, conforme condições e exigências estabelecidas neste instrumento

2. DOS PREÇOS, ESPECIFICAÇÕES E QUANTITATIVOS.

2.1. O preço registrado, as especificações do objeto, a quantidade, fornecedor (es) e as demais condições ofertadas na(s) proposta(s) são as que seguem:

ITEM	Fornecedor *(razão social, CNPJ/MF, endereço, contatos, representante)*						
X	Especificação	*Marca (se exigida no edital)*	*Modelo (se exigido no edital)*	Unidade	Quantidade Máxima	Quantidade Mínima	Valor Un
1	Serviço de provimento de solução de Firewall de Nova Geração e SD- WAN (Alta Disponibilidade						

	)						
2	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva						
3	Serviço de Link dedicado de Acesso à internet, bloco /29 e Banda Mínima de Acesso						

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/D822-BE8B-F69C-28C2 e informe o código D822-BE8B-F69C-28C2

	Garantida de 500Mbps (Alta Disponibilidade) SEDE (Link de ASN e Rota Diferentes)						
4	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 150Mbps Sites Remotos (Fibra Óptica)						
5	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G)						
6	Implantação da Solução						

rio - 029/2025 | [illegible] (229/256) [illegible]

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE

7	Capacitação especializada da equipe com emissão de certificação.						
8	Consultoria Política de Segurança						

3. DA ADESÃO À ATA DE REGISTRO DE PREÇOS

3.1. Será admitida a adesão à ata de registro de preços decorrente desta licitação , conforme lei 14.133/2021.

4. VALIDADE DA ATA , FORMALIZAÇÃO DA ATA DE REGISTRO DE PREÇOS E CADASTRO RESERVA

4.1 A validade da Ata de Registro de Preços será de 1 (um) ano, contado a partir do primeiro dia útil subsequente à data de divulgação da ata do registro de preço, podendo ser prorrogada por igual período, mediante a anuência do fornecedor, desde que comprovado o preço vantajoso.

4.1.1. O contrato decorrente da ata de registro de preços terá sua vigência estabelecida no próprio instrumento contratual e observará 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.

4.1.2. Na formalização do contrato ou do instrumento substituto deverá haver a indicação da disponibilidade dos créditos orçamentários respectivos.

4.2 A contratação com os fornecedores registrados na ata será formalizada pelo órgão ou pela entidade interessada por intermédio de instrumento contratual, emissão de nota de empenho de despesa, autorização de compra ou outro instrumento hábil, conforme o art. 95 da Lei nº 14.133, de 2021.

4.2.1. O instrumento contratual de que trata deste processo. deverá ser assinado no prazo de validade da ata de registro de preços.

4.3 Os contratos decorrentes do sistema de registro de preços poderão ser alterados, observado o art. 124 da Lei nº 14.133, de 2021.

4.4 Após a homologação da licitação ou da contratação direta, deverão ser observadas as seguintes condições para formalização da ata de registro de preços:

4.4.1 Serão registrados na ata os preços e os quantitativos do adjudicatário.

4.4.2 Será incluído na ata, na forma de anexo, o registro dos licitantes ou dos fornecedores que:

4.4.2.1 Aceitarem cotar os bens, as obras ou os serviços com preços iguais aos do adjudicatário, observada a classificação da licitação; e

4.4.2.2 Mantiverem sua proposta original.

4.4.3 Será respeitada, nas contratações, a ordem de classificação dos licitantes ou dos fornecedores registrados na ata.

4.5 O registro a que se refere a este termo tem por objetivo a formação de cadastro de reserva para o caso de impossibilidade de atendimento pelo signatário da ata.

4.6 Para fins da ordem de classificação, os licitantes ou fornecedores que aceitarem reduzir suas propostas para o preço do adjudicatário antecederão aqueles que mantiverem sua proposta original.

4.7 A habilitação dos licitantes que comporão o cadastro de reserva a que se refere a este processo somente será efetuada quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:

4.7.1 Quando o licitante vencedor não assinar a ata de registro de preços, no prazo e nas condições estabelecidos *no edital.*

4.7.2 Quando houver o cancelamento do registro do licitante ou do registro de preços nas hipóteses previstas no edital.

4.8 O preço registrado com indicação dos licitantes e fornecedores será divulgado a ata de registro de preços e ficará disponibilizado durante a vigência da ata de registro de preços.

4.9 Após a homologação da licitação ou da contratação direta, o licitante mais bem classificado ou o fornecedor, no caso da contratação direta, será convocado para assinar a ata de registro de preços, no prazo e nas condições estabelecidos no edital de licitação ou no aviso de contratação direta, sob pena de decair o direito, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021.

4.9.1. O prazo de convocação poderá ser prorrogado 1 (uma) vez, por igual período, mediante solicitação do licitante ou fornecedor convocado, desde que apresentada dentro do prazo, devidamente justificada, e que a justificativa seja aceita pela Administração.

4.10 A ata de registro de preços será assinada por meio de assinatura digital e disponibilizada no Sistema de Registro de Preços.

4.11 Quando o convocado não assinar a ata de registro de preços no prazo e nas condições estabelecidos no edital ou no aviso de contratação, e observado o disposto no edital, observando o edital e seu anexo subitens, fica facultado à Administração convocar os licitantes remanescentes do cadastro de reserva, na ordem de classificação, para fazê-lo em igual prazo e nas condições propostas pelo primeiro classificado.

4.12 Na hipótese de nenhum dos licitantes que trata a ata de registro de preço, aceitar a contratação nos termos do item anterior, a Administração, observados o valor estimado e sua eventual atualização nos termos *do edital*, poderá:

4.12.1 Convocar para negociação os demais licitantes ou fornecedores remanescentes cujos preços foram registrados sem redução, observada a ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário; ou

4.12.2 Adjudicar e firmar o contrato nas condições ofertadas pelos licitantes ou fornecedores remanescentes, atendida a ordem classificatória, quando frustrada a negociação de melhor condição.

4.13. A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente justificada

5. ALTERAÇÃO OU ATUALIZAÇÃO DOS PREÇOS REGISTRADOS

5.1 Os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, nas seguintes situações:

5.2 Em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução de ata tal como pactuada, mediante pedido formal do interessado, nos termos da alínea “d” do inciso II do caput do art. 124 da lei n.º 14.133, de 2021”, quando o ônus de prova incumbe ao contratante via requerimento fundamentado, que será analisado, se possível, em até 30 dias pela Administração Municipal.

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

5.2.2. Na hipótese de previsão no edital de cláusula de reajustamento ou repactuação sobre os preços registrados, nos termos da Lei nº 14.133, de 2021.

5.2.2.1. No caso do reajustamento, deverá ser respeitada a contagem da anualidade e
. o índice previstos para a contratação;

5.2.2.2. No caso da repactuação, poderá ser a pedido do interessado, conforme critérios definidos para a contratação.

5.2.2.3. No caso da repactuação, poderá ser a pedido do interessado, conforme critérios definidos para a contratação.

5.3. O requerimento de reequilíbrio da equação econômico-financeira deverá demonstrar o desequilíbrio havido minuciosamente por meio de memória de cálculo e a modificação dos encargos ser proporcional ao mesmo, e ser documentalmente comprovada.

6. NEGOCIAÇÃO DE PREÇOS REGISTRADOS

6.1. Na hipótese de o preço registrado tornar-se superior ao preço praticado no mercado por motivo superveniente, o órgão ou entidade gerenciadora convocará o fornecedor para negociar a redução do preço registrado.

6.1.1 Caso não aceite reduzir seu preço aos valores praticados pelo mercado, o fornecedor será liberado do compromisso assumido quanto ao item registrado, sem aplicação de penalidades administrativas.

6.2. Na hipótese prevista no item anterior, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam reduzir seus preços aos valores de mercado e não convocará os licitantes ou fornecedores que tiverem seu registro cancelado.

6.2.1 Se não obtiver êxito nas negociações, o órgão ou entidade gerenciadora procederá ao cancelamento da ata de registro de preços, adotando as medidas cabíveis para obtenção de contratação mais vantajosa.

6.2.2 Na hipótese de redução do preço registrado, o gerenciador comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços para que avaliem a conveniência e a oportunidade de diligenciarem negociação com vistas à alteração contratual, observado o disposto no art. 124 da Lei nº 14.133, de 2021.

6.3 Na hipótese de o preço de mercado tornar-se superior ao preço registrado e o fornecedor não poder cumprir as obrigações estabelecidas na ata, será facultado ao fornecedor requerer ao gerenciador a alteração do preço registrado, mediante comprovação de fato superveniente que supostamente o impossibilite de cumprir o compromisso.

6.3.1 Neste caso, o fornecedor encaminhará, juntamente com o pedido de alteração, a documentação comprobatória ou à planilha de custos que demonstre a inviabilidade do preço registrado em relação às condições inicialmente pactuadas.

6.3.2 Não hipótese de não comprovação da existência de fato superveniente que inviabilize o preço registrado, o pedido será indeferido pelo órgão ou entidade gerenciadora e o fornecedor deverá cumprir as obrigações estabelecidas na ata, sob pena de cancelamento do seu registro, nos termos do edital, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021, e na legislação aplicável.

6.3.3 Na hipótese de cancelamento do registro do fornecedor, nos termos do item anterior, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam manter seus preços registrados, observado o disposto no edital.

6.3.4 Se não obtiver êxito nas negociações, o órgão ou entidade gerenciadora procederá ao cancelamento da ata de registro de preços, nos termos do edital, e adotará as medidas cabíveis para a obtenção da contratação mais vantajosa.

6.3.5 Na hipótese de comprovação da majoração do preço de mercado que inviabilize o preço registrado, conforme previsto no edital, o órgão ou entidade gerenciadora atualizará o preço registrado, de acordo com a realidade dos valores praticados pelo mercado.

6.3.6 O órgão ou entidade gerenciadora comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços sobre a efetiva alteração do preço registrado, para que avaliem a necessidade de alteração contratual, observado o disposto no art. 124 da Lei nº 14.133, de 2021.

7. REVISÃO E CANCELAMENTO.

7.1. O registro do fornecedor será cancelado pelo gerenciador, quando o fornecedor:

7.1.1. Descumprir as condições da ata de registro de preços, sem motivo justificado;

7.1.2. Não retirar a nota de empenho, ou instrumento equivalente, no prazo estabelecido pela Administração sem justificativa razoável;

7.1.3. Não aceitar manter seu preço registrado, na hipótese prevista no edital.

7.1.4. Sofrer sanção prevista nos incisos III ou IV do caput do art. 156 da Lei nº 14.133, de 2021. Na hipótese de aplicação de sanção prevista nos incisos III ou IV do caput do art. 156 da Lei nº 14.133, de 2021, caso a penalidade aplicada ao fornecedor não ultrapasse prazo de vigência da ata de registro de preços, poderá o órgão ou a entidade gerenciadora poderá, mediante decisão fundamentada, decidir pela manutenção do registro de preços, vedadas contratações derivadas da ata enquanto perdurarem os efeitos da sanção.

7.2. O cancelamento de registros nas hipóteses previstas deste instrumento será formalizado por despacho do órgão ou da entidade gerenciadora, garantidos os princípios do contraditório e da ampla defesa.

7.3. Na hipótese de cancelamento do registro do fornecedor, o órgão ou a entidade gerenciadora poderá convocar os licitantes que compõem o cadastro de reserva, observada a ordem de classificação.

7.4. O cancelamento dos preços registrados poderá ser realizado pelo gerenciador, em determinada ata de registro de preços, total ou parcialmente, nas seguintes hipóteses, desde que devidamente comprovadas e justificadas:

7.4.1. Por razão de interesse público;

7.4.2. A pedido do fornecedor, decorrente de caso fortuito ou força maior; ou

7.4.3. Se não houver êxito nas negociações, nas hipóteses em que o preço de mercado se tornar superior ou inferior ao preço registrado.

8. DAS PENALIDADES

8.1. O descumprimento da Ata de Registro de Preços ensejará aplicação das penalidades estabelecidas *no edital.*

8.2. As sanções também se aplicam aos integrantes do cadastro de reserva no registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente após terem assinado a ata.

9. CONDIÇÕES GERAIS

9.1. As condições gerais de execução do objeto, tais como os prazos para entrega e recebimento, as obrigações da Administração e do fornecedor registrado, penalidades e demais condições do ajuste, encontram-se definidos no Termo de Referência, ANEXO *AO EDITAL.*

9.2. Para firmeza e validade do pactuado, a presente Ata foi lavrada em 2 (duas) vias de igual teor, que, depois de lida e achada em ordem, vai assinada pelas partes.

Cáceres - MT, de__________2025. CONTRATANTE:

____

MUNICIPIO DE CÁCERES – MT

Secretário Municipal Especial de Assuntos Estratégicos.
CONTRATADA

Empresa: CNPJ:
Represente: CPF: RG:

rio - 029/2025

ANEXO III - TERMO DE CONTRATO

TERMO DE CONTRATO DE COMPRA Nº ..../...., QUE FAZEM ENTRE SI O(A)... E A EMPRESA ....

A Prefeitura Municipal de Cáceres, por intermédio do(a).....................................(órgão) contratante), com sede no(a) ...., na cidade de .... /Estado ..., inscrito(a) no CNPJ sob o nº ...., neste ato representado(a) pelo(a)..........................(cargo e nome), nomeado(a) pela Portaria nº ......, de ..... de .... de 20..., publicada no DOU de ..... de .... de ...., portador da matrícula funcional nº ....,., doravante denominada CONTRATANTE, e o(a) .... inscrito(a) no CNPJ/MF sob o nº ...., sediado(a) na ...., em .... doravante designada CONTRATADA, neste ato representada pelo(a) Sr.(a) ...., portador(a) da Carteira de Identidade nº ...., expedida pela (o) ...., e CPF nº ...., tendo em vista o que consta no Processo nº .... e em observância às disposições da LEI 14.133/2021.

1. CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto do presente instrumento é a contratação de empresa especializada para prestação de serviços de segurança cibernética com Inteligência Artificial Preditiva, fornecimento, em regime de comodato, instalação e configuração de Next Generation Firewall (NGFW) e SD-WAN, redundância composta por links primário e secundário de ASN e rotas diferentes, manutenção contínua, suporte técnico, software de gerenciamento, conectividade segura para unidades externas e praças públicas, capacitação certificada da equipe e atendimento técnico especializado, garantindo alta disponibilidade, segurança, eficiência e sustentabilidade no atendimento às demandas do Município de Cáceres, conforme as condições estabelecidas no Termo de Referência.

1.2. Objeto da contratação:

ITEM	CÓDIGO TCE- MT	CÓDIGO CATMAT	ESPECIFICAÇÃO	UNIDADE	QUANTIDADE	QUANTIDADE ANUAL

1	257560-4	609340	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)	Serviço	173	2076
2	152969	481647	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	Serviço	2	24
3	00065206	26174	Serviço de Link dedicado de Acesso à internet, bloco /29 e Banda Mínima de Acesso Garantida de 500Mbps (Alta Disponibilidade) SEDE (Link de ASN e Rota Diferentes)	Serviço	2	24
4	152970	26484	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 150Mbps Sites	Serviço	171	2052
			Remotos (Fibra Óptica)			
5	152972	26557	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida	Serviço	171	2052

[illegible]

			de 35Mbps Sites Remotos (Fibra Óptica e 4/5G)			
6	339905-2	1988	Implantação da Solução	Serviço	1	1
7	404876-8	16837	Capacitação especializada da equipe com emissão de certificação.	Treinamento	1	1
8	332679-9	27340	Consultoria Política de Segurança	Serviço	1	1

1.3. Vinculam esta contratação, independentemente de transcrição:

1.3.1. O Termo de Referência;

1.3.2. O Edital da Licitação;

1.3.3. A Proposta do contratado;

1.3.4. Eventuais anexos dos documentos supracitados.

1.4. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

1.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

1.6. 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.

1.7. 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.

1.8. O reajuste será realizado por apostilamento.

1.9. o prazo para resposta ao pedido de repactuação de preços será preferencialmente de 1 (um) mês, contado da data do fornecimento da documentação prevista no § 6º do art.

2. CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1. O prazo de vigência da contratação é de 12 (doze) meses contados do(a), prorrogável sucessivamente, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

2.2. A prorrogação de que trata este item é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o contratado, atentando, ainda, para o cumprimento dos seguintes requisitos:

a) Estar formalmente demonstrado no processo que a forma de prestação dos serviços tem natureza continuada;

b) Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;

c) Seja juntada justificativa e motivo, por escrito, de que a Administração mantém interesse na realização do serviço;

d) Haja manifestação expressa do contratado informando o interesse na prorrogação;

e) Seja comprovado que o contratado mantém as condições iniciais de habilitação.

2.3. O contratado não tem direito subjetivo à prorrogação contratual.

2.4. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

2.5. Nas eventuais prorrogações contratuais, os custos não renováveis já pagos ou amortizados ao longo do primeiro período de vigência da contratação deverão ser reduzidos ou eliminados como condição para a renovação.

2.6. O contrato não poderá ser prorrogado quando o contratado tiver sido penalizado nas sanções de declaração de inidoneidade ou impedimento de licitar e contratar com poder público, observadas as abrangências de aplicação.

3. CLÁUSULA QUARTA – DOTAÇÃO ORÇAMENTÁRIA

3.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União deste exercício, na dotação abaixo discriminada:

Gestão/Unidade:
Fonte de Recursos:
Programa de Trabalho:
Elemento de Despesa:
Plano Interno:
Nota de Empenho

3.2. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

4. CLÁUSULA QUINTA – PAGAMENTO

4.1. O prazo para pagamento e demais condições a ele referentes encontram-se no Termo de Referência.

> V - O preço e as condições de pagamento, os critérios, a data-base e a periodicidade do reajustamento de preços e os critérios de atualização monetária entre a data do adimplemento das obrigações e a do efetivo pagamento;
>
> VI - os critérios e a periodicidade da medição, quando for o caso, e o prazo para liquidação e para pagamento; VII - os prazos de início das etapas de execução, conclusão, entrega, observação e recebimento definitivo, quando for o caso; da prestação do serviço aos ditames da Lei Federal nº 8.078/1990.

5. CLÁUSULA SEXTA – REAJUSTE

5.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do Orçamento.

5.2. Após o interregno de um ano do orçamento estimado, mediante pedido expresso do contratado, os preços iniciais serão reajustados pelo contratante, mediante a aplicação do índice IPCA ou outro que reflita a inflação e seja mais vantajoso à Administração Pública Municipal, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

5.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

5.4. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

5.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

5.6. 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.

5.7. 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.

5.8.O reajuste será realizado por apostilamento.

5.9. o prazo para resposta ao pedido de repactuação de preços será preferencialmente de 1 (um) mês, contado da data do fornecimento da documentação prevista no § 6º do art.

6. CLÁUSULA OITAVA - ENTREGA E RECEBIMENTO DO OBJETO

6.1. As condições de entrega e recebimento do objeto são aquelas previstas no Termo de Referência, anexo ao Edital.

7. CLAÚSULA NONA – FISCALIZAÇÃO

7.1. A fiscalização da execução do objeto será efetuada por Comissão/Representante designado pela CONTRATANTE, na forma estabelecida no Termo de Referência, anexo do Edital.

8. CLÁUSULA DÉCIMA – OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

8.1. As obrigações da CONTRATANTE e da CONTRATADA são aquelas previstas no Termo de Referência, anexo do Edital.

9. CLÁUSULA DÉCIMA PRIMEIRA – SANÇÕES ADMINISTRATIVAS

9.1. As sanções referentes à execução do contrato são aquelas previstas no Termo de Referência, anexo do Edital.

10. CLÁUSULA DÉCIMA SEGUNDA – RESCISÃO

10.1. O contrato será extinto quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes.

10.2. O contrato poderá ser extinto antes do prazo nele fixado, sem ônus para o contratante, quando este não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

10.3. A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja notificação do contratado pelo contratante nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia.

10.4. Caso a notificação da não-continuidade do contrato de que trata este subitem ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação.

10.5. O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no [artigo 137 da Lei nº 14.133/21](), bem como amigavelmente, assegurados o contraditório e a ampla defesa.

10.6. Nesta hipótese, aplicam-se também os [artigos 138 e 139]() da mesma Lei.

10.7. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a extinção se não restringir sua capacidade de concluir o contrato.

10.8. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

10.9. O termo de extinção, sempre que possível, será precedido:

10.9.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

10.9.2. Relação dos pagamentos já efetuados e ainda devidos;

10.9.3. Indenizações e multas.,

10.10. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório ([art. 131, *caput,*]() [da Lei n.º 14.133, de 2021).]()

10.11. O não pagamento dos salários e das verbas trabalhistas, e o não recolhimento das contribuições sociais, previdenciárias e para com o FGTS poderá dar ensejo à extinção do contrato por ato unilateral e escrito do contratante e à aplicação das penalidades cabíveis.

10.12. O contratante poderá conceder prazo para que o contratado regularize suas obrigações trabalhistas ou suas condições de habilitação, sob pena de extinção contratual, quando não identificar má-fé ou a incapacidade de correção.

10.13. Quando da extinção, o fiscal administrativo deverá verificar o pagamento pelo contratado das verbas rescisórias ou os documentos que comprovem que os empregados serão realocados em outra atividade de prestação de serviços, sem que ocorra a interrupção do contrato de trabalho.

10.14. Até que o contratado comprove o disposto no item anterior, o contratante reterá:

10.14.1. A garantia contratual - prestada com cobertura para os casos de descumprimento das obrigações de natureza trabalhista e previdenciária, incluídas as verbas rescisórias -, a qual será executada para reembolso dos prejuízos sofridos pela Administração, nos termos da legislação que rege a matéria (art. 121,

§ 3º, I, e art. 139, III, b, da Lei n.º 14.133/2021); e

10.14.2. Os valores das Notas fiscais ou Faturas correspondentes em valor proporcional ao inadimplemento, até que a situação seja regularizada.

10.15. Na hipótese do subitem anterior, não havendo quitação das obrigações por parte do contratado no prazo de 15 (quinze) dias, o contratante poderá efetuar o pagamento das obrigações diretamente aos empregados que tenham participado da execução dos serviços objeto do contrato, deduzindo o respectivo valor do pagamento devido ao contratado (art. 121, §3º, inciso II, da Lei nº 14.133/2021).

10.16. O contratante poderá ainda:

10.16.1. nos casos de obrigação de pagamento de multa pelo contratado, reter a garantia prestada a ser executada (art. 139, III, "c", da Lei n.º 14.133/2021), conforme legislação que rege a matéria; e

10.16.2. nos casos em que houver necessidade de ressarcimento de prejuízos causados à Administração, nos termos do inciso IV do art. 139 da Lei n.º 14.133, de 2021, reter os eventuais créditos existentes em favor do contratado decorrentes do contrato.

10.17. O contrato poderá ser extinto caso se constate que o contratado mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que tenha desempenhado função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau (art. 14, inciso IV, da Lei n.º 14.133, de 2021).

11. CLÁUSULA DÉCIMA TERCEIRA – VEDAÇÕES

11.1. É vedado à CONTRATADA:

11.1.1. caucionar ou utilizar este Termo de Contrato para qualquer operação financeira;

11.1.2. interromper a execução contratual sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

12. CLÁUSULA DÉCIMA QUARTA – ALTERAÇÕES

12.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

12.2. O contratado é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

12.3. As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da consultoria jurídica do contratante, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês (art. 132 da Lei nº 14.133, de 2021).

12.4. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

13. CLÁUSULA DÉCIMA QUINTA - DOS CASOS OMISSOS.

13.1. Os casos omissos serão decididos pelo contratante, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor

14. CLÁUSULA DÉCIMA SEXTA – PUBLICAÇÃO

14.1. Incumbirá ao contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, *caput*, da Lei n.º 14.133, de 2021, e ao art. 8º, §2º, da Lei n. 12.527, de 2011, c/c art. 7º, §3º, inciso V, do Decreto n. 7.724, de 2012.

15. CLÁUSULA DÉCIMA SÉTIMA – FORO

15.1. Fica eleito o Foro da Justiça Federal em ......, Seção Judiciária de ...... para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme art. 92, §1º, da Lei nº 14.133/21.

16. MATRIZ DE RISCO

16.1. Por se tratar de objeto rotineiro, sem aferição de riscos aparentes para a Administração Pública, dispensa a elaboração da matriz de risco.

...., ... de... de 20.....

____

Responsável legal da CONTRATANTE

____

Responsável legal da CONTRATADA TESTEMUNHAS:

1-

2-

rio - 029/2025 | [illegible] (242/256) [illegible]

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: D822-BE8B-F69C-28C2

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

✓ JEREMIAS PEREIRA LEITE (CPF 045.XXX.XXX-72) em 26/05/2025 15:41:44 GMT-04:00
Papel: Parte
Emitido por: AC SOLUTI Multipla v5 << AC SOLUTI v5 << Autoridade Certificadora Raiz Brasileira v5 (Assinatura ICP-Brasil)

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

https://caceres.1doc.com.br/verificacao/D822-BE8B-F69C-28C2

De: Igor O. - SMA-CPL

Para: SMEAE - Compras - Gerência de Compras

Data: 26/05/2025 às 16:25:41

Senhor Secretário,

Solicitamos assinatura no anexo autorização da despesa.

_

Igor de Souza Oliveira
Pregoeiro Oficial

Anexos:

Autorizacao_da_despesa.pdf

Assinado digitalmente (anexos) por:

Assinante	Data	Assinatura	
Jeremias Pereira Leite	26/05/2025 16:38:16	ICP-Brasil	JEREMIAS PEREIRA LEITE CPF 045.XXX.XXX-72

Para verificar as assinaturas, acesse **https://caceres.1doc.com.br/verificacao/** e informe o código: **0A87-5C62-E334-B6A9**

ESTADO DE MATO GROSSO
PREFEITURA MUNICIPAL DE CÁCERES
SECRETARIA MUNICIPAL DE AGRICULTURA

PROCESSO ADMINISTRATIVO	ANO
29	2025

ATO DE AUTORIZAÇÃO

AUTORIZO nos termos da Lei 14.133/2021 e demais normas pertinentes, a abertura de licitação na modalidade PREGÃO ELETRÔNICO 15/2025, COMPRAS.GOV.BR 90015/2025. Registro de Preço para futura e eventual contratação de empresa especializada para prestação de serviços de segurança cibernética com Inteligência Artificial Preditiva, garantindo alta disponibilidade, segurança, eficiência e sustentabilidade no atendimento às demandas do Município de Cáceres.

Fundamento: Art. 28, inciso I, da Lei 14.133/21, amparados nos princípios da finalidade pública e princípio da continuidade do serviço público.

JEREMIAS PEREIRA LEITE
Secretário Municipal Especial de Assuntos estratégicos

Prefeitura Municipal de Cáceres, 26 de maio de 2025.

Assinado por 1 pessoa: JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/0A87-5C62-E334-B6A9 e informe o código 0A87-5C62-E334-B6A9

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: 0A87-5C62-E334-B6A9

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

✓ JEREMIAS PEREIRA LEITE (CPF 045.XXX.XXX-72) em 26/05/2025 15:38:13 GMT-04:00
Papel: Parte
Emitido por: AC SOLUTI Multipla v5 << AC SOLUTI v5 << Autoridade Certificadora Raiz Brasileira v5 (Assinatura ICP-Brasil)

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

https://caceres.1doc.com.br/verificacao/0A87-5C62-E334-B6A9

De: Igor O. - SMA-CPL

Para: SMA-CPL - Comissão Permanente de Licitação

Data: 27/05/2025 às 09:03:38

Segue em anexo comprovante de publicação do PNCP

_

Igor de Souza Oliveira
Pregoeiro Oficial

Anexos:

Portal_Nacional_de_Contratacoes_Publicas.pdf

Edital nº 90015/2025

Acessar Contratação

Última atualização 27/05/2025

Local: Cáceres/MT **Órgão:** MUNICIPIO DE CACERES

Unidade compradora: 989047 - PREFEITURA MUNICIPAL DE CACERES - MT

Modalidade da contratação: Pregão - Eletrônico **Amparo legal:** Lei 14.133/2021, Art. 28, I **Tipo:** Edital

Modo de disputa: Aberto **Registro de preço:** Sim **Fonte orçamentária:** Não informada

Data de divulgação no PNCP: 27/05/2025 **Situação:** Divulgada no PNCP

Data de início de recebimento de propostas: 27/05/2025 08:00 (horário de Brasília)

Data fim de recebimento de propostas: 11/06/2025 09:00 (horário de Brasília)

Id contratação PNCP: 03214145000183-1-000024/2025 **Fonte:** Compras.gov.br

Objeto:

Registro de Preço para futura e eventual contratação de empresa especializada para prestação de serviços de segurança cibernética com Inteligência Artificial Preditiva, garantindo alta disponibilidade, segurança, eficiência e sustentabilidade no atendimento às demandas do Município de Cáceres.

Informação complementar:

Para as respostas de esclarecimentos e impugnações deste edital acesse o link: https://cnetmobile.estaleiro.serpro.gov.br/comprasnet-web/public/landing?destino=quadro-informativo&compra=98904705900152025

VALOR TOTAL ESTIMADO DA COMPRA

SIGILOSO

Itens Arquivos Histórico

Número	Descrição	Quantidade	Valor unitário estimado
1	Firewall	2076	Sigiloso
2	Equipamento Segurança Rede	24	Sigiloso
3	Acesso a internet - stfc (banda larga)	24	Sigiloso
4	Acesso a Internet Via Cabo	2052	Sigiloso
5	Acesso a Internet Via Satélite	2052	Sigiloso

Exibir: 5 ▾ 1-5 de 8 itens Página: 1 ▾ ‹ ›

‹ Voltar

De: Jeremias L. - SMEAE

Para: SMA-CPL - Comissão Permanente de Licitação

Data: 27/05/2025 às 10:50:34

Prezados,

Venho por meio deste devolver o processo devidamente assinado.

_

Jeremias Pereira Leite
Secretário Municipal Especial de Assuntos Estratégicos

De: William C. - SMA-CPL

Para: SMA-CPL - Comissão Permanente de Licitação

Data: 27/05/2025 às 16:43:26

Segue em anexo comprovante de publicação.

_

William Marcos Castro Caxito
Assistente administrativo

Membro da Equipe de Licitação

Portaria nº 251-09/04/2025

Anexos:

Diario_Oficial_de_Contas.pdf
Jornal_Estadao.pdf
Jornal_Oficial_Eletronico_dos_Municipios_do_Estado_de_Mato_Grosso.pdf

MINUTA DO EDITAL PREGÃO ELETRÔNICO N° 15/2025
(Processo Administrativo n° 29/2025)
Número da licitação no compras.gov.br 90015/2025

Torna-se público, para conhecimento dos interessados, que a PREFEITURA MUNICIPAL DE CÁCERES, por meio da SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO, sediada na AV. BRASIL, 119, COC, BAIRRO JARDIM CELESTE, realizará licitação, para registro de preços, na modalidade PREGÃO, na forma ELETRÔNICA, **com critério de julgamento menor preço global, modo de disputa aberto**, nos termo da lei n.º 14.133 de 2021 e demais legislação aplicável e de acordo com as condições estabelecidas neste Edital.

Data da sessão: XX de XXXX de XXXX
Horário: 09h00min horário de Brasília
Portal de Compras do Governo Federal: compras.gov.br
UASG: 989047

1. DO OBJETO

Registro de Preço para futura e eventual contratação de empresa especializada para prestação de serviços de segurança cibernética com Inteligência Artificial Preditiva, garantindo alta disponibilidade, segurança, eficiência e sustentabilidade no atendimento às demandas do Município de Cáceres, conforme condições e exigências estabelecidas neste instrumento.

1.2. A licitação será realizada por meio de um único lote, contendo diversos itens, conforme especificado no Termo de Referência. O licitante deverá apresentar uma proposta para todos os itens dentro do lote, sendo vedada a oferta parcial.

1.3. O critério de julgamento adotado será o menor valor global, observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto. **Havendo qualquer divergência entre a especificação do CATSER e a deste Edital, prevalecerá a especificação deste Edital.**

2. DOS REGISTROS DE PREÇOS.

2.1. As regras referentes aos órgãos gerenciador e participante, bem como a eventuais adesões são as que constam da minuta de Ata de Registro de Preços.

2.2 Será admitida a adesão à ata de registro de preços decorrente desta licitação, conforme lei 14.133/2021 e 14.770/2023.

3. DO CREDENCIAMENTO.

3.1. O Credenciamento é o nível básico do registro cadastral no SICAF, que permite a participação dos interessados na modalidade licitatória Pregão, em sua forma eletrônica.

3.2. O cadastro no SICAF deverá ser feito no Portal de Compras do Governo Federal, no sítio **compras.gov.br**
por meio de certificado digital conferido pela Infraestrutura de Chaves Pública Brasileira – ICP - Brasil.

3.3. O credenciamento junto ao provedor do sistema implica a responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes a este Pregão.

3.4. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluídos a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

3.5. É de responsabilidade de o cadastrado conferir a exatidão dos seus dados cadastrais no SICAF e mantê- los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

3.5.1. A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação.

4. DA PARTICIPAÇÃO NO PREGÃO

4.1. Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal(**compras.gov.br**), por meio de Certificado Digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil.

4.1.1. Os interessados deverão atender às condições exigidas no cadastramento no Sicaf até o terceiro dia útil anterior à data prevista para recebimento das propostas.

4.2. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

4.3. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais nos Sistemas relacionados no item anterior e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

4.4. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

4.4.1. Não poderão disputar esta licitação:

4.4.2. Aquele que não atenda às condições deste Edital e seu(s) anexo(s);

4.4.3. pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

4.4.4. 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 do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

4.4.5. Empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

4.4.6. 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;

4.4.7. Pessoas jurídicas reunidas em consórcio;

4.4.8. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

4.4.9. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato 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 n.º 14.133, de 2021.

4.5. O impedimento de que trata **o item 4.4.3** 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. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

5.1. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço ou o percentual de desconto, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública.

5.2. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:

5.3. Está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

5.4. Não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

5.5. Não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal.

5.6. Cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

5.7. O licitante organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021.

5.8. O fornecedor enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021.

5.9. No item exclusivo para participação de microempresas e empresas de pequeno porte, a assinalação do campo "não" impedirá o prosseguimento no certame, para aquele item;

5.10. Nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo "não" apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006 mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.

5.11. A falsidade da declaração de que trata os itens 5.7 ou 5.8 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

5.12. Os licitantes poderão retirar ou substituir a proposta ou, na hipótese de a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, os documentos de habilitação anteriormente inseridos no sistema, até a abertura da sessão pública.

5.13. Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

5.14. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.

5.15. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo quando do cadastramento da proposta e obedecerá às seguintes regras:

5.16. A aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta;

5.17. Os lances serão de envio automático pelo sistema, respeitado o valor final mínimo estabelecido e o intervalo de que trata o subitem acima.

5.18. O valor final mínimo ou o percentual de desconto final máximo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

5.18.1. Palor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço; e

5.18.2. Percentual de desconto inferior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por maior desconto

5.18.3. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

5.19. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

6. DO PREENCHIMENTO DA PROPOSTA

6. 1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

6.1.1. Valor unitário e total;

6.1.2. Marca (quando for o caso);

6.1.3. Descrição do objeto, contendo as informações similares à especificação do Termo de Referência;

6.2. Todas as especificações do objeto contidas na proposta vinculam o licitante;

6.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, , tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

6.4. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto;

6.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, , a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses;

6.6. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos, na fonte, os percentuais estabelecidos na legislação vigente.

6.7. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

6.8. O prazo de validade da proposta não será inferior a 60(sessenta) dias, a contar da data de sua apresentação.

6.9. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas, quando participarem de licitações públicas.

6.10. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização pelo Tribunal de Contas da União e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

7. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES.

7.1. A abertura da presente licitação dar-se-á em sessão pública, por meio de sistema eletrônico, na data, horário e local indicado neste Edital.

7.2. Os licitantes poderão retirar ou substituir a proposta ou os documentos de habilitação, quando for o caso, anteriormente inseridos no sistema, até a abertura da sessão pública.

7.2.1. Serão aceitos somente lances em moeda corrente nacional (R$), com no máximo 02 (duas) casas decimais, considerando as quantidades constantes no TERMO DE REFERENCIA (anexo I) do presente edital.

7.2.2. Também será desclassificada a proposta que identifique o licitante.

7.2.3. A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

7.2.4. A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.

7.3. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

7.4. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

7.5. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

7.5.1. O lance deverá ser ofertado pelo valor unitário do item.

7.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

7.7. O licitante somente poderá oferecer lance de valor inferior ou percentual de desconto superior ao último por ele ofertado e registrado pelo sistema.

7.8. Será adotado para o envio de lances no pregão eletrônico o modo de disputa "aberto", em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

7.8.1. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de de R$ 0,01(um centavo) com valor de referência sigilos.

7.8.2. O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

7.9. A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

7.10. A prorrogação automática da etapa de lances, de que trata o item anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

7.11. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

7.11.1. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

7.11.2. Após o reinício previsto no item supra, os licitantes serão convocados para apresentar lances intermediários.

7.12. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

7.13. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

7.14. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

7.15. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

7.16. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

7.17. A melhor classificada nos termos do subitem anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

7.17.1. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

7.17.2. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

7.18. Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

7.18.1.1. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133, de 2021, nesta ordem:

7.18.1.2. Disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

7.18.1.3. Avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos nesta Lei;

7.18.1.4. Desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;

7.18.1.5. Desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

7.18.2. Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

7.18.2.1. Empresas estabelecidas no território do Estado ou do Distrito Federal do órgão ou entidade da Administração Pública estadual ou distrital licitante ou, no caso de licitação realizada por órgão ou entidade de Município, no território do Estado em que este se localize;

7.18.2.2. Empresas brasileiras;

7.18.2.3. Empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

7.18.2.4. Empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de dezembro de 2009.

7.19. Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo ou inferior ao desconto definido para a contratação, o pregoeiro poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

7.19.1. A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela Administração.

7.19.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

7.19.3. O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório

7.20. O pregoeiro solicitará ao licitante mais bem classificado que, no prazo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

7.21. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

7.22. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

8. DA FASE DE JULGAMENTO

8.1. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e no item 21 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

a) SICAF;

b) Cadastro Nacional de Empresas Inidôneas e Suspensas CEIS, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/ceis); e

C) Cadastro Nacional de Empresas Punidas – CNEP mantido pela Controladoria -Geral da União (https://www.portaltransparencia.gov.br/sancoes/cnep)

8.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei n° 8.429, de 1992.

8.3. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas. (IN nº 3/2018, art. 29, caput).

8.4. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros. (IN nº 3/2018, art. 29, §1º).

8.5. O licitante será convocado para manifestação previamente a uma eventual desclassificação. (IN nº 3/2018, art. 29, §2º).

8.6. Constatada a existência de sanção, o licitante será reputado inabilitado, por falta de condição de participação.

8.7. Caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

8.8. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício, em conformidade com o item 4.6 deste edital.

8.9. Verificadas as condições de participação e de utilização do tratamento favorecido, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no artigo 29 a 35 da IN SEGES nº 73, de 30 de setembro de 2022.

8.10. Será desclassificada a proposta vencedora que:

8.10.1.1. contiver vícios insanáveis;

8.10.1.2. não obedecer às especificações técnicas contidas no Termo de Referência;

8.10.1.3. apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

8.10.1.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

8.10.1.5. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

8.10.2.1. No caso de bens e serviços em geral, é indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

8.10.2.2. A inexequibilidade, na hipótese de que trata o **caput**, só será considerada após diligência do pregoeiro, que comprove:

8.10.2.3. Que o custo do licitante ultrapassa o valor da proposta; e

8.10.2.4. Inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

8.11. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a exequibilidade da proposta.

8.12. Erros no preenchimento da proposta não constituem motivo para a desclassificação da proposta. A proposta poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço.

8.12.1. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas;

8.12.2. Considera-se erro no preenchimento da proposta passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

8.13. Caso o Termo de Referência exija a apresentação de amostra, o licitante classificado em primeiro lugar deverá apresentá-la, conforme disciplinado no Termo de Referência, sob pena de não aceitação da proposta.

8.14. Por meio de mensagem no sistema, será divulgado o local e horário de realização do procedimento para a avaliação das amostras, cuja presença será facultada a todos os interessados, incluindo os demais licitantes.

8.15. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

8.16. No caso de não haver entrega da amostra ou ocorrer atraso na entrega, sem justificativa aceita pelo Pregoeiro, ou havendo entrega de amostra fora das especificações previstas neste Edital, a proposta do licitante será recusada.

8.16.1. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas;

8.16.2. Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

8.17. Caso o Termo de Referência exija a apresentação de amostra, o licitante classificado em primeiro lugar deverá apresentá-la, conforme disciplinado no Termo de Referência, sob pena de não aceitação da proposta.

8.18. Por meio de mensagem no sistema, será divulgado o local e horário de realização do procedimento para a avaliação das amostras, cuja presença será facultada a todos os interessados, incluindo os demais licitantes.

8.19. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

8.20. No caso de não haver entrega da amostra ou ocorrer atraso na entrega, sem justificativa aceita pelo Pregoeiro, ou havendo entrega de amostra fora das especificações previstas neste Edital, a proposta do licitante será recusada.

8.20.1. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas;

8.20.2. Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

8.21. Caso o Termo de Referência exija a apresentação de amostra, o licitante classificado em primeiro lugar deverá apresentá-la, conforme disciplinado no Termo de Referência, sob pena de não aceitação da proposta.

8.22. Por meio de mensagem no sistema, será divulgado o local e horário de realização do procedimento para a avaliação das amostras, cuja presença será facultada a todos os interessados, incluindo os demais licitantes.

8.23. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

8.24. No caso de não haver entrega da amostra ou ocorrer atraso na entrega, sem justificativa aceita pelo

Pregoeiro, ou havendo entrega de amostra fora das especificações previstas neste Edital, a proposta do licitante será recusada.

8.25. Se a(s) amostra(s) apresentada(s) pelo primeiro classificado não for(em) aceita(s), o Pregoeiro analisará a aceitabilidade da proposta ou lance ofertado pelo segundo classificado Seguir-se-á com a verificação da(s) amostra(s) e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no Termo de Referência.

9. DA FASE DE HABILITAÇÃO

9.1. Os documentos previstos no Termo de Referência, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021.

9.2. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, poderá ser substituída pelo registro cadastral no SICAF.

9.3. Na hipótese de o licitante vencedor ser empresa estrangeira que não funcione no País, para fins de assinatura do contrato ou da ata de registro de preços, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

9.4. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas na forma da lei (art. 63, I, da Lei nº 14.133/2021)

9.5. O licitante deverá apresentar, sob pena de desclassificação, declaração de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

9.6. A habilitação será verificada por meio do Sicaf, nos documentos por ele abrangidos.

9.6.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir. (IN nº 3/2018, art. 4º, §1º, e art. 6º, §4º).

9.6. É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no Sicaf e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados. (IN nº 3/2018, art. 7º, *caput*).

9.7. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

9.7.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de ***[NO MÍNIMO, DUAS HORAS]***, prorrogável por igual período, contado da solicitação do pregoeiro.

9.8. A verificação no Sicaf ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante vencedor.

9.8.1. Os documentos relativos à regularidade fiscal que constem do Termo de Referência somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

9.9. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para (Lei 14.133/21, art. 64, e IN 73/2022, art. 39, §4º):

9.9.1. Complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

9.9.2. Atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;

9.10. Na análise dos documentos de habilitação, o pregoeiro poderá sanar erros ou falhas, que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

9.11. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital, observado o prazo disposto no edital.

9.12. Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.

9.13. A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte somente será exigida para efeito de contratação, e não como condição para participação na licitação (art. 4º do Decreto nº 8.538/2015).

9.14. **Habilitação jurídica:**

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

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

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

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

9.14.5. **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;

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

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

9.14.8. **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

9.14.9. **Sociedade cooperativa:** ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

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

9.15. **Regularidade fiscal e trabalhista:**

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

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

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

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

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

9.15.6. Prova de regularidade com a Fazenda [Estadual/Distrital] e [Municipal/Distrital] do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre.

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

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

9.16. **Qualificação Econômico-Financeira.**

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

9.16.2. Certidão Negativa de Falência e Concordata expedida pelo distribuidor da sede da pessoa jurídica, datada de, no máximo, 30 (trinta) dias antes da data da abertura do certame, caso não apresente o seu prazo de validade.

Obs: Caso a Certidão seja Positiva de Recuperação, deverá a empresa apresentar a comprovação que seu Plano de Recuperação foi acolhido judicialmente, na forma do Art. 58 da Lei nº 11.101/2005, sob pena de inabilitação.

9.16.3. Atenção: Senhores licitantes, ao solicitar as Certidões de Falência e Concordata, ou Recuperação Judicial ou Extrajudicial, perante o Poder Judiciário do Estado De Mato Grosso, devem ser selecionadas as opções AUTOR e RÉU, para o cumprimento do Art. 69, II da Lei nº 14.133/2021. Para os licitantes dos demais estados, caso não contenha os termos acima, deverão certificar que as certidões expedidas em suas comarcas atestam a inexistência de ações de Falência e Concordata movidas ou em desfavor da empresa solicitante. Podendo o Agente de Contratação e/ou Pregoeiro realizar diligência a fim de verificar o atendimento da Lei Federal nº 14.133/2021, em vistas do art. 97 da Lei nº 11.101/05.

9.16.4. Índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), comprovados mediante a apresentação pelo licitante de **balanço patrimonial na forma da lei** e demais demonstrações contábeis **dos 2 (dois) últimos exercícios sociais** e obtidos pela aplicação das seguintes fórmulas:
I - Liquidez Geral (LG) = (Ativo Circulante + Realizável a Longo Prazo)/(Passivo Circulante + Passivo Não Circulante);II - Solvência Geral (SG)= (Ativo Total)/(Passivo Circulante +Passivo não Circulante); e III - Liquidez Corrente (LC) = (Ativo Circulante)/(Passivo Circulante).

9.16.5. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC)), será exigido para fins de habilitação [patrimônio líquido mínimo] de 5% do valor total de cada item.

9.16.6. 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).

9.16.7. O balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos. (Lei nº 14.133, de 2021, art. 69, §6º).

9.17. **Qualificação Técnica**

9.17.1. Comprovação de aptidão para o fornecimento de bens em características, compatíveis com o objeto desta licitação, ou com o item pertinente, por meio da apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado.

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

9.17.3. A existência de restrição relativamente à regularidade fiscal e trabalhista não impede que a licitante qualificada como microempresa ou empresa de pequeno porte seja declarada vencedora, uma vez que atenda a todas as demais exigências do edital.

9.17.4. A declaração do vencedor acontecerá no momento imediatamente posterior à fase de habilitação.

9.17.5. Caso a proposta mais vantajosa seja ofertada por licitante qualificada como microempresa ou empresa de pequeno porte, e uma vez constatada a existência de alguma restrição no que tange à regularidade fiscal e trabalhista, a mesma será convocada para, no prazo de 5 (cinco) dias úteis, após a declaração do vencedor, comprovar a regularização. O prazo poderá ser prorrogado por igual período, a critério da administração pública, quando requerida pelo licitante, mediante apresentação de justificativa.

9.17.6. A não-regularização fiscal e trabalhista no prazo previsto no subitem anterior acarretará a inabilitação do licitante, sem prejuízo das sanções previstas neste Edital, sendo facultada a convocação dos licitantes remanescentes, na ordem de classificação. Se, na ordem de classificação, seguir-se outra microempresa, empresa de pequeno porte ou sociedade cooperativa com alguma restrição na documentação fiscal e trabalhista, será concedido o mesmo prazo para regularização.

9.17.7. Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no "chat" a nova data e horário para a continuidade da mesma.

9.17.8. Será inabilitado o licitante que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste Edital.

9.17.9. Nos itens não exclusivos a microempresas e empresas de pequeno porte, em havendo inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

9.17.10. O licitante provisoriamente vencedor em um item, que estiver concorrendo em outro item, ficará obrigado a comprovar os requisitos de habilitação cumulativamente, isto é, somando as exigências do item em que venceu às do item em que estiver concorrendo, e assim sucessivamente, sob pena de inabilitação, além da aplicação das sanções cabíveis.

9.17.11. Não havendo a comprovação cumulativa dos requisitos de habilitação, a inabilitação recairá sobre o(s) itens de menor(es) valor(es) cuja retirada(s) seja(m) suficiente(s) para a habilitação do licitante nos remanescentes.

9.17.12. Constatado o atendimento às exigências de habilitação fixadas no Edital, o licitante será declarado vencedor.

10. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

10.1. A proposta final do licitante declarado vencedor deverá ser encaminhada no prazo de 2 (duas) horas, a contar da solicitação do Pregoeiro no sistema eletrônico e deverá:

10.1.1. Ser redigida em língua portuguesa, datilografada ou digitada, em uma via, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada e as demais rubricadas pelo licitante ou seu representante legal.

10.1.2. Conter a indicação do banco, número da conta e agência do licitante vencedor, para fins de pagamento.

10.2. A proposta final deverá ser documentada nos autos e será levada em consideração no decorrer da execução do contrato e aplicação de eventual sanção à Contratada, se for o caso.

10.2.1. Todas as especificações do objeto contidas na proposta, tais como marca, modelo, tipo, fabricante e procedência, vinculam a Contratada.

10.3. Os preços deverão ser expressos em moeda corrente nacional, o valor unitário em algarismos e o valor global em algarismos e por extenso.

10.3.1. Ocorrendo divergência entre os preços unitários e o preço global, prevalecerão os primeiros; no caso de divergência entre os valores numéricos e os valores expressos por extenso, prevalecerão estes últimos.

10.4. A oferta deverá ser firme e precisa, limitada, rigorosamente, ao objeto deste Edital, sem conter alternativas de preço ou de qualquer outra condição que induza o julgamento a mais de um resultado, sob pena de desclassificação.

10.5. A proposta deverá obedecer aos termos deste Edital e seus Anexos, não sendo considerada aquela que não corresponda às especificações ali contidas ou que estabeleça vínculo à proposta de outro licitante.

10.6. As propostas que contenham a descrição do objeto, o valor e os documentos complementares estarão disponíveis na internet, após a homologação.

11. DOS RECURSOS

11.6. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021.

11.7. O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata.

11.8. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:

11.8.1. A intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;

11.8.2. O prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

11.8.3. Na hipótese de adoção da inversão de fases prevista no § 1º do art. 17 da Lei nº 14.133, de 2021, o prazo para apresentação das razões recursais será iniciado na data de intimação da ata de julgamento.

11.9. Os recursos deverão ser encaminhados em campo próprio do sistema.

11.10. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

11.11. Os recursos interpostos fora do prazo não serão conhecidos.

11.12. O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de 3 (três) dias úteis, contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.

11.13. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

11.14. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

11.15. Os autos do processo permanecerão com vista franqueada aos interessados no sítio eletrônico licitacao@caceres.gov.mt.br.

12. DA REABERTURA DA SESSÃO PÚBLICA

12.1. A sessão pública poderá ser reaberta:

12.1.1. Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.

12.1.2. Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal

e trabalhista, nos termos do art. 43, §1º da LC nº 123/2006. Nessas hipóteses, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

12.2. Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.

12.2.1. A convocação se dará por meio do sistema eletrônico (“chat”), e-mail, ou, ainda, fac-símile, de acordo com a fase do procedimento licitatório.

12.2.2. A convocação feita por e-mail ou fac-símile dar-se-á de acordo com os dados contidos no SICAF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

13. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

13.1. Encerradas as fases e julgamento e habilitação, e exauridos os recursos adminitrativos, o ,processo licitatório será encaminhada à autoridade superior para adjudicar o objeto e homologar o procedimento, observado no art. 71 da lei n.º 14.133, de 2021.

14. DA GARANTIA DA EXECUÇÃO

14.1 Não será exigida a prestação de garantia na presente contratação, Termo de Referência.

15. A ATA DE REGISTRO DE PREÇOS

15.1. Homologado o resultado da licitação, terá o adjudicatário o prazo de 2 (dois) dias, contados a partir da data de sua convocação, para assinar a Ata de Registro de Preços, cujo prazo de validade encontra-se nela fixado, sob pena de decair do direito à contratação.

15.2. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura da Ata de Registro de Preços, a Administração poderá encaminhá-la para assinatura,meio eletrônico, para que seja assinada e devolvida no prazo de 2 (dois) dias, a contar da data de seu recebimento.

15.3. O prazo estabelecido no subitem anterior para assinatura da Ata de Registro de Preços poderá ser prorrogado uma única vez, por igual período, quando solicitado pelo(s) licitante(s) vencedor(s), durante o seu transcurso, e desde que devidamente aceito.

15.4. Serão formalizadas tantas Atas de Registro de Preços quanto necessárias para o registro de todos os itens constantes no Termo de Referência, com a indicação do licitante vencedor, a descrição do(s) item(ns), as respectivas quantidades, preços registrados e demais condições.

15.5. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades legalmente estabelecidas e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação.

16. DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE

16.1. Após a homologação da licitação, em sendo realizada a contratação, será firmado Termo de Contrato ou emitido instrumento equivalente.

16.2.1. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato ou aceite do instrumento equivalente, a Administração poderá encaminhá-lo para assinatura ou aceite da Adjudicatária, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinado ou aceito no prazo de 3 (três) dias, a contar da data de seu recebimento.

16.2.2. O prazo previsto no subitem anterior poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

16.3. O Aceite da Nota de Empenho ou do instrumento equivalente, emitida à empresa adjudicada, implica no reconhecimento de que:

16.3.2. A contratada se vincula à sua proposta e às previsões contidas no edital e seus anexos;

16.5. Previamente à contratação a Administração realizará consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018, e nos termos do art. 6º, III, da Lei nº 10.522, de 19 de julho de 2002, consulta prévia ao CADIN.

16.5.2. Na hipótese de irregularidade do registro no SICAF, o contratado deverá regularizar a sua situação perante o cadastro no prazo de até 05 (cinco) dias úteis, sob pena de aplicação das penalidades previstas no edital e anexos.

16.6. Na assinatura do contrato ou da ata de registro de preços, será exigida a comprovação das condições de habilitação consignadas no edital, que deverão ser mantidas pelo licitante durante a vigência do contrato ou da ata de registro de preços.

16.7. Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no edital ou se recusar a assinar o contrato ou a ata de registro de preços, a Administração, sem prejuízo da aplicação das sanções das demais cominações legais cabíveis a esse licitante, poderá convocar outro licitante, respeitada a ordem de classificação, para, após a comprovação dos requisitos para habilitação, analisada a proposta e eventuais documentos complementares e, feita a negociação, assinar o contrato ou a ata de registro de preços.

17. DO REAJUSTAMENTO EM SENTIDO GERAL

17.1. As regras acerca do reajustamento em sentido geral do valor contratual são as estabelecidas no Termo de Referência, anexo a este Edital.

18. DO RECEBIMENTO DO OBJETO E DA FISCALIZAÇÃO

18.1. Os critérios de recebimento e aceitação do objeto e de fiscalização estão previstos no Termo de Referência.

19. DO RECEBIMENTO DO OBJETO E DA FISCALIZAÇÃO

19.1. As obrigações da Contratante e da Contratada são as estabelecidas no Termo de Referência.

20. DO PAGAMENTO

20.1. As regras acerca do pagamento são as estabelecidas no Termo de Referência, anexo a este Edital.

21. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

21.6. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:

21.6.1. Deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a pregoeiro/a durante o certame;

21.6.2. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:

21.6.2.1. Não enviar a proposta adequada ao último lance ofertado ou após a negociação;

21.6.2.2. Recusar-se a enviar o detalhamento da proposta quando exigível;

21.6.2.3. Pedir para ser desclassificado quando encerrada a etapa competitiva; ou

21.6.2.4. Deixar de apresentar amostra;

21.6.2.5. Apresentar proposta ou amostra em desacordo com as especificações do edital;

21.6.3. Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

21.6.3.1. Recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

21.6.4. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação

21.6.5. Fraudar a licitação

21.6.6. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

21.6.6.1. Agir em conluio ou em desconformidade com a lei;

21.6.6.2. Induzir deliberadamente a erro no julgamento;

21.6.6.3. Apresentar amostra falsificada ou deteriorada;

21.6.7. Praticar atos ilícitos com vistas a frustrar os objetivos da licitação

21.6.8. Praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.

21.7. Com fulcro na Lei nº 14.133, de 2021, a Administração poderá, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

21.7.1. Advertência;
21.7.2. Multa;
21.7.3. Impedimento de licitar e contratar e
21.7.4. Declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

21.8. Na aplicação das sanções serão considerados:
21.8.1. A natureza e a gravidade da infração cometida.
21.8.2. As peculiaridades do caso concreto
21.8.3. As circunstâncias agravantes ou atenuantes
21.8.4. Os danos que dela provierem para a Administração Pública
21.8.5. A implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.
21.8.6. A multa será recolhida em percentual de 5% (cinco por cento) incidente sobre o valor incidente sobre o valor do contrato licitado, recolhida no prazo máximo de 30 (trinta) dias úteis, a contar da comunicação oficial.
21.8.7. Para as infrações previstas no Termo de Referência, a multa será de 5% (cinco por cento) do valor do contrato licitado.
21.8.8. Para as infrações previstas no Termo de Referência, a multa será de 5% (cinco por cento) do valor do contrato licitado.
21.8.9. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.
21.9. Na aplicação da sanção de multa será facultada a defesa do interessado no prazo de 15 quinze) dias úteis, contado da data de sua intimação.
21.10. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas no Termo de Referência, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.
21.10.1. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos Termo de Referência, que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar cuja duração observará o prazo previsto no art. 156 da lei n.º 14.133/2021.
21.10.2. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 21.6.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação, nos termos do art. 45, §4º da IN SEGES/ME n.º 73, de 2022.
21.10.3. A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15

(quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produz.

21.11. Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

21.11.1. Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

21.12. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

21.12.1. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causado.

22. DA FORMAÇÃO DO CADASTRO DE RESERVA

22.1. Após o encerramento da etapa competitiva, os licitantes poderão reduzir seus preços ao valor da proposta do licitante mais bem classificado.

22.2. A apresentação de novas propostas na forma deste item não prejudicará o resultado do certame em relação ao licitante melhor classificado.

22.3. Havendo um ou mais licitantes que aceitem cotar suas propostas em valor igual ao do licitante vencedor, estes serão classificados segundo a ordem da última proposta individual apresentada durante a fase competitiva.

22.4. Esta ordem de classificação dos licitantes registrados deverá ser respeitada nas contratações e somente será utilizado acaso o melhor colocado no certame não assine a ata ou tenha seu registro cancelado nas hipóteses previstas nos regulamentos vigentes.

23. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

23.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da Lei nº 14.133, de 2021, devendo protocolar o pedido até 3 (cinco) dias úteis antes da data da abertura do certame.

23.1.1. A resposta à impugnação ou ao pedido de esclarecimento será divulgado em sítio eletrônico oficial no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

23.2. A impugnação poderá ser realizada por forma eletrônica, pelo **e-mail licitacao@caceres.mt.gov.br** ou por petição dirigida ou protocolada diretamente na Secretaria de administração: Sala de licitações, da Prefeitura Municipal de Cáceres/MT – Endereço: Av. Brasil, 119, COC, Bairro Jardim Celeste – CEP 78.206- 910 – Cáceres – MT, dirigida ao(à) pregoeiro(a), contendo os documentos necessários de qualificação do requerente, sendo em qualquer dos casos durante o seguinte horário: das 07:30 as 11:30h e das 13:30 as 17:30 (horário local).

23.3. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

23.4. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro, nos autos do processo de licitação.

23.5. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

24. DA PUBLICAÇÃO

24.1. Incumbirá ao contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, *caput,* da Lei n.º 14.133, de 2021, e ao art. 8º, §2º, da Lei n. 12.527, de 2011, c/c art. 7º,
§3º, inciso V, do Decreto n. 7.724, de 2012.

25. DAS DISPOSIÇÕES GERAIS

25.6. Será divulgada ata da sessão pública no sistema eletrônico.

25.7. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.

25.8. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília - DF.

25.9. A homologação do resultado desta licitação não implicará direito à contratação.

25.10. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

25.11. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

25.12. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir- se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

25.13. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

25.14. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

24.10. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital. Havendo divergência entre as especificações dos itens do CATSER e do termo de referência, prevalecerá o termo de referência.

24.11. O Edital está disponibilizado, na íntegra, no endereço eletrônico **http://www.caceres.mt.gov.br/licitacao/,** e também poderão ser lidos e/ou obtidos no endereço **compras.gov.br** nos dias úteis, no horário das 07h:30min às 11h:30min das 13h:30min às 17h:30min, mesmo endereço e período no qual os autos do processo administrativo permanecerão com vista franqueada aos interessados.

24.12. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

24.12.1. ANEXO I – TERMO DE REFERÊNCIA

24.12.2. ANEXO II – MINUTA DA ATA DE REGISTRO DE PREÇO

24.12.3. ANEXO III – MINUTA DO TERMO DE CONTRATO

Cáceres/MT, 11 de junho de 2025.

JEREMIAS PEREIRA LEITE
Secretário Municipal Especial de Assustos estratégicos

tório - 029/2025 | [illegible] (21/233) [illegible]

ANEXO I – 1ª RETIFICAÇÃO DO TERMO DE REFERÊNCIA 01/2025

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Registro de Preço para futura e eventual contratação de empresa especializada para prestação de serviços de segurança cibernética com Inteligência Artificial Preditiva, garantindo alta disponibilidade, segurança, eficiência e sustentabilidade no atendimento às demandas do Município de Cáceres, conforme condições e exigências estabelecidas neste instrumento.

1.1.1. O serviço a ser prestado engloba, fornecimento em regime de comodato, instalação e configuração de Next Generation Firewall (NGFW) e SD-WAN, redundância composta por links primário e secundário de ASN e rotas diferentes, manutenção contínua, suporte técnico, software de gerenciamento, conectividade segura para unidades externas e praças públicas, capacitação certificada da equipe e atendimento técnico especializado.

LOTE	ITEM	CÓDIGO TCE-MT	CÓDIGO CAT MAT	ESPECIFICAÇÃO	UNIDADE	QUANTIDADE	QUANTIDADE ANUAL
1 (ÚNICO)	1	257560-4	609340	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)	Serviço	173	2076
	2	152969	481647	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	Serviço	2	24
	3	00065206	26174	Serviço de Link dedicado de Acesso à internet, bloco /29 e Banda Mínima de Acesso Garantida de 500Mbps (Alta Disponibilidade) SEDE (Link de ASN e Rota Diferentes)	Serviço	2	24
	4	152970	26484	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 150Mbps Sites Remotos (Fibra Óptica)	Serviço	171	2052
	5	152972	26557	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G)	Serviço	171	2052
	6	339905-2	1988	Implantação da Solução	Serviço	1	1
	7	404876-8	16837	Capacitação especializada da equipe com emissão de certificação.	Treinamento	1	1
	8	332679-9	27340	Consultoria Política de Segurança	Serviço	1	1

tório - 029/2025 | [illegible] .pdf (22/232) [illegible]

1.2. A licitação será realizada por meio de um único lote, contendo diversos itens, conforme especificado no Termo de Referência. O licitante deverá apresentar uma proposta para todos os itens dentro do lote, sendo vedada a oferta parcial.

1.3. A análise da documentação terá por finalidade verificar a habilitação da empresa, bem como sua capacidade de operar um projeto dessa complexidade.

1.3.1. Caso as exigências não sejam atendidas, será convocada a empresa subsequente que tenha apresentado o preço global imediatamente superior, observadas as regras de negociação.

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

1.5. O prazo de vigência da contratação será de 12 (doze) meses, contados a partir da assinatura do contrato, podendo ser prorrogado por períodos iguais e consecutivos, desde que, durante o planejamento e toda a execução do contrato, sejam observadas as seguintes condições:

a) seja emitido ateste da autoridade competente do órgão ou entidade contratante, confirmando que a contratação representa a alternativa mais vantajosa do ponto de vista econômico, em razão de sua natureza plurianual;

b) haja previsão e disponibilidade de créditos orçamentários vinculados à contratação e justificativa quanto à conveniência de sua manutenção; e

c) a Administração possa rescindir o contrato, sem ônus, caso não disponha dos recursos orçamentários necessários à sua continuidade ou caso entenda que a contratação deixou de atender ao interesse público.

Esse prazo poderá se estender até o limite de 15 (quinze) anos, conforme estabelecido no artigo 114 da Lei nº 14.133/2021, diante da natureza continuada da operação e da sua caracterização como sistema estruturante de tecnologia da informação, conforme demonstrado no Estudo Técnico Preliminar.

1.6. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico do Estudo Técnico Preliminar, apêndice deste Termo de Referência.

3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

3.1. A Fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada em tópico específico do Estudo Técnico Preliminar, apêndice deste Termo de Referência.

3.2. O objeto da contratação está previsto no Plano de Contratações Anual [2025], conforme detalhamento a seguir:

I) ID PCA no PNCP: 03214145000183-0-000001/2025;
II) Data de publicação no PNCP: 28/01/2025;
III) Id do item no PCA: 166;

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

4.1. A solução tem por objetivo proporcionar uma infraestrutura robusta, segura e eficiente para o ambiente de tecnologia da informação da Prefeitura Municipal de Cáceres, assegurando a continuidade dos serviços públicos e a proteção dos dados institucionais. O ciclo de vida da solução contempla todas as fases essenciais, desde a implantação até a operação contínua, manutenção e eventuais atualizações tecnológicas, garantindo um alto padrão de qualidade e desempenho ao longo da vigência do contrato.

4.2. A solução contempla segurança cibernética avançada, conectividade de alto desempenho e suporte especializado, alinhando-se às melhores práticas de governança digital e proteção de ativos públicos.

4.3. A implantação e execução do contrato seguem um modelo estruturado em duas fases principais:

4.3.1. **Fase de Implantação**, com prazo de até 60 dias após a assinatura do contrato, abrangendo a instalação dos equipamentos, ativação dos links, integração das unidades externas e capacitação da equipe técnica.

4.3.2. **Fase de Prestação de Serviço Mensal**, com duração de até 180 meses, garantindo manutenção contínua, suporte técnico especializado, atualizações tecnológicas e otimização da infraestrutura de segurança e comunicação de dados.

4.4. O ciclo de vida da solução envolve etapas bem definidas, assegurando que a infraestrutura implementada esteja sempre atualizada e alinhada com as necessidades da Prefeitura.

4.4.1. **Planejamento e Implantação**

4.4.1.1. Na fase inicial, serão executadas as atividades necessárias para a estruturação da solução contratada, garantindo que todos os componentes sejam devidamente configurados e operacionalizados. Essa etapa inclui:

4.4.1.1.1. Instalação e configuração dos equipamentos de segurança cibernética, incluindo Next Generation Firewall (NGFW) e SD-WAN, visando a proteção contra ameaças digitais e a otimização do tráfego de rede.

4.4.1.1.2. Implementação de serviços de segurança cibernética baseados em Inteligência Artificial Preditiva, permitindo a detecção e resposta antecipada a incidentes.

4.4.1.1.3. Ativação dos links dedicados de internet, garantindo 500 Mbps na sede, 150 Mbps nos sites remotos e 35 Mbps como link de contingência, assegurando conectividade estável para as operações administrativas e serviços públicos digitais.

4.4.1.1.4. Integração das unidades externas e praças públicas à infraestrutura de rede segura, possibilitando um acesso seguro e confiável aos sistemas municipais.

4.4.1.1.5. Capacitação certificada da equipe técnica da Prefeitura, garantindo a qualificação necessária para a gestão e monitoramento da solução implementada.

4.4.2. **Operação e Manutenção**

4.4.2.1. Após a implantação, a solução entrará em operação contínua, garantindo que os serviços contratados sejam entregues de forma eficiente e dentro dos padrões de qualidade exigidos. Esta fase inclui:

4.4.2.1.1. Monitoramento contínuo da infraestrutura, com análises preditivas para detecção de ameaças e otimização do desempenho dos sistemas.

4.4.2.1.2. Suporte técnico especializado, disponível para resolver quaisquer incidentes ou necessidades de ajustes na configuração da solução.

4.4.2.1.3. Gestão e atualização dos equipamentos e software, garantindo que os firewalls, SD-WAN e demais componentes tecnológicos operem sempre com as versões mais recentes e seguras.

4.4.2.1.4. Consultoria contínua para aprimoramento da política de segurança da informação, com foco na proteção de dados, conformidade regulatória e mitigação de riscos cibernéticos.

4.4.2.1.5. Garantia de alta disponibilidade, com suporte a redundância de links e contingência operacional para evitar interrupções nos serviços municipais.

4.4.3. **Evolução e Sustentabilidade da Solução**

4.4.3.1. Ao longo do ciclo de vida da solução, serão adotadas práticas que garantam sua evolução tecnológica e sustentabilidade, permitindo que o investimento realizado permaneça eficiente e alinhado às necessidades do município. Entre essas práticas, destacam-se:

4.4.3.1.1. Adoção de tecnologias emergentes para otimizar a performance e segurança da infraestrutura de TIC.

4.4.3.1.2. Revisão periódica da estratégia de segurança cibernética, considerando as tendências de ameaças digitais e as melhores práticas do setor.

4.4.3.1.3. Expansão escalável da solução, permitindo a incorporação de novas unidades e serviços de forma ágil e estruturada.

4.4.3.1.4. Otimização do consumo de recursos tecnológicos, garantindo um uso eficiente da infraestrutura contratada e contribuindo para a sustentabilidade financeira e operacional do município.

4.5. **Especificação do Produto**

4.5.1. **Funcionamento Geral da Solução**

4.5.1.1. A contratação deverá englobar além das soluções de defesa cibernética a prestação de serviços de rede de longa distância (WAN) para manter a interligação da Sede da Prefeitura de Cáceres aos Sites Remotos, localizados no interior do Município e fora dele.

4.5.1.2. A contratação também inclui a prestação de serviço de acesso à internet nos Sites Remotos e na sede da Prefeitura Municipal de Cáceres MT.

tório - 029/2025 | [illegible] (25/232) [illegible]

4.5.1.3. A contratação deverá englobar o fornecimento de um conjunto de equipamentos de redes incluindo recursos de IP para trabalhar em alta disponibilidade na Sede e cada equipamento deverá permitir no mínimo 4(quatro) conexões à Internet.

4.5.1.4. A nova solução de comunicação de dados entre os Sites Remotos e a Sede utilizará equipamentos com a tecnologia SD-WAN com o objetivo de balancear o tráfego de forma inteligente para otimizar o uso da rede. Para que o tráfego corporativo seja protegido quando trafegar pela internet, serão configurados túneis VPN IPSEC entre os equipamentos SD-WAN da Sede da Prefeitura e dos Sites Remotos.

4.5.1.5. Os equipamentos SD-WAN da Sede deverão trabalhar em alta disponibilidade.

4.5.1.6. A relação dos Sites Remotos e da Central nos quais os serviços serão prestados encontra-se descrita no item 7.2.1.3 deste Termo de Referência.

4.5.1.7. Em situações normais, os tráfegos de sistemas da prefeitura sobretudo os administrativos, além do tráfego de telefonia IP, devem ser encaminhados pela via IPSEC pelo melhor link. Por outro lado, os serviços de videoconferência das Plataformas Zoom, Google, Webex e Microsoft Teams devem ser acessados diretamente sem a necessidade de utilização deste túnel, além da navegação de Internet das redes dos assessores, colaboradores e cidadãos que acessam a rede social da Prefeitura.

4.5.1.8. Em situações de falha ou de uso intenso da rede, alternativamente os tráfegos corporativos devem ser encaminhados entre os Sites Central e remotos utilizando também túnel VPN IPSEC pelo link secundário estabelecidos pela Internet. Os túneis VPN devem utilizar a topologia hub-and-spoke, com centralização nos equipamentos SD-WAN na Sede.

4.5.1.9. Em situações de falha de um dos links de Internet dos Sites remotos, o tráfego deve ser encaminhado pela conexão de internet secundária até o Site Central da Prefeitura.

4.5.1.10. A configuração do encaminhamento do tráfego e da contingência em casos de falha deve ser feita utilizando tecnologia SD-WAN em que o encaminhamento de tráfego é feito com base no perfil de tráfego em vez da utilização de rotas.

4.5.1.11. A prestação dos serviços descritos em cada ITEM deverá ser considerada como entregue, a partir da assinatura do Termo de Recebimento Definitivo.

4.5.1.12. A prestação dos serviços será baseada no modelo de remuneração em função dos resultados apresentados, em que os pagamentos serão feitos após mensuração e verificação de métricas quantitativas e qualitativas, contendo indicadores de desempenho e metas, com Instrumento de Medição de Resultado (IMR) definido em contrato, de modo a resguardar a eficiência e a qualidade na prestação dos serviços.

4.5.1.13. Os serviços a serem prestados incluem, ainda, a elaboração prévia de um Projeto Executivo de rede, a ser analisado pela equipe técnica da Prefeitura para aprovação, conforme especificações incluídas neste documento. Esse documento deverá conter, no mínimo:

a) Definição de topologias físicas e lógicas;

b) Plano de Endereçamento;

c) Plano de balanceamento do tráfego;

d) Parâmetros de qualidade de serviço;

e) Dimensionamento de enlaces e interfaces de comunicação;

f) Documentação dos últimos 1000 metros de passagem das fibras ópticas.

4.5.1.14. Não haverá aquisição de equipamentos, incluindo roteadores, modens, appliances SD- WAN e demais ativos de rede. Contudo, deverão ser fornecidos equipamentos juntamente com a prestação dos serviços de tecnologia da informação e comunicações como parte integrante da solução contratada.

4.5.1.15. O CONTRATANTE poderá solicitar a desativação do serviço prestado a qualquer sítio, bem como mudança de local de prestação dos serviços. Entende-se por mudanças de local de prestação dos serviços a mudança de endereços de instalação dos equipamentos e acessos dentro da cidade.

4.5.1.16. Após a conclusão da etapa de instalação dos serviços, a CONTRATADA deverá apresentar documentação técnica da solução (As Built), contendo: topologia física e lógica da rede, descrição de equipamentos e circuitos de comunicação de dados, descrição dos níveis mínimos de serviços contratados, dados para acesso ao portal de monitoramento dos serviços e dados para abertura de chamados de suporte técnico.

4.5.1.17. A CONTRATADA deverá também realizar repasse de conhecimento na modalidade presencial para a equipe técnica do CONTRATANTE sobre a solução implantada, conforme descrito no item 5.2 deste Termo de Referência.

4.5.2. **Topologia Da Solução**

4.5.2.1. A solução foi estruturada com base nas necessidades específicas da Prefeitura Municipal de Cáceres, visando garantir conectividade segura, eficiente e de alta disponibilidade para todas as unidades envolvidas. A infraestrutura foi projetada para suportar um volume significativo de acessos simultâneos, assegurando a qualidade da comunicação de dados, a integridade das informações e a segurança cibernética dos sistemas institucionais.

4.5.2.1.1. Estruturação dos Sites e Capacidade dos Links

4.5.2.1.1.1. A topologia da solução foi desenhada considerando a divisão dos Sites Remotos e do Site Central em dois tipos distintos de tecnologia e capacidade de conexão, com base na demanda estimada de usuários simultâneos e nos requisitos operacionais de cada localidade.

4.5.2.1.1.1.1. **Sites Remotos:** A estrutura contempla unidades como Postos de Saúde, Centros de Saúde e espaços públicos, onde os serviços de tecnologia da informação serão utilizados para fins administrativos e sociais. A demanda estimada para os Postos de Saúde varia entre 7 e 10 usuários simultâneos, enquanto os Centros de Saúde podem atender de 15 a 50 usuários simultaneamente. O tráfego nesses locais incluirá tanto o acesso aos sistemas institucionais da Prefeitura quanto a utilização de serviços públicos digitais pelos cidadãos.

4.5.2.1.1.1.2. **Site Central:** A Sede da Prefeitura concentra entre 400 e 500 usuários simultâneos, entre servidores e colaboradores, acessando tanto recursos internos quanto externos. Devido ao alto volume de tráfego e à criticidade dos serviços processados, a conexão do Site Central conta com dois links dedicados de alta capacidade (500 Mbps cada), providos por ASN distintos e rotas diferentes, garantindo redundância e continuidade operacional.

4.5.2.1.1.2. A configuração dos links de internet e a implementação da tecnologia SD-WAN asseguram balanceamento inteligente do tráfego, priorização de pacotes críticos e segurança reforçada para as comunicações entre as unidades.

4.5.2.1.2. **Topologia Lógica da Solução**

4.5.2.1.2.1. A topologia lógica da solução foi elaborada para representar a interconexão dos elementos envolvidos e demonstrar o produto final desta contratação. A arquitetura contempla os seguintes componentes essenciais:

4.5.2.1.2.1.1. Next Generation Firewalls (NGFW) instalados no Site Central, atuando como pontos de controle de segurança cibernética, prevenindo ataques e garantindo a integridade dos dados trafegados entre as unidades.

4.5.2.1.2.1.2. Solução de segurança cibernética com utilização de Inteligência Preditiva.

4.5.2.1.2.1.3. Dispositivos SD-WAN implementados na Sede e nos Sites Remotos, possibilitando gerenciamento eficiente do tráfego, redundância e otimização dos links de comunicação.

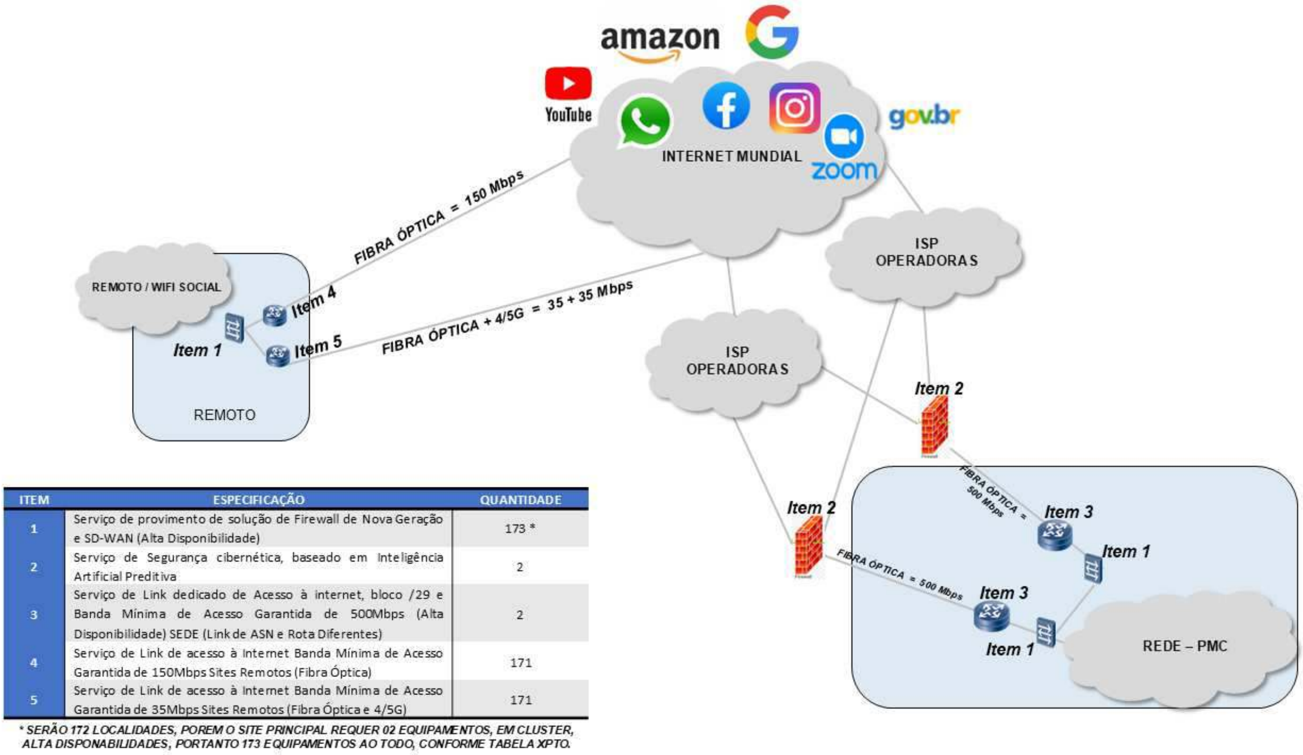
4.5.2.1.2.1.4. VPN IPSEC configurada em topologia hub-and-spoke, assegurando segurança na troca de informações entre os Sites Remotos e o Site Central.

tório - 029/2025 (28/232)

4.5.2.1.2.1.5. Monitoramento centralizado, por meio de um software de gestão e segurança, permitindo a visualização em tempo real do tráfego da rede, detecção de anomalias e gerenciamento proativo de incidentes.

4.5.2.1.2.1.6. Consultoria especializada e capacitação da equipe técnica da Prefeitura, garantindo conhecimento sobre a administração da solução e autonomia na gestão da infraestrutura implantada.

4.5.2.1.2.2. Foi elaborada uma topologia lógica da solução demonstrando o produto final desta contratação:



ITEM	ESPECIFICAÇÃO	QUANTIDADE
1	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)	173 *
2	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	2
3	Serviço de Link dedicado de Acesso à internet, bloco /29 e Banda Mínima de Acesso Garantida de 500Mbps (Alta Disponibilidade) SEDE (Link de ASN e Rota Diferentes)	2
4	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 150Mbps Sites Remotos (Fibra Óptica)	171
5	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G)	171

** SERÃO 172 LOCALIDADES, POREM O SITE PRINCIPAL REQUER 02 EQUIPAMENTOS, EM CLUSTER, ALTA DISPONABILIDADES, PORTANTO 173 EQUIPAMENTOS AO TODO, CONFORME TABELA XPTO.*

4.5.3. **Equipamentos e Funcionalidades Chave**

4.5.3.1. **Os equipamentos do ITEM 1, do Lote Único, deverão ser entregues no formato e características técnicas bem como funcionalidades conforme especificações abaixo:**

4.5.3.1.1. **Appliance NGFW de 5 Gbps de Capacidade de Firewall**

4.5.3.1.1.1. **Características do Hardware**

4.5.3.1.1.1.1. O equipamento deve se instalar em mesa ocupando no máximo 1U (44,45mm) da referida mesa;

4.5.3.1.1.1.2. Dispor de fonte de alimentação com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;

4.5.3.1.1.1.3. Deverão ser fornecidos todos os cabos de energia, serial (RS-232/RJ45), para instalação e funcionamento do dispositivo;

4.5.3.1.1.1.4. Possuir led indicador on/off, disco e devices de rede;

4.5.3.1.1.1.5. Possuir throughput mínimo de 5 Gbps para tráfego UDP;

4.5.3.1.1.1.6. Suportar no mínimo 4.000.000 (quatro milhões) conexões simultâneas;

4.5.3.1.1.1.7. Suportar no mínimo 37.000 (trinta e sete mil) novas conexões por segundo;

4.5.3.1.1.1.8. Possuir throughput mínimo de 300 Mbps para tráfego IPS/IDS;

4.5.3.1.1.1.9. Possuir throughput mínimo de 280 Mbps para tráfego VPN IPSEC com criptografia (AES-256);

4.5.3.1.1.1.10. Possuir throughput mínimo de 140 Mbps para tráfego VPN SSL com criptografia (AES-256);

4.5.3.1.1.1.11. Possuir throughput mínimo de 150 Mbps para SSL Inspection;

4.5.3.1.1.1.12. Possuir throughput mínimo de 200 Mbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

4.5.3.1.1.1.13. Possuir no mínimo 4 (quatro) interfaces de rede Gigabit Ethernet 10/100/1000/2500 Mbps com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

4.5.3.1.1.1.14. Possuir dispositivo de armazenamento interno de no mínimo 64 GB padrão SSD e deve suportar expansão futura para, no mínimo, 120 GB;

4.5.3.1.1.1.15. Possuir no mínimo 1 (uma) porta console de conexão para acesso a interface de comando CLI específica para esta finalidade, utilizando cabo do tipo serial RS-232 ou RJ-45;

4.5.3.1.1.1.16. Possuir pelo menos 1 (uma) portas USB para conexão de dispositivos externos;

4.5.3.1.1.1.17. A interface USB deve suportar o uso de modem 3G/4G/LTE e/ou possuir modem interno 3G/4G/LTE para conexão de link de Internet. O módulo deverá estar incluso no valor do equipamento;

4.5.3.1.2. **Appliance NGFW de 9.7 Gbps de Capacidade de Firewall**

4.5.3.1.2.1. **Características do Hardware**

4.5.3.1.2.1.1. O equipamento deve se instalar em mesa ocupando no máximo 1U (44,45mm) da referida mesa;

4.5.3.1.2.1.2. Dispor de fonte de alimentação com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;

4.5.3.1.2.1.3. Deverão ser fornecidos todos os cabos de energia, serial (RS-232/RJ45) ou similar, para instalação e funcionamento do dispositivo;

4.5.3.1.2.1.4. Possuir led indicador on/off, disco e devices de rede;

4.5.3.1.2.1.5. Possuir throughput mínimo de 9.7 Gbps para tráfego UDP;

4.5.3.1.2.1.6. Suportar no mínimo 6.000.000 (seis milhões) conexões simultâneas;

4.5.3.1.2.1.7. Suportar no mínimo 45.000 (quarenta e cinco mil) novas conexões por segundo;

4.5.3.1.2.1.8. Possuir throughput mínimo de 1.25 Gbps para tráfego IPS/IDS;

4.5.3.1.2.1.9. Possuir throughput mínimo de 2.0 Gbps para tráfego VPN IPSEC com criptografia (AES-256);

4.5.3.1.2.1.10. Possuir throughput mínimo de 1.2 Gbps para tráfego VPN SSL com criptografia (AES-256);

4.5.3.1.2.1.11. Possuir throughput mínimo de 700 Mbps para tráfego SSL Inspection;

4.5.3.1.2.1.12. Possuir throughput mínimo de 850 Mbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

4.5.3.1.2.1.13. Possuir no mínimo 4 (quatro) interfaces de rede Gigabit Ethernet 10/100/1000/2500 Mbps com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis ou seja, não será aceito equipamento com porta do tipo switch;

4.5.3.1.2.1.14. Possuir dispositivo de armazenamento interno de no mínimo 64 GB padrão SSD e deve suportar expansão futura para, no mínimo, 120 GB;

4.5.3.1.2.1.15. Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento;

4.5.3.1.2.1.16. Possuir pelo menos 1 (uma) porta USB para conexão de dispositivos externos;

4.5.3.1.2.1.17. A interface USB deve suportar o uso de modem 3G/4G/LTE e/ou possuir modem interno 3G/4G/LTE para conexão de link de Internet. O módulo deverá estar incluso no valor do equipamento;

4.5.3.1.3. **Appliance NGFW de 11.8 Gbps de Capacidade de Firewall**

4.5.3.1.3.1. **Características do Hardware**

4.5.3.1.3.1.1. O equipamento deve se instalar em mesa ocupando no máximo 1U (44,45mm) da referida mesa;

4.5.3.1.3.1.2. Dispor de fonte de alimentação com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;

4.5.3.1.3.1.3. Deverão ser fornecidos todos os cabos de energia, serial (RS-232/RJ45) ou similar, para instalação e funcionamento do dispositivo;

4.5.3.1.3.1.4. Possuir led indicador on/off, disco e devices de rede;

4.5.3.1.3.1.5. Possuir throughput mínimo de 11.8 Gbps para tráfego UDP;

4.5.3.1.3.1.6. Suportar no mínimo 7.000.000 (sete milhões) conexões simultâneas;

4.5.3.1.3.1.7. Suportar no mínimo 52.000 (cinquenta e duas mil) novas conexões por segundo;

4.5.3.1.3.1.8. Possuir throughput mínimo de 1.5 Gbps para tráfego IPS/IDS;

4.5.3.1.3.1.9. Possuir throughput mínimo de 2.5 Gbps para tráfego VPN IPSEC com criptografia (AES-256);

4.5.3.1.3.1.10. Possuir throughput mínimo de 1.5 Gbps para tráfego VPN SSL com criptografia (AES-256);

4.5.3.1.3.1.11. Possuir throughput mínimo de 900 Mbps para tráfego SSL Inspection;

4.5.3.1.3.1.12. Possuir throughput mínimo de 1.0 Gbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

4.5.3.1.3.1.13. Possuir no mínimo 6 (seis) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

4.5.3.1.3.1.14. Possuir dispositivo de armazenamento interno de no mínimo 120 GB padrão SSD;

4.5.3.1.3.1.15. Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento;

4.5.3.1.3.1.16. Possuir pelo menos 1 (uma) porta USB para conexão de dispositivos externos;

4.5.3.1.3.1.17. A interface USB deve suportar o uso de modem 3G/4G/LTE e/ou possuir modem interno 3G/4G/LTE para conexão de link de Internet. O módulo deverá estar incluso no valor do equipamento;

4.5.3.1.4. **Appliance NGFW de 19.4 Gbps de Capacidade de Firewall**

4.5.3.1.4.1. **Características do Hardware**

4.5.3.1.4.1.1. Deverá ser entregue dois equipamentos idênticos para atender a funcionalidade de cluster;

4.5.3.1.4.1.2. O equipamento deve se instalar em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 1U (44,45mm) do referido rack;

4.5.3.1.4.1.3. Dispor de fonte de alimentação interna com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;

4.5.3.1.4.1.4. Possuir painel/led indicador on/off, disco e devices de rede;

4.5.3.1.4.1.5. Possuir throughput de no mínimo 19.4 Gbps para tráfego UDP;

4.5.3.1.4.1.6. Suportar no mínimo 8.200.000 (oito milhões e duzentas mil) conexões simultâneas;

4.5.3.1.4.1.7. Suportar no mínimo 65.000 (sessenta e cinco mil) novas conexões por segundo;

4.5.3.1.4.1.8. Possuir throughput mínimo de 3.0 Gbps para tráfego IPS/IDS;

4.5.3.1.4.1.9. Possuir throughput mínimo de 3.0 Gbps para tráfego VPN IPSEC com criptografia (AES-256);

4.5.3.1.4.1.10. Possuir throughput mínimo de 1.8 Gbps para tráfego VPN SSL com criptografia (AES-256);

4.5.3.1.4.1.11. Possuir throughput mínimo de 1.3 Gbps para tráfego SSL Inspection;

tório - 029/2025 | [illegible] .pdf (33/232) [illegible]

4.5.3.1.4.1.12. Possuir throughput mínimo de 2.5 Gbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

4.5.3.1.4.1.13. Possuir pelo menos 6 (seis) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

4.5.3.1.4.1.14. Possuir dispositivo de armazenamento interno de no mínimo 120 GB padrão SSD;

4.5.3.1.4.1.15. Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento;

4.5.3.1.4.1.16. Possuir no mínimo 1 (uma) porta USB para conexão de dispositivos externos;

4.5.3.1.4.1.17. A interface USB deve suportar o uso de modem 3G/4G/LTE e/ou possuir modem interno 3G/4G/LTE para conexão de link de Internet. O módulo deverá estar incluso no valor do equipamento;

4.5.3.2. **Especificações Gerais de Software NGFW Para Todos os Itens**

4.5.3.2.1. **Das Funcionalidades do Firewall, SD-Wan, VPN IPsec/SSL**

4.5.3.2.1.1. **Características Gerais**

4.5.3.2.1.1.1. Quaisquer licenças que forem entregues para atender aos recursos da solução especificado no termo de referência deverão ter seu vencimento de acordo com o período de contrato.

4.5.3.2.1.1.2. O desempenho e as interfaces solicitados deverão ser comprovados através de datasheet público na internet. Caso haja divergência entre métricas do mesmo datasheet, será aceito o valor de menor capacidade.

4.5.3.2.1.1.3. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

4.5.3.2.1.1.4. Todos os recursos listados neste termo de referência deverão ser suportado e estar disponíveis na versão mais atual do software fornecido;

4.5.3.2.1.1.5. Os desempenhos dos appliances ofertados devem ser mensurados através da metodologia baseada em proxy

(Proxy Based), não serão aceitos appliances mensurados somente no método baseado em fluxo (Flow Based);

4.5.3.2.1.1.6. Interface sendo em exclusivo ou em conjunto na linguagem português e/ou espanhol e/ou inglês;

4.5.3.2.1.1.7. Suportar notificação de vencimento da licença na janela de alertas com os dias restantes da data vencimento;

4.5.3.2.1.1.8. Suportar acesso à Web por HTTP e CLI por TELNET;

4.5.3.2.1.1.9. Permitir alterar a porta padrão para os acessos a interface de administração via HTTP, HTTPs e CLI;

4.5.3.2.1.1.10. Atualização de modo “offline”, onde pode ser baixado na base do fabricante e posteriormente fazer o upload do arquivo na solução.

4.5.3.2.1.1.11. Restore de Snapshot sem executar o Wizard e sem licenciamento;

4.5.3.2.1.1.12. A solução deve oferecer suporte ao NAT444 (CGNAT) ou funcionalidade que implemente a persistência no NAT de saída independente da porta de destino, de forma que o endereço IP e porta traduzidos para um determinado usuário se mantenham os mesmos nas novas sessões que cheguem com o mesmo endereçamento IP e porta de origem;

4.5.3.2.1.1.13. Suportar segundo fator de autenticação (2FA/MFA) via token / OTP (One Time Password);

4.5.3.2.1.1.14. Deve suportar sistemas virtuais;

4.5.3.2.1.1.15. 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 diferentemente;

4.5.3.2.1.1.16. Qualquer interface de rede do equipamento deverá ser utilizada como gerenciamento, ou seja, não deve haver nenhuma interface exclusiva para a função de gerenciamento;

4.5.3.2.1.1.17. O sistema deve permitir o acesso à interface de gerenciamento WEB por qualquer interface de rede configurada;

4.5.3.2.1.1.18. O software deverá ser fornecido em sua versão mais atualizada, não sendo permitido qualquer tipo de comprovação futura.

4.5.3.2.1.1.19. Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução.

4.5.3.2.1.1.20. Todos os recursos detalhados no termo de referência deverão ser providos por um único software.

4.5.3.2.1.1.21. Tanto os Gateways de Segurança bem como a Gerência Centralizada deverão suportar monitoramento através de SNMP v1, v2 e v3.

4.5.3.2.1.1.22. Deverá possuir uma janela para monitoramento do tráfego de rede com informações do throughput e da quantidade de conexões simultâneas;

4.5.3.2.1.1.23. A Solução deverá prover inspeção SSL:

4.5.3.2.1.1.24. Deve suportar cluster do tipo Failover (HA) com replicação da tabela de estado;

4.5.3.2.1.1.25. Suportar a utilização de um proxy para atualização do software e licenciamento e deverá permitir as seguintes opções de configuração:

a) Endereço do servidor;
b) Porta do servidor;
c) Usuário;
d) Senha;

4.5.3.2.1.1.26. Deverá permitir o monitoramento SNMP, no mínimo, dos seguintes itens:

a) Desempenho total (throughput);
b) Conexões simultâneas;
c) Usuários autenticados;
d) Serviços habilitados ou desabilitados;
e) Quantidade de endereços distribuídos pelo DHCP.

4.5.3.2.1.1.27. Deverá implementar a funcionalidade de "zero-touch" para sua primeira implementação ou substituição. Dessa forma, deverá ser possível provisionar a configuração do equipamento via sistema de gerenciamento centralizado, transformando a atividade em uma simples conexão física.

tório - 029/2025 | [illegible] (36/232) [illegible]

de equipamento, sem a necessidade de configurações individuais nos equipamentos;

4.5.3.2.1.1.28. A Solução deve permitir ao administrador associar na solução de gerenciamento centralizado o número de série dos equipamentos ao site onde será instalado, de maneira que ao se ativar um equipamento no site remoto, esse equipamento se conecte com a Sistema Central e receba a configuração;

4.5.3.2.1.1.29. Ao instalar um equipamento no site remoto, cabeá-lo e energizá-lo, ele deverá tentar localizar Sistema Central para receber a sua configuração, sem que seja necessária qualquer configuração via console local do equipamento;

4.5.3.2.1.1.30. Deverá possuir um painel centralizado para exportação e agendamento de relatórios e deverá permitir exportá-los nos formatos: HTML, PDF, CSV;

4.5.3.2.1.1.31. Implementar protocolo de coleta de informações de fluxos que circulam pelo equipamento, como Netflow v5, v9 e v10 (IPFIX):

4.5.3.2.1.1.32. Os módulos de IPS, SD-WAN, Controle de aplicativos, Proxy WEB e Antimalware devem ser disponibilizados em perfis e estes devem ser inseridos em uma única política;

4.5.3.2.1.1.33. Deve implementar o protocolo ECMP;

4.5.3.2.1.1.34. O sistema deverá implementar otimização de fluxos TCP em conjunto com mecanismo para evitar retransmissão ou implementar métodos de correção de erros que permitam a unidade receptora recuperar pacotes que venham a ser perdidos na transmissão.

4.5.3.2.1.1.35. Deve possuir suporte ao protocolo de encapsulamento de redes MPLS;

4.5.3.2.1.1.36. Esta condição deve permitir conectar links MPLS diretamente no equipamento sem a necessidade de estar plugado a um segundo roteador/dispositivo.

4.5.3.2.1.1.37. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;

4.5.3.2.1.1.38. 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;

4.5.3.2.1.2. **Recursos Gerais de Firewall**

4.5.3.2.1.2.1. Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas;

4.5.3.2.1.2.2. Possuir um sistema de armazenamento remoto para salvar backups da solução com suporte a conexões utilizando os protocolos Network File System (NFS), SSH e que permita salvar em dispositivo USB conectado localmente;

4.5.3.2.1.2.3. Possibilitar a visualização dos países de origem e destino nos logs de eventos, de acessos e ameaças.

4.5.3.2.1.2.4. Possuir mecanismo que permita a realização de cópias de segurança (backups) do sistema e restauração remota, através da interface gráfica, a solução deve permitir o agendamento diário ou semanal;

4.5.3.2.1.2.5. O sistema deve permitir configurar o período ou número de cópias que deseja manter no repositório remoto e executar a manutenção de período automaticamente.

4.5.3.2.1.2.6. As cópias de segurança devem ser salvas compactadas e criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;

4.5.3.2.1.2.7. O sistema ainda deve contemplar um recurso de cópia de segurança do tipo snapshot, que contemple a cópia completa das configurações dos serviços e recursos do sistema;

4.5.3.2.1.2.8. Deve possibilitar a restauração do snapshot através da interface web de qualquer ponto remoto, de modo a contribuir para uma restauração imediata sem a necessidade de reinicialização do sistema;

4.5.3.2.1.2.9. Deve permitir habilitar ou desabilitar o registro de log por política de firewall.

4.5.3.2.1.2.10. Possuir controle de acesso à internet por endereço IP de origem e destino;

4.5.3.2.1.2.11. Possuir controle de acesso à internet por sub-rede;

4.5.3.2.1.2.12. Possuir suporte a tags de VLAN (802.1q);

4.5.3.2.1.2.13. Suportar agregação de links, segundo padrão IEEE 802.3ad.

tório - 029/2025 | [illegible] (38/232) [illegible]

4.5.3.2.1.2.14. Possuir ferramenta de diagnóstico do tipo tcpdump;

4.5.3.2.1.2.15. Possuir integração com Servidores de Autenticação RADIUS, TACACS+, LDAP e Microsoft Active Directory;

4.5.3.2.1.2.16. Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

4.5.3.2.1.2.17. Possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um, vários para vários e vários para um.

4.5.3.2.1.2.18. Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;

4.5.3.2.1.2.19. Permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br;

4.5.3.2.1.2.20. Possuir suporte a roteamento dinâmico RIP V1, V2, OSPFv2, OSPFv3, BGP e suportar duplicação de pacotes;

4.5.3.2.1.2.21. Possuir funcionalidades de DHCP Cliente, Servidor e Relay;

4.5.3.2.1.2.22. Deve ser possível configurar um servidor RADIUS para a validação de usuários;

4.5.3.2.1.2.23. A solução deve consultar o Servidor Radius integrado, caso o Servidor Radius autorize, o NGFW deve entregar endereço IP do range; caso contrário, não fornece endereço IP e a máquina não recebe o endereço, ficando sem acesso à rede.

4.5.3.2.1.2.24. Deverá suportar aplicações multimídia como: H.323, SIP;

4.5.3.2.1.2.25. Possuir tecnologia de firewall do tipo Stateful;

4.5.3.2.1.2.26. Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo-passivo;

4.5.3.2.1.2.27. Permitir o funcionamento em modo transparente tipo "bridge";

4.5.3.2.1.2.28. Permitir a criação de mínimo 4090 VLANS no padrão IEEE 802.1q por interface de rede;

4.5.3.2.1.2.29. Possuir conexão entre estação de gerência e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando);

4.5.3.2.1.2.30. Deverá suportar forwarding de multicast;

4.5.3.2.1.2.31. Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP;

4.5.3.2.1.2.32. Permitir o agrupamento de serviços;

4.5.3.2.1.2.33. Possuir mecanismo de anti-spoofing;

4.5.3.2.1.2.34. Possuir a funcionalidade de balanceamento e contingência de links;

4.5.3.2.1.2.35. Possibilitar a configuração dos timeouts de resposta dos protocolos de conexão, devendo suportar no mínimo a definição das opções do timeout padrão do ICMP, estabelecimento do TCP, envio do SYN em sessões TCP.

4.5.3.2.1.2.36. Permitir a configuração de regras de entrada baseado em zona de rede, possibilitando habilitar recursos de autenticação e restrição por origem baseado em IP.

4.5.3.2.1.2.37. Deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas, suportando ao menos: Yahoo! Messenger, MSN Messenger, ICQ, Telegram, Whatsapp, WeChat, Snapchat BitTorrent, UTorrent, Vuze, eDonkey, GNUTella, Skype e Microsoft Teams.

4.5.3.2.1.2.38. A solução deverá suportar nativamente o recurso SIMET (nic.br) medidor de Internet.

4.5.3.2.1.3. **Política de Segurança**

4.5.3.2.1.3.1. Permitir limitar a quantidade máxima de pacotes por segundo no Firewall, evitando ataques distribuídos ou anomalias de tráfego causadas por possíveis malwares na rede;

4.5.3.2.1.3.2. A configuração de proteção DOS deve estar disponível para habilitar em modo global e por política de segurança;

4.5.3.2.1.3.3. Possuir recurso de validação das políticas de segurança para identificar regras duplicadas ou que se ofusquem;

4.5.3.2.1.3.4. Possui uma única janela de configuração de política de segurança onde seja possível inserir os perfis de Proxy WEB, IPS, APP control, SD-WAN e ATP.

4.5.3.2.1.3.5. Deverá permitir implementar filtros de IPS, WEB Filter, Threat Protection, SSL Inpection, Application Control, assim como definir roteamento de aplicativos por SD-Wan, limitação de taxa de DOS por pacotes em uma única política.

4.5.3.2.1.3.6. Exibir na própria política a visualização de quais módulos estão habilitados, sem que seja necessário a edição da regra de proteção.

4.5.3.2.1.3.7. Possibilitar a edição de objetos vinculados, sem a necessidade de recriar a política.

4.5.3.2.1.3.8. Possibilitar a duplicação de uma política, otimizando tempo de configuração;

4.5.3.2.1.4. **Identificação de Usuário**

4.5.3.2.1.4.1. Deve possuir a capacidade de criação de políticas de acesso de Firewall, VPN, IPS e Controle de aplicação integradas ao repositório de usuários sendo: Active Directory, LDAP, TACAC´S e Radius;

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

4.5.3.2.1.4.3. Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador (Captive Portal), sem a necessidade de agente;

4.5.3.2.1.4.4. Deve possuir Captive Portal com suporte a Autenticação Social (Facebook, Twitter, Google);

4.5.3.2.1.4.5. A solução deverá ser capaz de identificar nome do usuário, login, máquina/computador registrados no Microsoft Active Directory;

4.5.3.2.1.4.6. Para o sistema de controles no serviço de autenticação o produto deve possuir, no mínimo, as seguintes condições para o Controle de Autenticação:

a) Usuários e Grupos de Usuários;

b) Datas (Objetos de Datas)

c) Horários (Objetos de Horário)

d) Lista de palavras chave ou conjunto de combinações de expressões regulares, (Objetos de Dicionários)

e) Endereços Remotos (Objetos de IPv4 e IPv6)

f) Zona de Rede (Múltiplas Zonas)

4.5.3.2.1.4.7. A solução deve suportar autenticação por SSO utilizando WMI (Windows Management Instrument), ou seja, não deve ser necessário instalar nenhum agente no servidor de autenticação.

4.5.3.2.1.4.8. A solução deve suportar o sincronismo entre vários NGFW em relação a replicação das sessões autenticadas da filial (Branch) na matriz (Head Office) e vice-versa, sem a necessidade de agentes externos.

4.5.3.2.1.4.9. A solução deverá suportar múltiplos Servidores de Autenticação (MS AD e/ou Ldap) atuando no modo failover;

4.5.3.2.1.5. **Das Funcionalidades Da Vpn:**

4.5.3.2.1.5.1. VPN baseada em appliance;

4.5.3.2.1.5.2. Possuir algoritmos de criptografia para túneis VPN: AES, 3DES;

4.5.3.2.1.5.3. Suporte a certificados PKI X.509 para construção de VPNs;

4.5.3.2.1.5.4. Possuir suporte a VPNs IPSec site-to-site:

4.5.3.2.1.5.5. Criptografia, 3DES, AES128, AES256, AES-GCM-128

4.5.3.2.1.5.6. Integridade MD5, SHA-1, SHA-256, SHA384 e AES-XCBC;

4.5.3.2.1.5.7. Algoritmo Internet Key Exchange (IKE) versões I e II;

4.5.3.2.1.5.8. AES 128 e 256 (Advanced Encryption Standard);

4.5.3.2.1.5.9. Suporte a Diffie-Hellman Grupo 1, Grupo 2, Grupo 5, Grupo 14; Grupo 15, Grupo 16, Grupo 17, Grupo 18, Grupo 19, Grupo 20, Grupo 21, Grupo 22, Grupo 23, Grupo 24, Grupo 25, Grupo 26, Grupo 27, Grupo 28, Grupo 29, Grupo 30, Grupo 31, Grupo 32;

4.5.3.2.1.5.10. Possuir suporte a VPN SSL;

4.5.3.2.1.5.11. Possuir capacidade de realizar SSL VPNs utilizando certificados digitais;

4.5.3.2.1.5.12. Suportar VPN SSL Clientless, sem a necessidade de utilização de Java, no mínimo, para os serviços abaixo:

a) RDP;
b) VNC;
c) SSH;
d) WEB;

e) SMB.

4.5.3.2.1.5.13. Deve permitir a arquitetura de vpn hub and spoke;

4.5.3.2.1.5.14. Suporte a VPNs IPSec client-to-site;

4.5.3.2.1.5.15. Deverá possuir cliente próprio para Windows para o estabelecimento da VPN client-to-site.

4.5.3.2.1.5.16. Suporte à inclusão em autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol);

4.5.3.2.1.5.17. Possuir funcionalidades de Auto-Discovery VPN capaz de permitir criar tuneis de VPN dinâmicos entre múltiplos dispositivos (spokes) com um gateway centralizador (hub).;

4.5.3.2.1.5.18. A funcionalidade de AD-VPN deve suportar criar os seguintes tipos de tuneis:

a) Site-to-Site;

b) Full-Mesh;

c) Star.

4.5.3.2.1.5.19. Suportar configuração VTI (virtual interface) na configuração de túneis VPN site-to-site com BGP (Border Gateway Protocol). Os túneis são utilizados para prover uma comunicação criptografada e encapsulada, por rotas, entre o peer (NGFW local) e o host;

4.5.3.2.1.5.20. A solução poderá atuar como cliente de tuneis VPN IPSec com suporte à autenticação XAuth/PSK e/ou XAuth/RSA.

4.5.3.2.1.5.21. A VPN client-to-site deve suportar o estabelecimento automático da VPN nos protocolos ICMP ou DNS (53/UDP), caso o cliente remoto identifique que a porta padrão está sendo bloqueada;

4.5.3.2.1.5.22. Possuir recurso para configurar vários túneis simultâneos de VPN cliente-to-site, com o objetivo de aumentar o desempenho do tráfego;

4.5.3.2.1.5.23. Suportar segundo fator de autenticação (2FA/MFA) via token / OTP (One Time Password);

4.5.3.2.1.6. **SD-WAN:**

4.5.3.2.1.6.1. Entende-se como tecnologia SD-WAN (Software-Defined WAN) a rede de área ampla definida por software que centraliza a gerência da rede WAN em uma console única, eliminando a necessidade de intervenções manuais em roteadores em localidades remotas, proporcionando visibilidade do tráfego, seleção de caminho dinâmico baseado em políticas de QoS, aplicação ou performance e utilização de túneis VPN para comunicação entre os sites remotos;

4.5.3.2.1.6.2. Possuir o balanceamento automático para conexões externas à internet através das interfaces físicas;

4.5.3.2.1.6.3. Suportar modo de duplicação de pacotes de dados pelo links WAN, para que em caso de queda do link principal, possa ser enviado ao link secundário uma cópia do pacote de dados perdido permitindo assim a maior integridade e disponibilidade do tráfego;

4.5.3.2.1.6.4. Permitir utilizar VPN IPsec para interligar unidades remotas;

4.5.3.2.1.6.5. Possuir recurso de "persistência de link" para impedir a queda de conexões em aplicações que não suportam o load balance de link;

4.5.3.2.1.6.6. O balanceamento deverá ser baseado em critérios de desempenho, devendo no mínimo, permitir verificar o monitoramento do consumo de banda, perda de pacotes, jitter e latência;

4.5.3.2.1.6.7. Deve possuir uma janela web ou dashboard capaz de fornecer informações dos eventos e com informações de monitoramento de desempenho relacionado ao recurso SD-WAN;

4.5.3.2.1.6.8. O recurso de SD-WAN deverá suportar o roteamento de tráfego por política baseado em aplicação;

4.5.3.2.1.6.9. O appliance SD-WAN deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link monitorado recuperado seja avaliado. Deve suportar especificar um valor variando de 1 a 100.

4.5.3.2.1.6.10. O recurso de SD-WAN deverá permitir o monitoramento de, no mínimo 03 (três) endereços alvos para verificar a disponibilidade e desempenho do link;

4.5.3.2.1.6.11. A solução de SD-WAN NGFW deve permitir a configuração da funcionalidade de SD-WAN em qualquer interface WAN de forma agnóstica, independente se é internet, 3G/4G/LTE, entre outras;

4.5.3.2.1.6.12. A solução deverá suportar os seguintes métodos de seleção de link:

a) Failover;

b) Load Balance;

c) Spillover;

d) Dynamic Selection;

4.5.3.2.1.6.13. Deverá oferecer um monitor capaz de prover em tempo real as seguintes informações em uma única janela:

a) Consumo de banda;

b) Perda de pacotes;

c) Jitter;

d) Latência.

4.5.3.2.1.6.14. A Solução de SD-WAN deve desempenhar a função de Packet Duplication (PD) permitindo encaminhar o pacote por mais de um circuito para em casos de falhas não haver retransmissão;

4.5.3.2.1.7. **Das Funcionalidades de QoS**

4.5.3.2.1.7.1. Adotar solução de Qualidade de Serviço baseada em appliance;

4.5.3.2.1.7.2. Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;

4.5.3.2.1.7.3. Permitir modificação de valores DSCP;

4.5.3.2.1.7.4. Limitar individualmente a banda utilizada por programas de compartilhamento de arquivos do tipo peer-to-peer;

4.5.3.2.1.7.5. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

4.5.3.2.1.7.6. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;

4.5.3.2.1.7.7. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;

4.5.3.2.1.7.8. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino;

4.5.3.2.1.7.9. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

4.5.3.2.1.8. **Alta Disponibilidade**

4.5.3.2.1.8.1. Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Standby, com as implementações de Fail Over.

4.5.3.2.1.8.2. O Sincronismo dos servidores deve ser por interface exclusiva de Heartbeat;

4.5.3.2.1.8.3. No caso de falha do H.A. Ativo Primário, o H.A. Ativo secundário deve assumir de uma forma transparente sem impacto ao usuário ou perda de serviço;

4.5.3.2.1.8.4. Deverá suportar a persistências de sessão de usuarios e conexões estabelecidas, entre os membros da Alta Disponibilidade;

4.5.3.2.2. **Das Funcionalidades de Controle de Aplicação e Web Proxy**

4.5.3.2.2.1. **Controle de Aplicações**

4.5.3.2.2.1.1. As funcionalidades abaixo devem ser baseadas em appliance;

4.5.3.2.2.1.2. Deverá reconhecer no mínimo 4000 aplicações;

4.5.3.2.2.1.3. Deverá possuir, no mínimo, 19 categorias para classificação de aplicações;

4.5.3.2.2.1.4. Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações como:

a) P2P;
b) Web;
c) Transferência de arquivos;
d) Social;

4.5.3.2.2.1.5. Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;

4.5.3.2.2.1.6. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

4.5.3.2.2.1.7. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

4.5.3.2.2.1.8. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;

4.5.3.2.2.1.9. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;

4.5.3.2.2.1.10. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

4.5.3.2.2.1.11. Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino;

4.5.3.2.2.1.12. Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.

4.5.3.2.2.2. **Filtro de Conteúdo Web**

4.5.3.2.2.2.1. Possuir solução de filtro de conteúdo web integrado a solução de segurança

4.5.3.2.2.2.2. Possuir pelo menos 80 categorias para classificação de sites web

4.5.3.2.2.2.3. Possuir base mínima contendo, 48 milhões de sites internet web já registrados e classificados;

4.5.3.2.2.2.4. Possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites web como:

a) Webmail;
b) Instituições de Saúde;
c) Notícias;
d) Pornografia;
e) Restaurante;
f) Mídias Sociais;
g) Esporte;
h) Educação;
i) Games;
j) Compras;

4.5.3.2.2.2.5. Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

4.5.3.2.2.2.6. Possuir sistema de cache interno, armazenando requisições WEB em disco local e memória;

4.5.3.2.2.2.7. Deve permitir a definição do tamanho mínimo dos objetos salvos em cache no disco;

4.5.3.2.2.2.8. Deve permitir a definição do tamanho máximo dos objetos salvos em cache em memória;

4.5.3.2.2.2.9. Deve atender a estrutura de navegação através de hierarquia de proxy com e sem autenticação;

4.5.3.2.2.2.10. Possibilitar a integração com servidores de cache WEB externos;

4.5.3.2.2.2.11. Deve ser capaz de armazenar cache dinâmicos para as atualizações Microsoft Windows Update, Youtube, Sourceforge Downloads, Facebook, Google Maps;

4.5.3.2.2.2.12. Deve possuir a capacidade de excluir URL's específicas do cache web, configurável por listas de palavras chaves com suporte inclusive a expressões regulares;

4.5.3.2.2.2.13. Integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;

4.5.3.2.2.2.14. Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory, LDAP , TACACS+ e Radius;

4.5.3.2.2.2.15. Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança da contratante;

4.5.3.2.2.2.16. Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;

4.5.3.2.2.2.17. Deverá permitir o bloqueio de URLs inválidas cujo campo CN do certificado SSL não contém um domínio válido;

4.5.3.2.2.2.18. Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web;

4.5.3.2.2.2.19. Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;

4.5.3.2.2.2.20. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

4.5.3.2.2.2.21. Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem;

4.5.3.2.2.2.22. Possuir Logs e Relatórios de tempo de navegação de sites web - Domínios Web;

4.5.3.2.2.2.23. Possuir recurso capaz de controlar e restringir o acesso a sites com base em seus nomes de domínio, conhecido como DNS Content Filter;

4.5.3.2.2.3. **Recursos do Proxy**

4.5.3.2.2.3.1. Deverá funcionar em modo Proxy Explícito para HTTP, HTTPS, FTP, POP3 e SMTP e em Proxy Transparente;

4.5.3.2.2.3.2. A solução deve ser capaz de identificar o comportamento do protocolo SSH onde pode ser feito através da inspeção do protocolo;

4.5.3.2.2.3.3. Deverá permitir configurar a porta do Proxy Explícito;

4.5.3.2.2.3.4. O equipamento deverá poder suportar funcionalidades de antispam sem a necessidade de equipamento dedicado.

4.5.3.2.3. **Das Funcionalidades da Detecção de Intrusão e ATP**

4.5.3.2.3.1. **Das Funcionalidades da Detecção de Intrusão**

4.5.3.2.3.1.1. A Detecção de Intrusão deverá ser baseada em appliance:

4.5.3.2.3.1.2. Possuir no mínimo 82.000 (oitenta e duas mil) assinaturas ou regras de IPS/IDS;

4.5.3.2.3.1.3. Permitir a criação de assinaturas customizadas pelo administrador do NGFW;

4.5.3.2.3.1.4. O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;

4.5.3.2.3.1.5. Possuir tecnologia de detecção baseada em assinatura;

4.5.3.2.3.1.6. Deverá suportar a implantação em modo Gateway, inline e em modo sniffer;

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

4.5.3.2.3.1.8. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação.

4.5.3.2.3.1.9. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos.

4.5.3.2.3.1.10. Possuir opção para administrador as listas de Blacklist, Whitelist e Quarentena com suporte a endereços IPv6.

4.5.3.2.3.1.11. Possuir capacidade de remontagem de pacotes para identificação de ataques;

4.5.3.2.3.1.12. Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque; Exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de Servidores Web;

4.5.3.2.3.1.13. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;

4.5.3.2.3.1.14. Mecanismos de detecção/proteção de ataques;

4.5.3.2.3.1.15. Reconhecimento de padrões;

4.5.3.2.3.1.16. Análise de protocolos;

4.5.3.2.3.1.17. Detecção de anomalias;

4.5.3.2.3.1.18. Detecção de ataques de RPC (Remote procedure call);

4.5.3.2.3.1.19. Proteção contra-ataques de Windows ou NetBios;

4.5.3.2.3.1.20. Proteção contra-ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);

4.5.3.2.3.1.21. Proteção contra-ataques DNS (Domain Name System);

4.5.3.2.3.1.22. Proteção contra-ataques a FTP, SSH , Telnet e rlogin;

4.5.3.2.3.1.23. Proteção contra-ataques de ICMP (Internet Control Message Protocol);

4.5.3.2.3.1.24. Alarmes na console de administração;

4.5.3.2.3.1.25. Alertas via correio eletrônico;

4.5.3.2.3.1.26. Monitoração do comportamento do appliance através de SNMP, o dispositivo deverá ser capaz de enviar traps de

SNMP quando ocorrer um evento relevante para a correta operação da rede;

4.5.3.2.3.1.27. Capacidade de resposta/logs ativa a ataques;

4.5.3.2.3.1.28. Terminação de sessões via TCP resets;

4.5.3.2.3.1.29. Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;

4.5.3.2.3.1.30. O Sistema de detecção de Intrusos deverá atenuar os efeitos dos ataques de negação de serviços;

4.5.3.2.3.1.31. Possuir filtros de ataques por anomalias;

4.5.3.2.3.1.32. Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;

4.5.3.2.3.1.33. Permitir filtros de anomalias de protocolos;

4.5.3.2.3.1.34. Suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;

4.5.3.2.3.1.35. Suportar verificação de ataque nas camadas de aplicação;

4.5.3.2.3.2. **Das Funcionalidades Do Threat Protection**

4.5.3.2.3.2.1. Possuir funções de Antivírus, Anti-spyware;

4.5.3.2.3.2.2. Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, POP3, SMB/CIFS e FTP;

4.5.3.2.3.2.3. Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.)

4.5.3.2.3.2.4. Permitir o bloqueio de download de arquivos por extensão e tipo de arquivo;

4.5.3.2.4. **Solução de Gerenciamento Centralizado de Firewall**

4.5.3.2.4.1. **Funcionalidades de Gerenciamento**

4.5.3.2.4.1.1. Como boa prática de segurança e de mercado, a solução de gerência deverá ser separada do gateway de segurança, onde irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste projeto;

4.5.3.2.4.1.2. A solução de gerenciamento centralizado deve possibilitar o gerenciamento de todos os Firewall contratados.

4.5.3.2.4.1.3. A solução de gerenciamento centralizado deverá ser do mesmo fabricante da solução de segurança.

4.5.3.2.4.1.4. O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance físico deve ser compatível com rack 19 polegadas e possuir todos os acessórios necessários para sua instalação. Caso seja entregue em appliance virtual, deverá ser compatível com VMware ESXi e todo custo da infraestrutura necessária para suportar o appliance virtual é responsabilidade da CONTRATANTE;

4.5.3.2.4.1.5. Centralizar a administração de regras e políticas do(s) cluster(s), usando uma única interface de gerenciamento;

4.5.3.2.4.1.6. A solução deverá permitir seu gerenciamento por: CLI (Command Line Interface) via SSH, Web GUI utilizando protocolo HTTPS ou console gráfica;

4.5.3.2.4.1.7. Deve manter um canal de comunicação segura, com encriptação baseada em certificados, entre todos os componentes que fazem parte da solução de firewall, gerência, armazenamento de logs e emissão de relatórios;

4.5.3.2.4.1.8. A solução deve incluir a opção de segmentar a base de regra utilizando rótulos ou títulos de seção para organizar melhor a política facilitando a localização e gestão do administrador;

4.5.3.2.4.1.9. A solução de gerência deverá prover fácil administração na aplicação das políticas para os gateways, sendo capaz de realizar o processo de alteração de regras e configuração de todas as soluções de segurança, que pode ser aplicada nos gateways remotos em uma única sessão, evitando qualquer tipo de retrabalho.

4.5.3.2.4.1.10. Deve possibilitar a realização de “backup” e restauração de dados.

4.5.3.2.4.1.11. Deve possibilitar a gerência de “logs”, realizando as configurações de relatórios de todos os “firewalls” integrados.

4.5.3.2.4.1.12. Deve permitir buscas e realizar análise de usuários e grupos, rastreando toda a sua atividade e uso da internet.

4.5.3.2.4.1.13. O gerenciamento deve permitir/possuir:

4.5.3.2.4.1.14. Criação e administração de políticas de Firewall, Controle de aplicação e IPS, Antivírus e Anti-Malware, Filtro de URL e prevenção contra ameaças avançadas;

4.5.3.2.4.1.15. Monitoração de logs;

4.5.3.2.4.1.16. Debugging;

4.5.3.2.4.1.17. Deve permitir usar palavras chaves para facilitar identificação de regras;

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

4.5.3.2.4.1.19. Autenticação integrada à base de dados local;

4.5.3.2.4.1.20. Deve possuir ferramenta para localização de objetos (por exemplo: endereço IP, Range de IP, subrede) na base de regras;

4.5.3.2.4.1.21. Criação de regras que fiquem ativas em horário definido;

4.5.3.2.4.1.22. Habilidade de upgrade via interface de gerenciamento;

4.5.3.2.4.1.23. Deverá ter a capacidade de gerar um relatório gráfico, que permita visualizar as mudanças na utilização de aplicações na rede, no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações, no tempo presente com relação ao passado;

4.5.3.2.4.1.24. Controle sobre todos os equipamentos da plataforma de proteção em uma única console, com administração de privilégios e funções;

4.5.3.2.4.1.25. Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de proteção;

4.5.3.2.4.1.26. Deve permitir a criação de objetos e políticas compartilhadas;

4.5.3.2.4.1.27. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

4.5.3.2.4.1.28. Solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

4.5.3.2.4.1.29. A solução deve permitir gerenciar templates de customização visual e marca do produto pelo sistema de gerenciamento centralizado e permitir aplicar nos NGFW´s gerenciados. Portanto, deve ser possível customizar a interface gráfica nos seguintes itens:

a) Título da Página;
b) Ícone (favicon);
c) Logotipo;
d) Imagem de fundo;
e) Cores do menu (primária e secundária);

4.5.3.2.4.1.30. O sistema deve ser capaz de gerenciar de modo central as políticas de backup do equipamento remotos;

4.5.3.2.4.1.31. O sistema deve permitir habilitar uma mensagem de Disclaimer na página de login da Interface de Administração. Ou seja, a página de login deverá apresentar um banner com uma mensagem customizada pelo administrador. Essa mensagem poderá ser utilizada para avisos de políticas de uso e compliance do sistema.

4.5.3.2.4.1.32. Deve suportar sistema de cluster do tipo Alta Disponibilidade para a solução ofertada;

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

4.5.3.2.4.1.34. Deve permitir inserir uma notificação do tipo "Login Disclaimer" que deve ser exibida na página de login da Interface de Administração da solução de gerenciamento centralizado.

4.5.3.2.4.1.35. Suportar API para integração com sistemas de terceiros;

4.5.3.2.4.2. **Alta Disponibilidade**

4.5.3.2.4.2.1. Deve suportar recurso de Alta-Disponibilidade (HA), sendo um primário e outros em modo secundário com sincronização e replicação das configurações;

4.5.3.2.4.2.2. O sistema de cluster deve suportar utilizar 02 (duas) interfaces como heatbeat;

4.5.3.2.4.2.3. Deve suportar definir o intervalo do sincronismo em minutos;

4.5.3.2.4.2.4. Permitir definir o número máximo de falhas dos testes do heartbeat e a solução somente irá convergir para o segundo equipamento após atingir o valor definido;

4.5.3.2.4.2.5. Suportar inserir um endereço de email para receber notificações relacionadas ao cluster.

4.5.3.2.4.3. **Armazenamento e Gerenciamento de Logs e Eventos**

4.5.3.2.4.3.1. A solução de armazenamento e gerenciamento de logs e eventos, deverá suportar, no mínimo, e estar licenciada para receber no mínimo 50GB de logs por dia;

4.5.3.2.4.3.2. A solução de armazenamento e gerenciamento de logs e eventos poderá ser entrega na mesma solução de gerenciamento centralizado, desde que atenda aos requisitos solicitados.

4.5.3.2.4.3.3. A solução de armazenamento e gerenciamento de logs e eventos deverá ser do mesmo fabricante da solução de segurança e compatível com a ferramenta de gerenciamento centralizado.

4.5.3.2.4.3.4. Deverá prover análise de tráfego de rede de modo centralizado;

4.5.3.2.4.3.5. Deve possuir análise de tráfego de rede e ameaças por geolocalização;

4.5.3.2.4.3.6. Deverá ser capaz de receber os logs e eventos com o objetivo de prover os seguintes tipos de análises:

4.5.3.2.4.3.7. Análise de ameaças e incidentes de segurança;

4.5.3.2.4.3.8. Análise de tráfego e uso de categorias Web;

4.5.3.2.4.3.9. Análise de tráfego e uso de aplicativos;

4.5.3.2.4.3.10. Análise de tráfego e ameaças por usuário;

4.5.3.2.4.3.11. Análise de desempenho de políticas de segurança;

4.5.3.2.4.3.12. A solução ofertada deve ser capaz de fazer o gerenciamento centralizado de logs, consolidação de logs, arquivamento de logs, busca avançada de logs;

4.5.3.2.4.3.13. Deverá possuir ferramenta para salvar consultas avançadas;

4.5.3.2.4.3.14. Deve possuir relatórios personalizados;

4.5.3.2.4.3.15. Deverá ser capaz de efetuar o arquivamento de relatórios;

4.5.3.2.4.3.16. Deve possuir agendamento de relatórios;

4.5.3.2.4.3.17. Os Relatórios deverão, no mínimo, serem exportados em formatos flexíveis (PDF, CSV);

4.5.3.2.4.3.18. Logs e Relatórios de tempo de navegação de sites web - Domínios Web;

4.5.3.2.4.3.19. Permitir o envio de relatórios por e-mail;

4.5.3.2.4.3.20. Relatório por Dispositivo/Consolidado;

4.5.3.2.5. **Tabela de Distribuição do Item 1, do Lote Único**

SUBITEM DO TR Nº	DESCRIÇÃO	QTDE
4.5.3.1.1	APPLIANCE NGFW DE 5 GBPS DE CAPACIDADE DE FIREWALL	157
4.5.3.1.2	APPLIANCE NGFW DE 9.7 GBPS DE CAPACIDADE DE FIREWALL	11
4.5.3.1.3	APPLIANCE NGFW DE 11.8 GBPS DE CAPACIDADE DE FIREWALL	3
4.5.3.1.4	APPLIANCE NGFW DE 19.4 GBPS DE CAPACIDADE DE FIREWALL	2
4.5.3.2.4	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE FIREWALL	1

4.5.3.3. **A solução de segurança cibernética de bloqueio de ameaças, conforme ITEM 2, do Lote Único, deve possuir as seguintes características:**

4.5.3.3.1. **Interface e Gestão:**

4.5.3.3.1.1. Deve ser instalado em equipamento com S.O. Linux, Unix ou BSD.

4.5.3.3.1.2. Deve ter uma interface amigável para configuração e gestão.

4.5.3.3.1.3. Não deve possuir endereçamento IP nas interfaces pelas quais passam o tráfego internet.

4.5.3.3.1.4. Não deve permitir a identificação da existência da solução.

4.5.3.3.1.5. Não ser suscetível à exploração externa de possíveis vulnerabilidades no software.

4.5.3.3.1.6. Deve permitir instalação de forma transparente, sem necessidade de alterações nas configurações lógicas de rede, IP ou do roteamento do ambiente atual.

4.5.3.3.1.7. Deve atuar diretamente no tráfego de entrada da internet.

4.5.3.3.1.8. Deve proporcionar proteção abrangente para toda a infraestrutura, desde o firewall podendo incluir os roteadores à internet.

4.5.3.3.1.9. O aumento de latência no tráfego de rede não deve ser superior a 5 milésimos de segundo.

4.5.3.3.1.10. Deve permitir comunicação com a internet através de proxy.

4.5.3.3.1.11. Deve possuir painel para configuração de mecanismo para detecção de acesso indesejado.

4.5.3.3.1.12. Deve possuir painel para configuração de origens confiáveis.

4.5.3.3.1.13. Deve possuir mecanismo de autoproteção.

4.5.3.3.1.14. Deve possuir log de auditoria de tudo que foi feito na solução, devendo no mínimo identificar user, data-hora e atividade realizada.

4.5.3.3.1.15. Deve armazenar no mínimo os últimos 8.000 registros de log de auditoria.

4.5.3.3.2. **Inteligência Artificial Avançada:**

4.5.3.3.2.1. Deve ser uma solução baseada em Inteligência Artificial Preditiva.

4.5.3.3.2.2. Deve ser capaz de analisar padrões de comportamento no tráfego de internet.

4.5.3.3.2.3. Deve identificar origens maliciosas e neutralizá-las imediatamente e automaticamente, sem intervenção humana.

4.5.3.3.2.4. A solução não deve depender de assinaturas para reconhecer tráfegos indesejados.

4.5.3.3.2.5. Deve criar uma blacklist local com as origens maliciosas.

4.5.3.3.2.6. Deve possuir mecanismo de gestão do tempo de guarda dos dados da blacklist.

4.5.3.3.2.7. Deve possuir capacidade de aprendizado de acessos indesejados.

4.5.3.3.3. **Taxa de Falso Positivo:**

4.5.3.3.3.1. Deve apresentar uma taxa de falso positivo inferior a 0,0001% (uma identificação errada a cada um milhão de identificações), garantindo precisão nas identificações e bloqueios.

4.5.3.3.4. **Proteção Contra Ataques de "Zero Day":**

4.5.3.3.4.1. Deve oferecer proteção eficaz contra ataques de "Zero Day", mesmo aqueles que ainda não tenham sido identificados e que ainda não possuam "assinatura de identificação" ou "patch de correção" dos fabricantes das outras soluções informáticas que o órgão disponibiliza na internet.

4.5.3.3.5. **Visibilidade:**

4.5.3.3.5.1. Deve fornecer visibilidade das origens maliciosas dos ataques.

4.5.3.3.5.2. Deve fornecer visibilidade das tentativas de acessos bloqueadas.

4.5.3.3.5.3. Deve fornecer visibilidade dos serviços de rede alvos de ataques.

4.5.3.3.5.4. Deve possuir funcionalidade que permita identificar de forma fácil e ágil o motivo do bloqueio do ataque.

4.5.3.3.5.5. Deve apresentar um dashboard para a equipe de monitoramento (SOC) com mapa dos países dos IPS atacantes.

4.5.3.3.5.6. Deve apresentar um dashboard para a equipe de monitoramento (SOC) com mapa dos países de onde foram gerados os ataques.

4.5.3.3.5.7. Deve permitir a consulta através de vários tipos de indicadores como por exemplo, IP de origem, IP de Destino, Porta de origem, Porta de destino entre outros.

4.5.3.3.5.8. Deve possuir funcionalidade de geolocalização de IP identificado como malicioso.

4.5.3.3.5.9. Deve possuir busca de CVEs na base do MITRE.

4.5.3.3.5.10. Deve possuir mecanismo de autogestão do armazenamento dos logs de ataque.

4.5.3.3.6. **Relatórios e Integrações:**

4.5.3.3.6.1. Deve permitir integração, através de API, com outros equipamentos/soluções de segurança como por exemplo firewall ou soluções de observabilidade.

4.5.3.3.6.2. Deve permitir envio dos logs de ataques para servidor externo.

4.5.3.3.6.3. Deve possuir integração com rede externa de Inteligência de Ameaças Global, com capacidade de aprendizado sobre novas ameaças identificadas exercendo atividade hacker recente pelo mundo e, de forma automática e pró-ativa, ativar proteção contra essas origens.

4.5.3.3.6.4. Deve gerar relatório gerencial mensal com pelo menos as seguintes informações: quantidade de ataques, bloqueios, origens mais frequentes, países de origem e serviços mais atacados.

4.5.3.3.6.5. Deve possuir capacidade suficiente para armazenar e disponibilizar consultas aos relatórios gerenciais mensais de pelo menos 5 anos.

4.5.3.3.6.6. Deve permitir exportar os relatórios para PDF.

4.5.3.3.7. **Especificações Técnicas do Equipamento**

4.5.3.3.7.1. **O equipamento físico deve atender aos seguintes requisitos:**

4.5.3.3.7.1.1. **Dimensões e Montagem:**

4.5.3.3.7.1.1.1. Deve ser compatível com rack de 19 polegadas, com tamanho de 1U ou 2U.

4.5.3.3.7.1.2. **Conectividade:**

4.5.3.3.7.1.2.1. Deve possuir no mínimo 8 interfaces de rede Gigabit Ethernet com conexão do tipo RJ45.

4.5.3.3.7.1.2.2. Deve ter porta console para configuração local.

4.5.3.3.7.1.2.3. Deve possuir interface de rede exclusiva para acesso e gerenciamento interno do equipamento.

4.5.3.3.7.1.3. **Alimentação elétrica:**

4.5.3.3.7.1.3.1. Deve ter fonte de alimentação elétrica VAC automática nos padrões brasileiros conforme a continuidade operacional.

4.5.3.4. **Os serviços e equipamentos do ITEM 3, do Lote Único, deverão ser entregues no formato e características técnicas bem como funcionalidades conforme especificações abaixo:**

4.5.3.4.1. O serviço de acesso à Internet compreenderá a instalação, operação, manutenção e gerenciamento da infraestrutura de acesso à Internet através de roteador PE, integrado imediatamente ao roteamento BGP da Operadora. Entende-se operadora, Provedor de Internet Autônomo, ou seja, que possua ASN (Autonomous System Number) vinculado a um CNPJ de um ISP distinto, ou seja, a CONTRATADA deverá suportar a operação através de dois link dedicado distintos, oriundo de 02(dois) ASN diferentes, através de infraestrutura de chegada ao prédio da Prefeitura percorrida por caminhos diferentes, visando a eventual queda de um dos link não haver impacto na operação como um todo.

4.5.3.4.2. Cada link deverá ser entregue com blocos IPV4 /29 e IPV6 /64, públicos, os quais serão cadastrados no portal numeração.br, compreendendo inicialmente banda de 500 Mbps mas a porta de rede não pode haver limite rate, devendo suportar os serviço em wire speed, pois eventual queda de um dos link, a operadora redundante deverá suportar o tráfego na integralidade.

4.5.3.4.3. Conforme topologia da rede, a CONTRATADA deverá entregar o link em duas portas distintas, uma porta conectada no equipamento de cibersegurança A e outra porta a ser conectada no equipamento de cibersegurança B. Tal feito se repetirá em cada ASN conforme topologia apresentada.

4.5.3.4.4. Em caso de falha no equipamento A, o serviço deverá realizar a migração automática para o equipamento redundante em regime de failover, sem necessidade de configurações adicionais ou intervenções técnicas. O mesmo procedimento deverá ocorrer em situação inversa. Caso este Termo de Referência não detalhe alguma instrução específica, caberá à CONTRATADA assegurar a entrega da solução em pleno funcionamento, incluindo todos os custos inerentes à implantação, sem qualquer cobrança adicional.

4.5.3.4.5. A CONTRATADA deverá fornecer todos os equipamentos, acessórios e demais componentes indispensáveis à disponibilização do serviço no local designado, ainda que não estejam expressamente mencionados neste Termo de Referência, desde que sejam essenciais à operação da solução ou ao cumprimento das funcionalidades e configurações exigidas, sem gerar ônus adicionais à CONTRATANTE.

tório - 029/2025 [illegible] (59/232) [illegible]

4.5.3.4.6. O acesso entre a operadora e o ambiente de TI da CONTRATANTE deverá ser feito exclusivamente por meio de fibra óptica da CONTRATADA.

4.5.3.4.7. Devem transportar pacotes IPv4 e IPv6 com no mínimo 1500 bytes sem exigir a fragmentação dos mesmos na camada 3 do modelo OSI.

4.5.3.4.8. Os links devem suportar IPv6, sendo necessário o fornecimento de endereçamento para as redes internas do CONTRATANTE.

4.5.3.4.9. Deverão ser fornecidos 1 (roteador) por link dedicado que irá compor o ambiente de alta disponibilidade.

4.5.3.4.10. Deverá suportar todos os protocolos de roteamento necessários para suportar as conexões WANs em ambiente de alta disponibilidade (OSPF, BGP, RIP etc).

4.5.3.4.11. Cada equipamento deve possuir no mínimo 2 (duas) interfaces WAN de 1 Gbps e 2 (duas) ou mais interfaces LAN de 1 Gbps.

4.5.3.4.12. Possuir LEDs de diagnóstico sobre alimentação, atividade e diagnóstico das portas.

4.5.3.4.13. Deve possuir funcionalidades necessárias para monitoramento, diagnóstico e features como QoS, permitir a atualização remota do SO e arquivos de configuração via ethernet ou serial, FTP e TFTP; Permitir a gravação de log externo via syslog; Suportar o recurso port mirroring para um endereço IP; e suportar protocolo de coleta de tráfego Netflow ou IPFIX para a realização de coleta de informações de fluxo, tráfego que circulam no equipamento.

4.5.3.5. **Os serviços e equipamentos dos ITENS 4 e 5 deverão ser entregues no formato e características técnicas bem como funcionalidades conforme especificações abaixo:**

4.5.3.5.1. As velocidades de acesso à internet contratadas serão classificadas da seguinte maneira:

4.5.3.5.1.1. Link principal (item 4, do Lote Único): 150Mbps

4.5.3.5.1.2. Link redundante (item 5, do Lote Único): 75Mbps

4.5.3.5.1.2.1. A CONTRATADA deverá comprovar que possui capacidade de operar com dois circuitos distintos, em fibra óptica.

4.5.3.5.1.2.2. A CONTRATADA deverá comprovar que possui capacidade operacional através de redes espectrais.

4.5.3.5.2. A CONTRATADA deverá garantir largura de banda simétrica (download/upload) de 100% da velocidade contratada, em link único para o link principal (Item 4, do Lote Único), não sendo aceita a agregação de múltiplos links para atingir a velocidade contratada.

4.5.3.5.3. A CONTRATADA deverá garantir largura de banda simétrica (download/upload) de pelo menos 70% da velocidade contratada, podendo ser em 02(dois) link (Item 4, do Lote Único), um link performando em fibra óptica e outro através de chip especial para suportar esta operação estruturante, não sendo possível chip de dados convencionais.

tório - 029/2025 | [illegible] (60/233)

com limite de dados. Neste caso específico será aceito a agregação desses 2 link em comento, para atingir a velocidade contratada.

4.5.3.5.4. A localização e classificação de cada unidade está relacionada nos itens 7.2.1.3.1, 7.2.1.3.2 e 7.2.1.3.3.

4.5.3.5.5. O acesso de fibra óptica até o ambiente de TI da CONTRATANTE deverá ser feito exclusivamente por meio de fibra óptica da CONTRATADA, exceto chip 4/5Gbps.

4.5.3.5.6. Cada acesso de fibra óptica ao ambiente de TI deve ser percorrido por caminhos distintos; não serão aceitos acessos de redes convergindo para um mesmo ISP, sendo necessária a validação de comprovação deste quesito no momento do certame.

4.5.3.6. **Requisitos Tecnológicos Mínimos Para Suportar a Conectividade das Praças**

4.5.3.6.1. **Ponto de Acesso Outdoor Wi-Fi 6 2x2**

4.5.3.6.1.1. **Conectividade:**

4.5.3.6.1.1.1. Deve possuir, no mínimo, 1 porta uplink ethernet 100/1000/2.5G Base-T em conector RJ45 com suporte a alimentação PoE compatível com o padrão IEEE 802.3at e com reconhecimento automático de crossover MDI/MDIX;

4.5.3.6.1.1.2. Deve possuir 1 porta LAN ethernet 100/1000Base-T em conector RJ45 e com reconhecimento automático de crossover MDI/MDIX;

4.5.3.6.1.1.3. Possuir porta de console para gerenciamento e configuração via linha de comando (CLI – command line interface) com conector RJ-45 diferente da porta de rede solicitada anteriormente;

4.5.3.6.1.1.4. Deve possuir 2 rádios operando nas frequências de 2,4GHz e 5GHz simultaneamente;

4.5.3.6.1.1.5. Deve possuir rádio Bluetooth Low-Energy (BLE) integrado ao equipamento;

4.5.3.6.1.1.6. Deve possuir antenas omnidirecionais internas ao equipamento com ganho mínimo de 5 dBi na frequência de 2,4GHz, 6 dBi na frequência de 5GHz;

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

4.5.3.6.1.1.8. Deve possuir LEDs indicadores de conectividade;

4.5.3.6.1.2. **Funcionalidades WLAN Deve Atender aos Seguintes Padrões:**

4.5.3.6.1.2.1. IEEE 802.11a/b/g/n/ac/ax;

4.5.3.6.1.2.2. Dupla banda 2,4 e 5GHz simultâneas;

4.5.3.6.1.2.3. Deve operar em MIMO 2x2 com suporte a 2 spatial streams e suporte a MU-MIMO;

4.5.3.6.1.2.4. Deve suportar as seguintes taxas de dados:

a) IEEE 802.11b: 1, 2, 5.5, 11 Mbps;
b) IEEE 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps;
c) IEEE 802.11n: 6.5 – 300 Mbps (20 / 40 MHz);
d) IEEE 802.11ac: 6.5 – 866 Mbps (20 / 40 / 80 MHz);
e) IEEE 802.11ax: 3.6 - 574 Mbps (2.4GHz, 20 / 40 MHZ)
f) IEEE 802.11ax: 3.6 - 2400 Mbps (5GHz, 20 / 40 / 80 / 160MHz)

4.5.3.6.1.2.5. Deve oferecer potência mínima de transmissão RF de 26dBm em 2,4GHz e 25dBm em 5GHz;

4.5.3.6.1.2.6. Deve suportar no mínimo 16 SSIDs simultaneamente por rádio totalizando até 32 SSIDs no sistema;

4.5.3.6.1.2.7. Deve suportar a configuração de no mínimo 16 VLANs ativas simultaneamente por rádio totalizando até 32 VLANs ativas simultaneamente no sistema;

4.5.3.6.1.2.8. O equipamento proposto deverá poder operar nos seguintes modos:

a) Access Point;
b) Wireless Mesh;

4.5.3.6.1.2.9. Deverá permitir o controle de tráfego para cada SSID;

4.5.3.6.1.2.10. Deverá selecionar dinamicamente os canais de operação;

4.5.3.6.1.2.11. Deverá selecionar automaticamente a melhor opção de conexão dos clientes (Band Steering);

4.5.3.6.1.3. **Gerenciamento**

4.5.3.6.1.3.1. Deve suportar gerenciamento SNMP v2c;

4.5.3.6.1.3.2. Deve permitir configuração dos parâmetros IP através de serviço DHCP Cliente;

4.5.3.6.1.3.3. Deve permitir acesso remoto a console via HTTP e HTTPs;

4.5.3.6.1.3.4. Deve permitir a atualização de firmware via TFTP ou HTTP;

4.5.3.6.1.3.5. Deve suportar sincronização de relógio através de SNTP ou NTP;

4.5.3.6.1.3.6. Deve suportar atualização automática do firmware quando estiver operando em modo gerenciado;

4.5.3.6.1.3.7. Deve suportar plataforma em nuvem que permite o gerenciamento de pontos de acesso de diferentes fabricantes;

4.5.3.6.1.4. **Segurança**

4.5.3.6.1.4.1. Deve suportar autenticação através de servidor RADIUS;

4.5.3.6.1.4.2. Deve suportar WiFi Protected Access (WPA/WPA2);

4.5.3.6.1.4.3. Deve suportar WPA/WPA2 (PSK);

4.5.3.6.1.4.4. Deve suportar WPA3;

4.5.3.6.1.4.5. Deve permitir bloqueio da divulgação do SSID;

4.5.3.6.1.5. **Gerais**

4.5.3.6.1.5.1. Deve suportar fonte de alimentação DC externa operando em tensões de 100 a 240 V e em frequências de 50 a 60 Hz automaticamente;

4.5.3.6.1.5.2. Deve possuir a classificação IP68 de resistência a intempéries;

4.5.3.6.1.5.3. Deve permitir montagem em parede ou poste;

4.5.3.6.1.5.4. Deve suportar temperatura de operação entre - 40°C a 60°C;

4.5.3.6.1.5.5. Deve suportar sistema operacional em conformidade com o OpenWiFi da Telecom Infra Project;

4.5.3.6.1.5.6. Deverá suportar o padrão OpenRoaming para garantir a facilidade e segurança de conexão dos clientes à rede sem fio, permitindo a ampla utilização da rede pelos usuários finais;

4.5.3.6.1.5.7. A controladora deve permitir que o access point seja controlado simultaneamente com access points de diferentes fabricantes

4.5.3.6.1.5.8. A empresa fornecedora da solução deverá apresentar uma prova de conceito (PoC) comprovando o funcionamento da controladora gerenciando no mínimo 2 access points de fabricantes diferentes

4.5.3.6.1.5.9. A empresa fornecedora deverá possuir atestado de capacidade de implementação de solução equivalente com ecossistema OpenWiFi

4.5.3.6.2. **Ponto de Acesso Indoor Wi-Fi 6 2x2**

4.5.3.6.2.1. **Conectividade**

4.5.3.6.2.1.1. Deve possuir, no mínimo, 1 porta uplink ethernet 100/1000/2.5G Base-T em conector RJ45 com suporte a alimentação PoE compatível com o padrão IEEE 802.3at e com reconhecimento automático de crossover MDI/MDIX;

4.5.3.6.2.1.2. Deve possuir 1 porta LAN ethernet 100/1000Base-T em conector RJ45 e com reconhecimento automático de crossover MDI/MDIX;

4.5.3.6.2.1.3. Possuir porta de console para gerenciamento e configuração via linha de comando (CLI – command line interface) com conector RJ-45 diferente da porta de rede solicitada anteriormente;

4.5.3.6.2.1.4. Deve possuir 1 porta USB;

4.5.3.6.2.1.5. Deve possuir 2 rádios operando nas frequências de 2,4GHz e 5GHz simultáneamente;

4.5.3.6.2.1.6. Deve possuir rádio Bluetooth Low-Energy (BLE) integrado ao equipamento;

4.5.3.6.2.1.7. Deve possuir antenas omnidirecionais internas ao equipamento com ganho mínimo de 4 dBi na frequência de 2,4GHz, 6 dBi na frequência de 5GHz e 4 dBi para BLE;

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

4.5.3.6.2.1.9. Deve possuir LEDs indicadores de conectividade WLAN e Power/Diag;

4.5.3.6.2.2. **Funcionalidades WLAN Deve Atender aos Seguintes Padrões:**

4.5.3.6.2.2.1. IEEE 802.11a/b/g/n/ac/ax;

4.5.3.6.2.2.2. Dupla banda 2,4 e 5GHz simultâneas;

4.5.3.6.2.2.3. Deve operar em MIMO 2x2 com suporte a 2 spatial streams e suporte a MU-MIMO;

4.5.3.6.2.2.4. Deve suportar as seguintes taxas de dados:

a) IEEE 802.11b: 1, 2, 5.5, 11 Mbps;

b) IEEE 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps;

c) IEEE 802.11n: 6.5 – 300 Mbps (20 / 40 MHz);

d) IEEE 802.11ac: 6.5 – 866 Mbps (20 / 40 / 80 MHz);

e) IEEE 802.11ax: 3.6 - 574 Mbps (2.4GHz, 20 / 40 MHZ)

f) IEEE 802.11ax: 3.6 - 1200 Mbps (5GHz, 20 / 40 / 80 MHz)

4.5.3.6.2.2.5. Deve oferecer potência mínima de transmissão RF de 23dBm em 2,4GHz e 23dBm em 5GHz;

4.5.3.6.2.2.6. Deve suportar Wi-Fi Multimedia (WMM);

4.5.3.6.2.2.7. Deve suportar no mínimo 16 SSIDs simultaneamente por rádio totalizando até 32 SSIDs no sistema;

4.5.3.6.2.2.8. Deve suportar a configuração de no mínimo 16 VLANs ativas simultaneamente por rádio totalizando até 32 VLANs ativas simultaneamente no sistema;

4.5.3.6.2.2.9. O equipamento proposto deverá poder operar nos seguintes modos:

a) Access Point;

b) Wireless Mesh;

4.5.3.6.2.2.10. Deverá permitir o controle de tráfego para cada SSID;

4.5.3.6.2.2.11. Deverá selecionar dinamicamente os canais de operação;

4.5.3.6.2.2.12. Deverá selecionar automaticamente a melhor opção de conexão dos clientes (Band Steering);

4.5.3.6.2.3. **Gerenciamento**

4.5.3.6.2.3.1. Deve suportar gerenciamento SNMP v2c;

4.5.3.6.2.3.2. Deve permitir configuração dos parâmetros IP através de serviço DHCP Cliente;

4.5.3.6.2.3.3. Deve permitir acesso remoto a console via HTTP e HTTPs;

4.5.3.6.2.3.4. Deve permitir a atualização de firmware via TFTP ou HTTP;

4.5.3.6.2.3.5. Deve suportar sincronização de relógio através de SNTP ou NTP;

4.5.3.6.2.3.6. Deve suportar atualização automática do firmware quando estiver operando em modo gerenciado;

4.5.3.6.2.3.7. Deve suportar plataforma em nuvem que permite gerenciamento de pontos de acesso de diferentes fabricantes;

4.5.3.6.2.4. **Segurança**

4.5.3.6.2.4.1. Deve suportar autenticação através de servidor RADIUS;

4.5.3.6.2.4.2. Deve suportar WiFi Protected Access (WPA/WPA2);

4.5.3.6.2.4.3. Deve suportar WPA/WPA2 (PSK);

4.5.3.6.2.4.4. Deve suportar WPA3;

4.5.3.6.2.4.5. Deve permitir bloqueio da divulgação do SSID;

4.5.3.6.2.4.6. Desempenho

4.5.3.6.2.4.7. Deve possibilitar a conexão de até 250 clientes concorrentes por rádio totalizando 500 simultaneamente;

4.5.3.6.2.5. **Gerais**

4.5.3.6.2.5.1. Deve suportar fonte de alimentação DC externa operando em tensões de 100 a 240 V e em frequências de 50 a 60 Hz automaticamente;

4.5.3.6.2.5.2. Deve permitir montagem em parede ou teto e vir acompanhado dos devidos kits de instalação;

4.5.3.6.2.5.3. Deve permitir a instalação de trava tipo Kensington;

4.5.3.6.2.5.4. Deve suportar temperatura de operação entre 0°C a 50°C;

4.5.3.6.2.5.5. Possuir certificado válido de homologação emitido pela Anatel.

4.5.3.6.2.5.6. Deverá ser apresentado certificado válido de interoperabilidade fornecido pela Wi-Fi Alliance na categoria de Enterprise Access Point;

4.5.3.6.2.5.7. Deve suportar sistema operacional em conformidade com o OpenWiFi da Telecom Infra Project;

4.5.3.6.2.5.8. Deverá suportar o padrão OpenRoaming para garantir a facilidade e segurança de conexão dos clientes à rede sem fio, permitindo a ampla utilização da rede pelos usuários finais;

4.5.3.6.2.5.9. A controladora deve permitir que o access point seja controlado simultaneamente com access points de diferentes fabricantes

4.5.3.6.2.5.10. A empresa fornecedora da solução deverá apresentar uma prova de conceito (PoC) comprovando o funcionamento da controladora gerenciando no mínimo 2 access points de fabricantes diferentes

4.5.3.6.2.5.11. A empresa fornecedora deverá possuir atestado de capacidade de implementação de solução equivalente com ecossistema OpenWiFi

4.5.3.6.3. **Switch de Acesso POE 8 Portas 2.5base-T e 2 Portas 10G SFP+**

4.5.3.6.3.1. **Conectividade**

4.5.3.6.3.1.1. Deve possuir 8 portas padrão 2.5G/1000 Base-T em conector RJ45 compatível com o padrão IEEE 802.3az de eficiência energética;

4.5.3.6.3.1.2. Deve possuir no mínimo 2 portas 10G Base-X padrão SFP+ para a instalação de módulos padrão SFP+ ou cabos DAC;

4.5.3.6.3.1.3. As portas Base-T deverão suportar autonegociação de velocidade, modo de operação e detecção MDI-MDIX;

4.5.3.6.3.1.4. Deve possuir porta console serial padrão RS-232 em conector DB-9 ou RJ45 acompanhado do respectivo cabo para conexão ao PC;

4.5.3.6.3.2. **PoE**

4.5.3.6.3.2.1. Deve suportar alimentação PoE conforme o padrão IEEE 802.3af/802.3at nas 8 portas RJ45 dentro da disponibilidade de potência destinada a esse fim;

4.5.3.6.3.2.2. Deve suportar alimentação PoE++ conforme o padrão IEEE 802.3bt em, no mínimo, 4 portas RJ45 de forma simultânea;

4.5.3.6.3.2.3. Deve possibilitar visualização da alimentação através de LED exclusivo ou de múltipla funcionalidade;

4.5.3.6.3.2.4. Deve disponibilizar no mínimo 240W para utilização exclusiva no PoE sem utilização de fonte adicional para esse fim;

4.5.3.6.3.3. **Controle**

4.5.3.6.3.3.1. Deve suportar Jumbo Frames de 12K;

4.5.3.6.3.3.2. Deve suportar até 4K VLANs segundo o protocolo IEEE 802.1Q, por porta e por protocolo;

4.5.3.6.3.3.3. Deve suportar implementação de VLANs Privativas;

4.5.3.6.3.3.4. Deve suportar implementação de Voice VLANs;

4.5.3.6.3.3.5. Deve implementar suporte a QinQ;

4.5.3.6.3.3.6. Possuir no mínimo oito filas em hardware para priorização de tráfego por porta;

4.5.3.6.3.3.7. Implementar QoS com base no protocolo 802.1p e DSCP;

4.5.3.6.3.3.8. Deve implementar controle de fluxo com o protocolo 802.3X e Back Pressure;

4.5.3.6.3.3.9. Deve implementar IGMP Snooping v1, v2 e v3;

4.5.3.6.3.3.10. Deve implementar IGMP Filtering, Immediate Leave Querier;

4.5.3.6.3.3.11. Deve implementar MLD Snooping;

4.5.3.6.3.3.12. Deve possibilitar a limitação de Broadcast, Multicast Unicast;

4.5.3.6.3.3.13. Deve implementar o gerenciamento de banda com valores distintos para entrada e saída;

4.5.3.6.3.3.14. Deve implementar os mecanismos de controle de fila: SP (Strict Priority) e WRR (Weighted Round Robin);

4.5.3.6.3.4. **Disponibilidade**

4.5.3.6.3.4.1. Implementar o protocolo Spanning Tree (802.1D);

4.5.3.6.3.4.2. Implementar o protocolo Rapid Spanning Tree (802.1w);

4.5.3.6.3.4.3. Deve implementar o protocolo Multiple Spanning Tree (802.1s);

4.5.3.6.3.4.4. Deve suportar detecção de laço (loopback detection);

4.5.3.6.3.4.5. Deve implementar BPDU Guard/Filter e ROOT Guard;

4.5.3.6.3.4.6. Deve suportar até 8 grupos de agregação dinâmicos no padrão LACP ou estático de até 8 portas GbE;

4.5.3.6.3.5. **Gerenciamento**

4.5.3.6.3.5.1. Deve possuir suporte a pilha dupla de protocolo IPv4/IPv6;

4.5.3.6.3.5.2. Deve suportar gerenciamento SNMP v1, v2c e v3;

4.5.3.6.3.5.3. Deve permitir configuração dos parâmetros IP através de serviço DHCP Cliente;

4.5.3.6.3.5.4. Deve permitir acesso remoto a console via Telnet, SSHv2, HTTP e HTTPs;

4.5.3.6.3.5.5. Deve permitir configuração através de plataforma de gerenciamento em nuvem com suporte a OpenLan Switching (OLS) e OpenWiFi em conformidade com as especificações da Telecom Infra Project (TIP);

4.5.3.6.3.5.6. Deve permitir acesso local a console CLI;

4.5.3.6.3.5.7. Deve permitir atualização e provisionamento automáticos, podendo este ser executado por sistema de gestão externo sendo, neste caso, necessário proporcionar a solução completa;

4.5.3.6.3.5.8. Deve suportar os grupos 1, 2, 3 e 9 de RMON;

4.5.3.6.3.5.9. Deve suportar o protocolo LLDP (IEEE 802.1ab);

4.5.3.6.3.5.10. Deve permitir armazenar no mínimo duas imagens de firmware em memória flash interna;

4.5.3.6.3.5.11. Deve permitir a atualização de firmware via HTTP, TFTP ou FTP em memória tipo flash;

4.5.3.6.3.5.12. Deve permitir armazenar no mínimo duas configurações distintas em memória flash interna;

4.5.3.6.3.5.13. Deve permitir salvar as configurações em um computador local (backup) via HTTP, TFTP ou FTP;

4.5.3.6.3.5.14. Deve suportar espelhamento de tráfego;

4.5.3.6.3.5.15. Deve suportar SNMP over IPv6;

4.5.3.6.3.5.16. Deve suportar HTTP over IPv6;

4.5.3.6.3.5.17. Deve suportar IPv6 remote ping;

4.5.3.6.3.5.18. Deve suportar NTP ou SNTP;

4.5.3.6.3.5.19. Deve implementar log de eventos em memória flash e permitir a gravação em servidor externo padrão Syslog;

4.5.3.6.3.6. **Segurança**

4.5.3.6.3.6.1. Deve possuir proteção a ataques Denial of Service;

4.5.3.6.3.6.2. Deve suportar autenticação local e através de servidor RADIUS e TACACS+;

4.5.3.6.3.6.3. Deve implementar segurança de acesso através do protocolo IEEE 802.1X e autenticação por MAC;

4.5.3.6.3.6.4. Deve suportar assinalamento automático de VLAN e política de QoS;

4.5.3.6.3.6.5. Deve possuir suporte à AAA (Authentication, Authorization and Account) em servidores RADIUS ou TACACS+;

4.5.3.6.3.6.6. Deve suportar implementação de VLANs para visitantes;

4.5.3.6.3.6.7. Deve permitir filtragem de pacotes identificados por cabeçalho ethernet ou IP;

4.5.3.6.3.6.8. Deve suportar DHCP snooping;

4.5.3.6.3.6.9. Deve suportar IP Source Guard;

4.5.3.6.3.6.10. Deve possuir Port Security ou funcionalidade similar;

4.5.3.6.3.6.11. Deve possuir Dynamic ARP Inspection ou funcionalidade similar;

4.5.3.6.3.6.12. Deve implementar MAC based ACL;

4.5.3.6.3.7. **Desempenho**

4.5.3.6.3.7.1. Deve possuir capacidade de vazão de ao menos 80 Gbps;

4.5.3.6.3.7.2. Deve chavear no mínimo 59 Mpps;

4.5.3.6.3.7.3. Tabela de endereços MAC com capacidade para no mínimo 16.000 endereços;

4.5.3.6.3.7.4. Funções camada 3

tório - 029/2025 | Documento_assinado_1EE7025... processo_administrativo_54_pregao_2025_assinado ... (69/233) 4550/4786

4.5.3.6.3.7.5. Deve implementar rotas estáticas;

4.5.3.6.3.7.6. Deve implementar o protocolo RIP;

4.5.3.6.3.8. **Padronização**

4.5.3.6.3.8.1. Deve ser compatível com os seguintes padrões:

a) IEEE 802.1D (STP)
b) IEEE 802.1p (COS)
c) IEEE 802.1Q (VLAN)
d) IEEE 802.1s (MSTP)
e) IEEE 802.1v (VLAN)
f) IEEE 802.1w (RSTP)
g) IEEE 802.1X (Security)
h) IEEE 802.3ad (Link aggregation)
i) IEEE 802.3x (Flow control)
j) IEEE 802.3z (Gigabit)
k) IEEE 802.1AB (Link Layer Discovery Protocol)
l) IEEE 802.3az (Energy Efficiency)

4.5.3.6.3.9. **Gerais**

4.5.3.6.3.9.1. Deve possuir fonte de alimentação interna operando em tensões de 100 a 240 V e em frequências de 50 a 60 Hz automaticamente;

4.5.3.6.3.9.2. Deve vir acompanhado do kit de suporte específico para montagem em Rack de 19;

4.5.3.6.3.9.3. O equipamento deverá ocupar uma unidade de rack;

4.5.3.6.3.9.4. Deve possuir temperatura de operação de 0° C a 50° C;

4.5.3.6.3.9.5. Deve possuir sistema operacional OpenLan Switching (OLS) em conformidade com as especificações da Telecom Infra Project (TIP);

4.6. O sistema de gerenciamento de acesso das praças deverá ser de responsabilidade da Contratada, seguindo todas as normas da lei 13.709/2018 (LEI GERAL DE PROTEÇÃO DE DADOS - LGPD) e Lei Federal nº 12.965/2014, Decreto Federal nº 8.771/2016 que regulamenta o Marco Civil da Internet e demais legislações Federais ou Municipais relativas à matéria.

4.7. O caráter confidencial das informações dos usuários será garantido, não podendo ser compartilhado, em nenhuma hipótese, inclusive para uso comercial, publicitário ou estatístico.

4.8. A contratada deverá fornecer acesso ao sistema de gerenciamento das Praças, quantidade de acesso, acesso para inserção de informações e ações da Prefeitura e demais secretarias, não sendo aceito propagandas da contratada.

4.9. O SSID da rede não poderá associar o nome do eventual contratante privado.

4.10. O formato do SSID será definido pela Prefeitura Municipal de Cáceres / Coordenação de Tecnologia da Informação (CTI).

4.11. A Contratada deverá fornecer o sistema de gerenciamento hotspot de fácil acesso para os visitantes, que seja feito a coleta do nome, telefone e e-mail dos visitantes.

4.12. Será obrigação contratual a armazenagem, por todo o período de vigência, do registro de conexão, de medições básicas da rede e de todas as informações de cadastro de usuários, incluindo as informações de preenchimento voluntário.

4.13. Ao pressionar o botão destinado à conexão com a internet pela primeira vez, ele será transferido para a página de cadastro definido pela Contratante;

4.14. Que os usuários não tenham acesso a equipamentos de outros usuários conectados à rede WI-FI.

4.15. A contratada deverá fornecer sistema ou API de gerenciamento de funcionamento dos Wi-Fi das praças para auxiliar a fiscalização e acompanhamento do funcionamento das conexões, além de identificar cada Wi-Fi com o nome das respectivas Praças.

4.16. A Contratada deverá apresentar junto à emissão de Nota Fiscal, os respectivos relatórios de funcionamento, login acessos dos visitantes e consumo de banda por aparelho de rádio, identificando cada praça conforme mês referência da Nota Fiscal.

4.17. A contratada, se achar necessário, poderá fazer uma visita técnica aos pontos das possíveis praças que receberão a internet, para mensurar o custo de cada praça, para a montagem da proposta do preço médio total.

4.18. A contratada deverá fornecer os aparelhos que sejam capazes de abranger geograficamente toda a área da praça ofertada, podendo ser de 1(um) ou mais aparelhos para cada praça.

4.19. Deverão ser previstos todos os equipamentos ativos e passivos de rede, infraestrutura e insumos necessários ao bom funcionamento do sistema, tais como, mas não exclusivamente: postes, fios, cabos, conectores, amplificadores, racks, pontos de conexão (access points), no- breaks, wireless controllers, watch dogs, software e suprimentos complementares de energia elétrica, conforme o caso.

4.20. Cada aparelho de acesso das Praças deverá aceitar até 500 conexões simultâneas, dividindo assim a banda de internet 100mbs igualmente para os visitantes.

4.21. Internets Wi-Fi instaladas deverão ser capazes de garantir a qualidade e estabilidade do sinal aos usuários, evitando jitters e latências, sendo compatíveis com notebooks, celulares, smartphones, netbooks, tablets e outros dispositivos comumente utilizados para acesso à internet, dentro dos padrões mínimos: 802.11b, 802.11g, 802.11n e 802.11ac.

4.22. A contratada deverá garantir o nível de sinal de pelo menos -65 dBm na área de cobertura em todas as localidades e em ambas as faixas de frequência (2,4 GHz e 5 GHz).

4.23. CONTRATADA deverá dispor de ferramentas e recursos de monitoramento e controles de hardware e/ou software que possam ser operados por seus técnicos, e que possibilitem a imediata identificação de anormalidades na operação da infraestrutura de comunicação da rede Wi-Fi

4.24. A Contratada deverá fornecer uma banda de internet de 150 Mbs dedicada para cada ponto instalado.

4.25. O funcionamento de cada praça ofertada será por 24 (vinte e quatro) horas por dia, durante 7 (sete) dias da semana.

4.26. A combinação dessas tecnologias resulta em uma infraestrutura altamente disponível, segura e escalável, proporcionando continuidade operacional, proteção avançada contra ameaças cibernéticas e eficiência na comunicação entre as unidades municipais.

4.27. A solução foi desenhada para assegurar a proteção e a disponibilidade dos serviços municipais ao longo de todo o ciclo de vida do contrato, abrangendo desde a implantação inicial até a gestão contínua da infraestrutura de segurança e conectividade. A abordagem adotada permite que o município de Cáceres modernize sua infraestrutura digital, proteja seus ativos de TI e garanta a prestação eficiente de serviços à população, sempre com segurança, confiabilidade e alta performance.

5. REQUISITOS DA CONTRATAÇÃO

5.1. **Requisitos De Negócio**

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

5.1.1.1. Implementação de tecnologia Next Generation Firewall (NGFW) para garantir proteção robusta contra ameaças cibernéticas e manutenção da integridade das operações de rede.

5.1.1.2. Implementação de sistema baseado em Inteligência Artificial Preditiva capaz de analisar padrões de comportamento na rede, identificar e neutralizar automaticamente ameaças sem necessidade de intervenção humana.

5.1.1.3. Disponibilização de equipamentos de hardware necessários à proteção da rede, sem a necessidade de aquisição direta, com manutenção e suporte garantidos pelo fornecedor, promovendo economicidade e flexibilidade.

5.1.1.4. Proteção eficaz contra ataques de “Zero Day”.

5.1.1.5. Atuação direta no tráfego de entrada da internet, identificando e neutralizando instantaneamente origens maliciosas.

5.1.1.6. Proteção abrangente para toda a infraestrutura, incluindo firewalls e roteadores.

5.1.1.7. Proteção abrangente para toda a infraestrutura, incluindo firewalls e roteadores.

5.1.1.8. Inclusão de software para configuração, monitoramento e gestão centralizada das políticas de segurança da rede de forma integrada e eficiente, permitindo maior controle e visibilidade.

5.1.1.9. Garantia de licenças válidas durante todo o período contratual, permitindo o pleno uso das funcionalidades da solução contratada.

5.1.1.10. Provisão de link dedicado de acesso à internet, bloco /29 e banda mínima de acesso garantida de 500Mbps para a solução NGFW SEDE (Dois Link de ASN e Rota Diferentes), essa configuração garante alta disponibilidade, resiliência a falhas e suporte eficiente às operações críticas.

5.1.1.11. Configuração e integração dos links diretamente com a solução NGFW, permitindo a gestão eficiente do tráfego e a aplicação das políticas de segurança.

5.1.1.12. Implementação de soluções SD-WAN integradas ao NGFW para conectar unidades externas vinculadas às secretarias municipais, promovendo segurança, desempenho e centralização na gestão de tráfego entre os locais.

5.1.1.13. Provisão de link primário de acesso à internet banda mínima de acesso garantida de 150Mbps Sites Remotos (Fibra Óptica), e link secundário de acesso à internet banda mínima de acesso garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G), link de ASN e rota diferentes, específicos para cada unidade externa e praças municipais, assegurando a continuidade das operações e a resiliência da rede em caso de falhas.

5.1.1.14. Realização de serviços especializados para instalação, configuração inicial e adequação às necessidades específicas do contratante e das unidades externas.

5.1.1.15. Implantação nas unidades externas de redes Wi-Fi seguras e segregadas para uso exclusivo dos servidores municipais, otimizando a conectividade e produtividade.

5.1.1.16. Garantia de autenticação por usuário e integração com políticas de segurança baseadas no NGFW.

5.1.1.17. Oferta de internet Wi-Fi gratuita nas unidades externas e nas praças municipais, com políticas de acesso baseadas no NGFW, assegurando privacidade e controle de navegação.

5.1.1.18. Implementação de mecanismos de limitação de banda e monitoramento para manter a qualidade do serviço e evitar o uso inadequado.

5.1.1.19. Atualizações regulares de firmware e assinaturas de segurança e patches, assegurando proteção contra ameaças emergentes e melhorias contínuas no desempenho da solução.

5.1.1.20. Capacitação especializada para a equipe do contratante, com emissão de certificação que ateste o domínio das funcionalidades e a capacidade de operação e manutenção da solução.

5.1.1.21. Oferta de suporte técnico com níveis de serviço bem definidos (SLA), cobrindo atendimento remoto e presencial, para resolução de incidentes e dúvidas operacionais.

5.1.1.22. Expansibilidade da solução para atender a demandas futuras de crescimento em tráfego, usuários e funcionalidades.

5.1.1.23. Ferramentas para supervisão em tempo real e geração de relatórios detalhados para análise de desempenho, auditorias e conformidade.

5.1.1.24. Garantia de aderência às regulamentações aplicáveis à proteção de dados e segurança da informação, incluindo requisitos legais e normativos vigentes.

5.1.1.25. Solução projetada para assegurar operação ininterrupta, com mecanismos de failover, redundância e backup que minimizem o impacto de falhas ou interrupções.

5.1.1.26. Redução da complexidade operacional, proporcionando maior eficiência no gerenciamento da segurança da rede e otimização de recursos técnicos e financeiros.

5.1.1.27. Configuração de políticas de tráfego e priorização de dados para garantir a performance ideal em aplicações críticas.

5.2. **Requisitos De Capacitação**

5.2.1. Deverá ser incluído na contratação capacitação técnica para a operação da solução, a serem conduzidos diretamente pelo fabricante ou por parceiro nacional devidamente capacitado, certificado e autorizado pelo fabricante para ministrar capacitações oficiais.

5.2.2. Deverá ser ministrado em Língua Portuguesa/Brasil.

5.2.3. Realização de capacitação básica com duração de 40 horas, abrangendo os conhecimentos essenciais para operar e gerenciar a solução implantada.

5.2.4. Deverá ser realizada uma reunião prévia entre o contratante e a empresa contratada para definição do calendário da capacitação básica que trata o item 5.2.3.

5.2.4.1. O cronograma deverá ser ajustado às necessidades da equipe da Coordenação de TI e compatível com a disponibilidade operacional, garantindo a participação integral dos envolvidos e a eficácia do processo de aprendizado.

5.2.5. Capacitação destinada a uma equipe de até 10 participantes da Coordenação de TI, garantindo maior interação com os instrutores e personalização do aprendizado.

5.2.6. Emissão de certificação oficial reconhecida pelo fabricante da solução ou por entidades de referência na área de segurança de rede, atestando a qualificação da equipe.

5.2.7. Capacitação presencial, realizado na sede da Prefeitura Municipal de Cáceres, para otimizar o tempo e garantir a participação efetiva da equipe.

5.2.8. Divisão do conteúdo em módulos, facilitando o aprendizado progressivo:

- Módulo 1: Introdução ao NGFW, IA Preditiva e princípios de segurança de rede.
- Módulo 2: Configuração inicial e operação básica dos equipamentos e software.
- Módulo 3: Gerenciamento de políticas de segurança e monitoramento da rede.
- Módulo 4: Configuração de links dedicados (redundância e backup).
- Módulo 5: Resolução de problemas e resposta a incidentes.

5.2.9. A divisão de conteúdo que trata o item 5.2.8 poderá ser alterado mediante reunião prévia entre o contratante e a empresa contratada.

5.2.10. Inclusão de laboratórios práticos para simulação de cenários reais, como aplicação de políticas de segurança, monitoramento de tráfego e configuração de redundância e backup.

5.2.11. Disponibilização de apostilas, guias de configuração, tutoriais e acesso a uma base de conhecimento técnico para consulta pós-capacitação.

5.2.12. Instruções específicas sobre a configuração, gerenciamento e monitoramento dos links de redundância e backup, incluindo a utilização de IPs fixos.

5.2.13. Aplicação de avaliação ao final da capacitação para validação do conhecimento adquirido, seguido da entrega de certificados aos aprovados.

5.2.14. Abordagem de procedimentos para garantir a continuidade operacional da solução, como atualizações, backup de configurações e gerenciamento de logs.

5.2.15. Disponibilização de suporte técnico após a capacitação, para auxiliar na aplicação prática dos conhecimentos adquiridos.

5.2.16. Orientação sobre as melhores práticas para gestão segura da rede, incluindo conformidade com normas e regulamentações aplicáveis, como a LGPD.

5.2.17. Previsão de um workshop complementar, podendo este ser por vídeo conferencia, a ser realizado após a conclusão da capacitação, para reforçar conteúdos e sanar dúvidas remanescentes.

5.2.18. Elaboração de relatórios detalhados com informações sobre a participação, desempenho e certificação da equipe, para acompanhamento da gestão de competências.

5.3. **Requisitos Legais**

5.3.1. **Conformidade Legal e Normativa:**

5.3.1.1. A contratação deve obedecer à Constituição Federal, garantindo os princípios da legalidade, moralidade, publicidade, eficiência e economicidade.

5.3.1.2. Estar em conformidade com a Lei nº 14.133/2021, que regula as normas gerais de licitação e contratação pública.

5.3.1.3. Atender à Instrução Normativa SGD/ME nº 94, de 2022, que disciplina contratações de TIC no setor público.

5.3.1.4. Respeitar a Instrução Normativa SEGES/ME nº 65, de 2021, que trata da governança em aquisições de TIC.

5.3.1.5. Observar a Lei nº 13.709, de 2018 (LGPD), garantindo a proteção de dados pessoais.

5.3.1.6. Aplicar as disposições da Lei nº 10.520, de 2001, e do Decreto nº 10.024, de 2019, referentes ao pregão eletrônico.

5.3.1.7. Cumprir o Decreto Municipal nº 665, de 09 de outubro de 2024, que regulamenta contratações de TIC no âmbito municipal.

5.3.2. **Proteção de Dados e Privacidade:**

5.3.2.1. Garantir conformidade integral com a LGPD, implementando medidas para prevenir acessos não autorizados e vazamentos de dados pessoais.

5.3.2.2. O contratado deve demonstrar, quando solicitado, os mecanismos e políticas utilizados para assegurar a proteção de dados, sujeitos à auditoria da contratante.

5.3.3. **Transparência e Publicidade:**

5.3.3.1. Todos os atos do processo licitatório e de execução contratual deverão ser registrados e divulgados nos meios oficiais, conforme exigido por lei.

5.3.3.2. Relatórios e informações sobre a execução do contrato deverão ser disponibilizados periodicamente para consulta pública, garantindo transparência no uso dos recursos.

5.3.4. **Responsabilidade do Contratado:**

5.3.4.1. O contratado é responsável por cumprir integralmente as obrigações legais aplicáveis, incluindo as previstas na Lei nº 14.133/2021 e no Decreto Municipal nº 665/2024, respondendo por eventuais descumprimentos com as penalidades previstas em contrato e em lei.

5.4. **Requisitos De Manutenção**

5.4.1. **Manutenção Preventiva (Não Emergencial):**

5.4.1.1. Realização de manutenções programadas para garantir o funcionamento ideal da solução NGFW, incluindo inspeções, limpeza, análise de logs, e aplicação de atualizações de firmware.

5.4.1.2. Frequência mínima semestral ou conforme cronograma estabelecido entre as partes.

5.4.2. **Manutenção Corretiva (Emergencial):**

5.4.2.1. Atendimento imediato para corrigir falhas ou defeitos nos equipamentos ou no software, visando a restauração do funcionamento normal da solução NGFW.

5.4.2.2. Inclui diagnóstico remoto e, quando necessário, deslocamento técnico para reparos ou substituição de componentes.

5.4.3. **Manutenção Adaptativa (Não Emergencial):**

5.4.3.1. Adequação da solução NGFW às mudanças no ambiente operacional ou aos requisitos específicos do contratante, como ajustes de configuração ou implementação de novas políticas de segurança.

5.4.4. **Manutenção Evolutiva (Não Emergencial):**

5.4.4.1. Implementação de melhorias na solução, incluindo a integração de novas funcionalidades, suporte a tecnologias emergentes e expansão da capacidade para atender a demandas crescentes.

5.4.5. **Monitoramento Proativo (Não Emergencial):**

5.4.5.1. Serviço contínuo de monitoramento da solução, com análise de logs e detecção antecipada de falhas ou ameaças que exijam intervenção.

5.4.6. **Substituição de Equipamentos (Emergencial):**

5.4.6.1. Garantia de substituição rápida e sem custos adicionais de equipamentos defeituosos durante a vigência contratual, minimizando interrupções.

5.4.7. **Relatórios Periódicos (Não Emergencial):**

5.4.7.1. Emissão de relatórios detalhados sobre intervenções realizadas, estado dos equipamentos, atualizações aplicadas e resultados das manutenções.

5.4.8. **Classificação de Ocorrências:**

5.4.8.1. Critérios claros para categorizar os atendimentos em emergenciais e não emergenciais, com tratamento prioritário para problemas críticos.

5.4.9. **Tabela de atendimento:**

TIPO DE ATENDIMENTO	DESCRIÇÃO	EMERGENCIAL/NÃO EMERGENCIAL	TEMPO DE RESPOSTA	TEMPO DE SOLUÇÃO	MEIO DE ATENDIMENTO
Emergencial	Ocorrências críticas que impactem diretamente a operação da rede, como falhas graves nos equipamentos NGFW, links de redundância ou brechas de segurança.	Emergencial	Até 1 hora	Até 4 horas	Suporte remoto e, se necessário, presencial.
Corretiva	Problemas pontuais ou defeitos que não sejam de natureza crítica, mas que exijam reparo técnico para evitar impactos futuros.	Emergencial	Até 4 horas	Até 8 horas	Suporte remoto ou presencial agendado.
Preventiva	Ações periódicas de inspeção e manutenção para prevenir falhas e garantir o desempenho ideal da solução.	Não Emergencial	Agendamento prévio	Conforme cronograma	Suporte presencial planejado.
Adaptativa	Ajustes para adequação da solução a novas necessidades operacionais ou mudanças no ambiente do contratante.	Não Emergencial	Até 2 dias úteis	Até 7 dias úteis	Suporte remoto ou presencial agendado.
Evolutiva	Melhorias e implementações que ampliem as funcionalidades ou capacidades da solução NGFW.	Não Emergencial	Até 5 dias úteis	Conforme projeto	Suporte remoto ou presencial planejado.
Substituição de Equipamentos	Substituição de equipamentos defeituosos ou que apresentem falhas que afetem a continuidade do serviço.	Emergencial	Até 1 hora	Até 4 horas	Suporte remoto e, se necessário, presencial.
Monitoramento Proativo	Monitoramento contínuo da solução para antecipar	Não Emergencial	Até 4 horas	Contínuo	Suporte remoto.

	problemas, como detecção de falhas ou anomalias.				
Relatórios Periódicos	Emissão de relatórios detalhados sobre o status da solução NGFW, ações realizadas e estado dos equipamentos.	Não Emergencial	Até 24 horas	Conforme cronograma	Suporte remoto ou presencial agendado.

5.5. **Requisitos Temporais**

5.5.1. **Prazos de Entrega dos Equipamentos e Solução:**

5.5.1.1. O fornecimento dos equipamentos necessários para a implementação da solução, incluindo hardware, licenças e software de gerenciamento, deverá ser realizado no prazo máximo de 30 dias corridos a partir da assinatura do contrato.

5.5.1.2. A instalação, configuração e ativação completa da solução, incluindo os links de internet e redundância, deverá ser concluída no prazo máximo de 45 dias corridos após a entrega dos equipamentos.

5.5.1.3. O treinamento básico com carga horária de 40 horas para a equipe técnica da Prefeitura Municipal de Cáceres deverá ser realizada uma reunião prévia entre o contratante e a empresa contratada para definição do calendário da capacitação básica.

5.5.2. **Prazos de Atendimento para Suporte Técnico:**

5.5.2.1. **Atendimento Emergencial:**

5.5.2.1.1. Chamados emergenciais, que incluem falhas críticas que afetam diretamente a operação da rede ou a disponibilidade de serviços essenciais, deverão ser atendidos no prazo máximo de 4 horas após a abertura do chamado.

5.5.2.1.2. A solução completa para o problema deverá ser implementada no prazo máximo de 8 horas, salvo situações excepcionais que exijam medidas corretivas complexas.

5.5.2.2. **Atendimento Não Emergencial:**

5.5.2.2.1. Chamados de manutenção corretiva, preventiva, adaptativa ou evolutiva que não impactem diretamente a operação da rede deverão ser atendidos no prazo máximo de 24 horas úteis após a abertura do chamado.

5.5.2.2.2. A resolução deverá ocorrer no prazo de até 5 dias úteis, salvo a necessidade de ajustes ou implementações que exijam maior prazo, o qual será acordado previamente.

5.5.3. **Forma de Atendimento do Suporte Técnico:**

5.5.3.1. **Atendimento Remoto:**

5.5.3.1.1. O suporte técnico deverá ser disponibilizado remotamente como primeira opção para resolução de problemas, utilizando ferramentas seguras para acesso remoto e diagnóstico.

5.5.3.1.2. O suporte remoto deverá estar disponível 24x7 (24 horas por dia, 7 dias por semana) para incidentes emergenciais.

5.5.3.2. **Atendimento Presencial:**

5.5.3.2.1. Quando a resolução do problema não for possível de forma remota, será realizado atendimento presencial por técnicos especializados.

5.5.3.2.2. O prazo para deslocamento e início do atendimento no local para casos emergenciais será de até 4 horas úteis a partir da solicitação.

5.5.3.2.3. Para casos não emergenciais, o atendimento presencial será agendado com a equipe de TI da Prefeitura, respeitando o prazo máximo de 2 dias úteis.

5.5.4. **Monitoramento e Relatórios de SLA:**

5.5.4.1. A empresa contratada deverá monitorar e registrar os tempos de atendimento e resolução de chamados, emitindo relatórios mensais que comprovem o cumprimento dos SLAs estabelecidos.

5.5.4.2. O descumprimento dos prazos estabelecidos implicará penalidades contratuais conforme especificado nos termos do contrato.

5.5.5. **Atendimento de Manutenção Preventiva e Evolutiva:**

5.5.5.1. Manutenções preventivas deverão ser realizadas trimestralmente, com agendamento prévio com a equipe de TI da Prefeitura Municipal de Cáceres.

5.5.5.2. Manutenções evolutivas, que envolvam atualizações ou melhorias significativas na solução, deverão ser realizadas mediante planejamento e acordo prévio, com prazo máximo de implementação em 30 dias úteis após a aprovação.

5.6. **Requisitos de Segurança e Privacidade**

5.6.1. **Políticas de Segurança Baseadas no NGFW**

5.6.1.1. Permitir a configuração de políticas robustas de segurança para controle e monitoramento de tráfego de rede, assegurando proteção contra ataques cibernéticos, intrusões, malwares e acessos não autorizados.

5.6.1.2. Definir regras personalizadas para bloquear tráfego malicioso e permitir apenas conexões seguras e autorizadas.

5.6.1.3. Configuração de proteção contra ataques de negação de serviço (DoS), com a opção de habilitação global ou por política específica.

5.6.1.4. Disponibilizar uma interface única para configuração de políticas, integrando perfis de segurança como Proxy Web, IPS, Controle de Aplicações, SD-WAN e Proteção contra Ameaças Avançadas (ATP).

5.6.1.5. Implementar validação automatizada das políticas de segurança para identificar e resolver regras duplicadas ou conflitantes.

5.6.2. **Segmentação e Isolamento de Redes**

5.6.2.1. Segmentação lógica da rede principal e das redes das unidades externas, garantindo o isolamento entre setores e usuários, reduzindo os riscos de propagação de ataques.

5.6.2.2. Configuração de SD-WAN para roteamento dinâmico de tráfego entre diferentes unidades e praças municipais, assegurando desempenho e segurança.

5.6.3. **Proteção Avançada Contra Ameaças**

5.6.3.1. Ativação de funcionalidades como inspeção profunda de pacotes (DPI), prevenção contra intrusões (IPS) e detecção de anomalias baseadas em inteligência artificial.

5.6.3.2. Integração com serviços de inteligência de ameaças para identificação e mitigação de ataques emergentes.

5.6.4. **Criptografia de Dados e Segurança em Trânsito**

5.6.4.1. Garantir que todas as comunicações de dados entre firewall principal, unidades externas e dispositivos sejam protegidas por protocolos de criptografia avançados, como TLS/SSL.

5.6.4.2. Implementação de inspeção de tráfego criptografado (SSL Inspection) para detecção de ameaças em comunicações seguras.

5.6.5. **Controle de Acessos e Gerenciamento Centralizado**

5.6.5.1. Adotar autenticação multifator (MFA) para acesso ao sistema de gerenciamento do NGFW e a serviços críticos.

5.6.5.2. Realizar o gerenciamento centralizado de permissões, com auditoria detalhada de acessos e atividades realizadas na rede.

5.6.6. **Monitoramento, Logs e Alertas de Segurança**

5.6.6.1. Configuração de logs detalhados de eventos e atividades, com centralização das informações em uma solução de SIEM (Gestão de Informações e Eventos de Segurança).

5.6.6.2. Geração de alertas em tempo real para eventos críticos, como tentativas de intrusão ou anomalias de tráfego.

5.6.6.3. Emissão de relatórios periódicos sobre segurança da rede, destacando vulnerabilidades detectadas e ações tomadas.

5.6.7. **Conformidade com Normas de Segurança e Privacidade**

5.6.7.1. Garantir que a solução NGFW esteja em conformidade com a LGPD e outras legislações aplicáveis, assegurando a proteção e privacidade dos dados pessoais.

5.6.7.2. Disponibilizar recursos para anonimização ou pseudonimização de dados, conforme exigido pelas normas.

5.6.8. **Testes e Avaliações Periódicas de Segurança**

5.6.8.1. Realização de testes de penetração (pentests) regulares para avaliar a eficácia das medidas de segurança.

5.6.8.2. Simulações de incidentes de segurança para treinar equipes e validar os planos de resposta a incidentes.

5.6.9. **Backup e Recuperação Segura**

5.6.9.1. Implementar backups automáticos e criptografados das configurações do NGFW e de dados críticos, com armazenamento em locais seguros.

5.6.9.2. Garantir processos rápidos de recuperação em caso de falha ou desastre, assegurando a continuidade operacional.

5.6.10. **Conscientização e Educação de Usuários**

5.6.10.1. Desenvolver programas regulares de conscientização sobre segurança da informação para servidores municipais, abordando práticas seguras de uso da internet.

5.6.10.2. Orientar os cidadãos sobre o uso responsável das redes Wi-Fi públicas disponibilizadas nas praças e unidades municipais.

5.7. **Requisitos de Metodologia de Trabalho**

5.7.1. Emissão de Ordem de Serviço (OS):

5.7.1.1. A execução de qualquer serviço contratado está condicionada ao recebimento pelo contratado de uma Ordem de Serviço (OS) emitida pela contratante.

5.7.1.2. A Ordem de Serviço deverá especificar, de forma clara:

- O serviço a ser executado.
- A quantidade de serviços.
- A localidade onde o serviço deverá ser prestado.

5.7.2. **Meios de Contato e Registro de Ocorrências:**

5.7.2.1. O contratado deve fornecer canais de comunicação para contato e registro de ocorrências, conforme as seguintes especificações:

- Atendimento eletrônico (e-mail, sistema de chamados ou aplicativo): 24 horas por dia, 7 dias por semana.
- Atendimento telefônico: 12 horas por dia, 5 dias por semana, garantindo resposta ágil a chamados emergenciais.

5.7.3. **Acompanhamento e Comunicação Durante a Execução:**

5.7.3.1. A execução de todos os serviços deverá ser acompanhada diretamente pelo contratado, assegurando o cumprimento das especificações definidas na Ordem de Serviço.

5.7.3.2. Eventuais ocorrências ou desvios identificados durante a execução deverão ser imediatamente comunicados à contratante, com descrição detalhada da situação e das medidas corretivas adotadas.

5.7.4. **Prazos de Atendimento e Execução:**

5.7.4.1. O prazo para início da execução dos serviços será contado a partir do recebimento da Ordem de Serviço, respeitando os prazos definidos nos Requisitos Temporais.

5.7.4.2. Os serviços deverão ser finalizados dentro dos prazos estabelecidos, salvo justificativas formalmente apresentadas e aceitas pela contratante.

5.7.5. **Registro e Relatório de Serviços Executados:**

5.7.5.1. Ao término de cada serviço, o contratado deverá entregar à contratante um relatório detalhado contendo:

- Descrição do serviço realizado.
- Data e horário de início e conclusão do serviço.
- Identificação dos profissionais envolvidos.
- Observações sobre eventuais dificuldades ou necessidades futuras.

5.7.5.2. O relatório deverá ser aprovado pela contratante para formalizar a conclusão do serviço.

5.7.6. **Garantia de Qualidade e Conformidade:**

5.7.6.1. O contratado deverá assegurar que todos os serviços sejam executados em conformidade com as especificações técnicas, normativas e de segurança previamente acordadas.

5.7.6.2. Qualquer serviço executado em desacordo com o estabelecido será considerado não conforme, cabendo ao contratado refazê-lo sem custos adicionais para a contratante.

5.7.7. **Reuniões de Alinhamento e Planejamento:**

5.7.7.1. O contratado deverá participar de reuniões periódicas com a contratante para alinhar prioridades, revisar o cronograma e discutir ajustes necessários nos serviços prestados.

5.7.7.2. Essas reuniões ocorrerão em frequência mínima trimestral ou conforme solicitado pela contratante.

5.7.8. **Garantia de Resposta a Ocorrências:**

5.7.8.1. O contratado deverá manter equipe disponível para atender a chamados dentro dos prazos especificados nos Requisitos de Manutenção, priorizando serviços emergenciais.

5.7.8.2. As ocorrências serão classificadas conforme sua criticidade, e o atendimento será realizado de acordo com a priorização estabelecida na Ordem de Serviço.

5.8. **Requisitos de Experiência Profissional**

5.8.1. **Experiência Comprovada no Fornecimento de Soluções NGFW:**

5.8.1.1. O contratado deverá comprovar experiência na implementação e gerenciamento de soluções de Next Generation Firewall (NGFW) em instituições públicas ou privadas de grande porte, preferencialmente na administração municipal.

5.8.1.2. Será exigida a comprovação da capacidade técnico-operacional da licitante, mediante a apresentação de atestados emitidos por pessoa jurídica de direito público ou privado, que comprovem a execução de serviços compatíveis em características, quantidades e prazos com o objeto deste contrato, incluindo o fornecimento e a instalação de equipamentos correlatos aos ofertados, bem como a prestação de serviços de instalação, configuração e suporte técnico. A

tório - 029/2025 | [illegible] (82/232) [illegible]

licitante deverá comprovar, no mínimo, experiência prévia correspondente a **30% (trinta por cento)** do quantitativo estimado do **item 1 – Solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)**, considerado de maior relevância técnica para a consecução do objeto. Tal exigência encontra amparo no inciso III do art. 67 da Lei nº 14.133/2021, sendo justificada pela complexidade e especificidade do objeto, que demanda experiência comprovada na execução de soluções integradas de segurança cibernética, com destaque para componentes baseados em Inteligência Artificial Preditiva, visando garantir a eficiência, a continuidade dos serviços e a mitigação de riscos operacionais, em observância aos princípios da legalidade, razoabilidade, eficiência e interesse público. O detalhamento das condições para aceitação dos atestados encontra-se disciplinado no item **10.2.1.5.1** e respectivos subitens.

5.8.2. **Qualificação da Equipe Técnica:**

5.8.2.1. A equipe técnica alocada deve possuir profissionais certificados pelo fabricante da solução NGFW a ser implementada, garantindo competência técnica para execução dos serviços contratados.

5.8.2.2. Os profissionais responsáveis pela execução dos serviços devem ter experiência mínima de 2 (dois) anos em funções relacionadas à implantação, manutenção e suporte de soluções de segurança da informação.

5.8.3. **Experiência em Projetos de TIC para o Setor Público:**

5.8.3.1. O contratado deverá demonstrar experiência específica em projetos de Tecnologia da Informação e Comunicação (TIC) realizados para órgãos da administração pública, especialmente em contextos municipais.

5.8.3.2. A comprovação poderá incluir contratos anteriores, declarações ou relatórios técnicos que atestem a capacidade do contratado em atender às exigências específicas de órgãos públicos.

5.8.4. **Atendimento a Requisitos de Escalabilidade e Complexidade:**

5.8.4.1. A empresa deverá comprovar ter executado projetos que envolvam ambientes complexos, com integração de múltiplas unidades ou localidades, utilizando tecnologias como SD-WAN e links redundantes.

5.8.4.2. Será considerado diferencial a experiência em projetos que incluíram a disponibilização de internet Wi-Fi para servidores e cidadãos.

5.8.5. **Experiência em Treinamento e Capacitação:**

5.8.5.1. A empresa deve demonstrar ter conduzido treinamentos técnicos relacionados à operação de soluções NGFW, com fornecimento de certificações reconhecidas.

5.8.5.2. O contratado deverá apresentar registro de treinamentos realizados, com informações sobre a carga horária, conteúdo programático e feedback dos participantes.

5.8.6. **Critérios de Avaliação da Experiência:**

5.8.6.1. A experiência profissional será avaliada com base nos documentos apresentados, como contratos, atestados, certificados de conclusão de projetos e outros registros comprobatórios.

5.8.6.2. A ausência de comprovação adequada poderá resultar na desclassificação da proposta, conforme previsto na legislação vigente.

5.9. **Requisitos de Segurança da Informação e Privacidade**

5.9.1. **Conformidade com Normas e Padrões de Segurança:**

5.9.1.1. O contratado deve aderir às diretrizes da ISO/IEC 27001, garantindo a gestão eficiente da segurança da informação durante toda a execução do contrato.

5.9.1.2. Implementar controles técnicos e organizacionais para mitigar riscos de acessos não autorizados, vazamentos de dados e interrupções nos serviços.

5.9.2. **Proteção de Dados Sensíveis:**

5.9.2.1. A CONTRATADA deverá assegurar a proteção de todos os dados sensíveis e confidenciais trafegados, processados ou armazenados nos equipamentos fornecidos, utilizando criptografia adequada e outros mecanismos de segurança, em estrita conformidade com a Lei Geral de Proteção de Dados (LGPD).

5.9.2.2. É vedado à CONTRATADA compartilhar, divulgar ou permitir o acesso de terceiros a quaisquer dados sensíveis ou confidenciais, salvo mediante autorização expressa e formal da CONTRATANTE, observadas as disposições legais aplicáveis.

5.9.3. **Gestão de Políticas de Segurança:**

5.9.3.1. A solução fornecida deverá possibilitar a criação, gerenciamento e auditoria de políticas de segurança de forma centralizada, assegurando a rastreabilidade de todas as alterações e acessos.

5.9.3.2. As políticas deverão integrar funcionalidades de IPS (Prevenção contra Intrusões), SD-WAN, controle de aplicações, filtros de conteúdo web e inspeção de tráfego criptografado (SSL/TLS).

5.9.4. **Monitoramento e Resposta a Incidentes:**

5.9.4.1. O sistema deve realizar monitoramento contínuo para identificar e mitigar incidentes de segurança em tempo real.

5.9.4.2. Eventos críticos deverão gerar alertas automáticos e relatórios detalhados, a serem compartilhados com a CONTRATANTE conforme prazos previamente estabelecidos.

5.9.5. **Controle de Acesso:**

5.9.5.1. O acesso ao sistema de gerenciamento do NGFW e demais serviços críticos deverá ser protegido por mecanismos robustos de autenticação, incluindo autenticação multifator (MFA).

5.9.5.2. Os acessos deverão ser controlados por perfis de usuário, com registros completos (logs) de todas as atividades realizadas.

5.9.6. **Tratamento de Dados de Redes Wi-Fi:**

5.9.6.1. A solução deverá garantir a segregação lógica entre os dados trafegados por servidores municipais e cidadãos nas redes Wi-Fi disponibilizadas.

5.9.6.2. É vedada a utilização dos dados coletados ou trafegados na rede Wi-Fi para qualquer finalidade sem autorização formal da CONTRATANTE e em conformidade com a LGPD.

5.9.7. **Backup e Recuperação de Dados:**

5.9.7.1. O sistema deverá realizar backups automáticos e criptografados de todas as configurações, incluindo logs de segurança e políticas implementadas.

5.9.7.2. Deve-se garantir a recuperação rápida e segura dos dados em caso de falhas ou incidentes.

5.9.8. **Educação e Conscientização de Segurança:**

5.9.8.1. A CONTRATADA deverá fornecer materiais educativos ou treinamentos para conscientização dos servidores municipais sobre práticas seguras de navegação, uso de redes Wi-Fi e proteção contra ameaças cibernéticas.

5.9.9. **Auditorias e Testes de Segurança:**

5.9.9.1. Realizar auditorias periódicas no ambiente de segurança implementado, identificando vulnerabilidades e propondo medidas corretivas.

5.9.9.2. Realizar testes de vulnerabilidade e simulações de incidentes para avaliar a eficácia das medidas de proteção e identificar oportunidades de aprimoramento.

5.10. **Requisitos de Sustentabilidade**

5.10.1. **Uso Eficiente de Recursos Energéticos:**

5.10.1.1. Os equipamentos fornecidos, incluindo os dispositivos NGFW, deverão possuir características de eficiência energética, certificadas por padrões internacionais reconhecidos, como Energy Star ou equivalentes.

5.10.1.2. A empresa contratada deverá garantir que os equipamentos operem com consumo energético reduzido, promovendo a sustentabilidade ambiental e diminuindo os custos operacionais.

5.10.2. **Descarte Adequado de Equipamentos Obsoletos:**

5.10.2.1. Todos os equipamentos substituídos durante a vigência do contrato deverão ser descartados de forma responsável e conforme as normas ambientais vigentes, incluindo a Política Nacional de Resíduos Sólidos (PNRS).

5.10.2.2. A contratada deverá apresentar comprovantes de descarte adequado ou reciclagem dos componentes eletrônicos substituídos.

5.10.3. **Redução de Impacto Ambiental no Transporte:**

5.10.3.1. Sempre que possível, as atividades de instalação, manutenção e suporte deverão ser realizadas de forma remota, minimizando deslocamentos físicos e reduzindo a emissão de gases de efeito estufa.

5.10.3.2. Quando o atendimento presencial for indispensável, a empresa contratada deverá priorizar o uso de veículos elétricos ou de baixo consumo energético.

5.10.4. **Promoção de Práticas Digitais Sustentáveis:**

5.10.4.1. O contratado deverá implementar soluções digitais que reduzam o uso de papel, como relatórios, registros de manutenção e documentação de configuração disponibilizados exclusivamente em formato eletrônico.

5.10.4.2. Os sistemas e ferramentas utilizados deverão ser otimizados para minimizar o consumo de banda de rede, evitando desperdícios e sobrecargas desnecessárias.

5.10.5. **Gestão Responsável dos Links de Internet:**

5.10.5.1. A configuração dos links de internet deverá priorizar o uso eficiente dos recursos disponíveis, evitando sobrecargas e consumo desnecessário.

5.10.5.2. O contratado deverá implementar práticas de monitoramento contínuo para garantir que os links estejam sendo utilizados de forma sustentável e equilibrada.

5.10.6. **Capacitação com Enfoque Sustentável:**

5.10.6.1. Os treinamentos oferecidos para a equipe da Prefeitura deverão incluir orientações sobre práticas sustentáveis no uso e gerenciamento dos sistemas e dispositivos de rede.

5.10.6.2. A capacitação deverá enfatizar a importância da economia de recursos, como energia e banda, no contexto de TI sustentável.

5.10.7. **Relatórios de Sustentabilidade:**

5.10.7.1. A contratada deverá apresentar relatórios periódicos sobre ações e práticas sustentáveis implementadas, incluindo:

- Consumo energético dos equipamentos fornecidos.
- Impacto ambiental reduzido pelas operações remotas.
- Quantidade de materiais reciclados ou descartados adequadamente.

5.10.7.2. Esses relatórios deverão ser analisados em conjunto com a contratante para identificar oportunidades adicionais de sustentabilidade.

5.11. Da Exigência de Carta de Solidariedade

5.11.1. Será exigida a apresentação de Carta de Solidariedade, emitida pelo fabricante, como garantia de execução contratual.

5.11.2. A referida carta deverá ser apresentada juntamente com a qualificação técnica da licitante e abranger os seguintes itens da solução ofertada:

- Item 1, do Lote Único;
- Item 2, do Lote Único;
- Item 3, do Lote Único;
- Item 4, do Lote Único.

tório - 029/2025 | (86/232)

5.11.3. A exigência visa assegurar que as licitantes contratadas possuam plenas condições de fornecimento e manutenção dos equipamentos mencionados, garantindo seu pleno funcionamento durante a vigência do contrato.

5.11.4. A exigência busca resguardar a Administração contra eventuais prejuízos decorrentes da indisponibilidade de peças de reposição ou da ausência de suporte técnico necessário para ajustes e aprimoramentos dos equipamentos fornecidos.

5.12. **Subcontratação**

5.12.1. **Critérios para Subcontratação:**

5.12.1.1. A subcontratação de serviços pela empresa contratada será permitida apenas mediante autorização prévia e formal da Prefeitura Municipal de Cáceres.

5.12.1.2. A empresa contratada deverá garantir que a subcontratada possua capacidade técnica comprovada, com experiência e certificações relevantes ao escopo dos serviços a serem executados.

5.12.2. **Responsabilidades da Contratada em Caso de Subcontratação:**

5.12.2.1. A empresa contratada será responsável integralmente pelos serviços executados pela subcontratada, respondendo pelos mesmos padrões de qualidade, prazos e resultados exigidos no contrato.

5.12.2.2. A contratada deverá assegurar que os serviços realizados pela subcontratada estejam em conformidade com todos os requisitos técnicos, normativos e de segurança estabelecidos no contrato.

5.12.2.3. Qualquer prejuízo ou falha decorrente de serviços executados pela subcontratada será de total responsabilidade da empresa contratada, que deverá arcar com os custos e medidas corretivas necessárias.

5.12.3. **Obrigações Adicionais da Subcontratada:**

5.12.3.1. A subcontratada deverá seguir rigorosamente as normas de segurança e privacidade, especialmente aquelas relacionadas à Lei Geral de Proteção de Dados (LGPD).

5.12.3.2. A subcontratada deverá assinar um Termo de Confidencialidade, comprometendo-se a proteger todas as informações relacionadas ao projeto e à infraestrutura da Prefeitura Municipal de Cáceres.

5.12.4. **Limitações e Proibições:**

5.12.4.1. Não será permitido subcontratar o fornecimento de equipamentos essenciais, como os dispositivos NGFW, IA preditiva e softwares de gerenciamento, que deverão ser fornecidos diretamente pela contratada ou pelo fabricante autorizado.

5.12.4.2. Não será permitido subcontratar serviços que envolvam suporte emergencial ou atividades críticas que demandem resposta imediata.

5.12.4.3. A subcontratação de serviços especializados (ex.: treinamento oficial, suporte técnico avançado) somente será permitida se o subcontratado for certificado pelo fabricante da solução NGFW, IA preditiva e softwares de gerenciamento.

5.12.5. **Comunicação e Relatórios:**

5.12.5.1. A empresa contratada deverá notificar previamente a Prefeitura Municipal de Cáceres sobre qualquer intenção de subcontratar serviços, fornecendo informações detalhadas sobre a empresa subcontratada e os serviços a serem realizados.

5.12.5.2. Relatórios detalhados sobre a execução de serviços pela subcontratada deverão ser incluídos nos relatórios periódicos enviados pela empresa contratada.

5.12.6. **Penalidades em Caso de Irregularidades na Subcontratação:**

5.12.6.1. O não cumprimento das condições estabelecidas para subcontratação poderá implicar penalidades contratuais, incluindo advertências, multas ou até rescisão contratual.

5.12.6.2. A Prefeitura Municipal de Cáceres poderá solicitar a substituição imediata da subcontratada caso se identifiquem falhas graves ou descumprimento dos requisitos contratuais.

5.13. Garantia Da Contratação

5.13.1. Não se aplica ao objeto deste Termo de Referência.

5.14. Da Alteração Subjetiva

5.14.1. Não se aplica no presente processo licitatório.

6. PAPÉIS E RESPONSABILIDADES

6.1. Durante o período de vigência do contrato sem prejuízo para as obrigações mencionadas em outros dispositivos deste instrumento ou de qualquer outra obrigação imposta por lei, **serão obrigações da CONTRATANTE**:

6.1.1. Proporcionar à CONTRATADA todas as condições necessárias para a execução dos serviços e entrega dos produtos, incluindo infraestrutura, suporte técnico e informações adicionais de responsabilidade da CONTRATANTE.

6.1.2. Prestar à CONTRATADA todas as informações, esclarecimentos, elementos e dados técnicos necessários ao cumprimento do contrato.

6.1.3. Encaminhar à CONTRATADA todas as solicitações relativas à execução dos serviços e ao fornecimento de produtos, detalhando requisitos, prazos e especificações.

6.1.4. Permitir o acesso de empregados, prepostos ou representantes da CONTRATADA às dependências da Prefeitura Municipal de Cáceres, desde que previamente autorizado e em conformidade com as normas de segurança do local.

6.1.5. Acompanhar e fiscalizar a execução do contrato, designando servidor ou comissão responsável para monitoramento das atividades da CONTRATADA, conforme previsto na Lei nº 14.133/2021.

6.1.6. Garantir que os fiscais designados documentem ocorrências, elaborem relatórios e comuniquem irregularidades à CONTRATADA de forma tempestiva.

6.1.7. Verificar, no prazo fixado, a conformidade dos serviços prestados e produtos entregues, garantindo sua adequação às especificações contratuais.

6.1.8. Rejeitar, total ou parcialmente, serviços ou produtos que não atendam aos requisitos contratuais, comunicando a necessidade de correção ou substituição.

6.1.9. Aplicar as penalidades cabíveis, garantindo a prévia e ampla defesa da CONTRATADA.

6.1.10. Informar imediatamente à CONTRATADA qualquer problema ou irregularidade detectada nos serviços ou produtos fornecidos.

6.1.11. Solicitar, por escrito, a substituição dos serviços que apresentarem desconformidade com o contrato.

6.1.12. Emitir o Termo de Aceite Definitivo após a devida implantação dos serviços contratados.

6.1.13. Atestar as faturas de serviço apresentadas mensalmente pela CONTRATADA.

6.1.14. Manifestar-se, no prazo de 3 dias úteis, sobre as informações contidas na planilha de memória de cálculo fornecida pela CONTRATADA.

6.1.15. Efetuar o pagamento à CONTRATADA no prazo estipulado, desde que todas as obrigações contratuais tenham sido devidamente cumpridas e homologadas.

6.1.16. Promover reuniões periódicas com a CONTRATADA para avaliação do andamento dos serviços, apresentação de relatórios técnicos e resolução de eventuais problemas.

6.1.17. Registrar todas as interações e ocorrências relacionadas ao contrato, garantindo rastreabilidade e acompanhamento das obrigações de ambas as partes.

6.2. Durante o período de vigência do contrato, sem prejuízo para as obrigações mencionadas em outros dispositivos deste instrumento ou de qualquer outra obrigação imposta por lei, **serão obrigações da CONTRATADA**:

6.2.1. Cumprir todas as obrigações previstas no Edital, seus anexos e na proposta apresentada, assumindo integralmente os riscos e as despesas decorrentes da execução do contrato.

6.2.2. Executar o objeto do contrato em sua totalidade, em conformidade com as especificações estabelecidas no Termo de Referência e no contrato firmado.

6.2.3. Efetuar a entrega dos serviços e produtos dentro dos prazos estabelecidos, garantindo que estejam em perfeitas condições e em conformidade com as especificações contratuais.

6.2.4. Acompanhar a entrega dos produtos com a devida nota fiscal, contendo marca, fabricante, modelo, procedência, prazo de garantia ou validade e demais informações exigidas.

6.2.5. Garantir que os serviços e produtos fornecidos sejam de boa qualidade, atendendo integralmente às condições, quantidades e padrões estipulados no contrato.

6.2.6. Resolver prontamente quaisquer falhas ou não conformidades apontadas pela CONTRATANTE, incluindo a substituição ou correção dos serviços e produtos rejeitados.

6.2.7. Manter, durante toda a execução do contrato, as condições de habilitação exigidas, incluindo requisitos técnicos, fiscais, trabalhistas e sociais.

6.2.8. Assumir integralmente as despesas relacionadas à execução do contrato, incluindo tributos, encargos trabalhistas e previdenciários de seus empregados.

6.2.9. Disponibilizar equipe técnica qualificada e apta a atender às demandas durante toda a vigência do contrato.

6.2.10. Implementar práticas de sustentabilidade ambiental, social e econômica na execução dos serviços, conforme princípios legais e normativos aplicáveis.

6.2.11. Permitir à CONTRATANTE a fiscalização da execução dos serviços e fornecimento dos produtos, prestando todos os esclarecimentos solicitados.

6.2.12. Registrar todas as interações e ocorrências relacionadas ao contrato, garantindo rastreabilidade e acompanhamento das obrigações contratuais.

6.2.13. Fornecer canais de atendimento eficientes para comunicação com a CONTRATANTE, garantindo solução ágil para eventuais problemas.

6.2.14. Tomar todas as providências necessárias para implantar e manter os serviços contratados em níveis satisfatórios, de acordo com o IMR e demais disposições contratuais.

6.2.15. Fornecer, sem custo adicional, todos os equipamentos e acessórios necessários à prestação dos serviços nas condições estabelecidas no contrato.

6.2.16. Diagnosticar falhas nos serviços relatadas pela CONTRATANTE e eliminar defeitos nos componentes sob sua responsabilidade.

6.2.17. Sanar quaisquer falhas, degradações ou indisponibilidades do serviço, independentemente de notificação da CONTRATANTE ou detecção via monitoramento proativo.

6.2.18. Executar serviços que acarretem riscos aos sistemas em produção ou requeiram parada de servidores, equipamentos ou rede elétrica somente fora do expediente, incluindo finais de semana e feriados, mediante prévia autorização do Setor de Tecnologia da Informação e Comunicação.

6.2.19. Comunicar à CONTRATANTE, via e-mail e com antecedência mínima de três horas, a presença de seus colaboradores no ambiente da CONTRATANTE, informando nome completo e CPF do técnico para prestação de serviços de instalação ou manutenção.

6.2.20. Fornecer crachá de identificação a seus prepostos durante a realização das atividades no ambiente da CONTRATANTE.

6.2.21. Apresentar mensalmente relatório contendo a planilha de memória de cálculo do faturamento, detalhando:

I) Período de faturamento;
II) Discriminação dos serviços prestados e seus valores;
III) Relação dos eventos, incluindo numeração de chamado, horários de início e término;
IV) Eventos que ensejam descontos contratuais e seus respectivos valores;

V) Totais e subtotais.

6.2.22. Informar, nos relatórios fornecidos, detalhes sobre indisponibilidades ocorridas, incluindo data, período, causas, total de minutos e percentual de disponibilidade do período faturado.

6.2.23. Aplicar os devidos descontos em fatura por descumprimento do IMR, conforme previsto no contrato.

6.2.24. Apresentar mensalmente as faturas dos serviços prestados, acompanhadas da planilha de memória de cálculo definitiva validada pela CONTRATANTE.

6.2.25. Atender a reclamações ou pedidos de esclarecimento relacionados ao faturamento dos serviços contratados.

7. MODELO DE EXECUÇÃO DO OBJETO

7.1. A execução do objeto será conduzida de forma estratégica, visando garantir a plena implementação da solução contratada, conforme os requisitos previamente estabelecidos. A prestação dos serviços envolverá a implantação de um ambiente de segurança cibernética robusto, integrando tecnologias de Firewall de Nova Geração (NGFW), SD-WAN e IA Preditiva, conectividade segura e suporte técnico especializado, de modo a proporcionar alta disponibilidade, eficiência operacional e proteção integral dos ativos digitais da Prefeitura Municipal de Cáceres.

7.2. A prestação do serviço se dará em duas fases, garantindo uma implementação estruturada e um suporte contínuo para a operação da solução contratada, respeitando os prazos estipulados:

7.2.1. **Fase de Implantação** (até 60 dias após a assinatura do contrato):

7.2.1.1. Essa etapa compreende todas as atividades relacionadas à implementação física e lógica da solução. Inclui a instalação e configuração dos equipamentos, ativação dos links dedicados de internet, integração das unidades externas e praças municipais à infraestrutura de comunicação, além da capacitação técnica da equipe da Prefeitura. A fase será concluída com a entrega da documentação técnica detalhada (As Built) e a validação operacional dos serviços prestados.

7.2.1.2. A solução será implantada na sede da Prefeitura e em todas as unidades externas e praças municipais, garantindo conectividade segura e redundante para os serviços essenciais. Para viabilizar a execução adequada, serão instalados e configurados equipamentos de última geração com capacidade para gerenciar múltiplas conexões simultâneas e otimizar o fluxo de dados.

7.2.1.3. A distribuição dos serviços seguirá a estrutura administrativa do município, contemplando unidades estratégicas vinculadas a diversas secretarias. O quantitativo necessário foi dimensionado considerando a demanda operacional de cada local, garantindo que todos os pontos críticos estejam devidamente atendidos. Entre as unidades contempladas, incluem-se:

7.2.1.3.1. **Unidades Centralizadas**

SECRETARIA	UNIDADE	LOCALIZAÇÃO	QUANTIDADE
SMEAE	SMEAE - PREFEITURA SEDE (COC)	https://maps.app.goo.gl/qTzbhDM8NCAEBxBf7	2

	UNIDADE CENTRALIZADA 1		1
	UNIDADE CENTRALIZADA 2		1
SMA	SMA - ALMOXARIFADO	https://maps.app.goo.gl/NiAhRcuDi3oF6Qvn9	1
	SMA - GUARDA MUNICIPAL	https://maps.app.goo.gl/hoMkt4EuyDL3BrFKA	1
SMAGRI	SMAGRI	https://maps.app.goo.gl/J1rDH3pp4oPSEfsj7	1
SMASC	SMASC - CCI	https://maps.app.goo.gl/j8UjTvfKLx4ypbPs5	1
SME	SME - CMEC	https://maps.app.goo.gl/ZUD6oU9HeMvLqXe89	1
SMIL	SMIL - GUARITA OBRAS	https://maps.app.goo.gl/PTWC8Lr3aGwXPxnP9	1
	SMIL - GUARITA PORTICO	https://maps.app.goo.gl/u39WX2UzVeVQQWS28	1
	SMIL - OFICINA	https://maps.app.goo.gl/wQmT4CxnPbdKZUYC9	1
TOTAL			**12**

7.2.1.3.2. **Unidades Descentralizadas**

SECRETARIA	UNIDADE	LOCALIZAÇÃO	QUANTIDADE
SMEAE	SMEAE - DEFESA CIVIL	https://maps.app.goo.gl/zYaMoX5jtfJ1VQ2h8	1
	UNIDADE DESCENTRALIZADA 1	-	1
SMA	SMA - ARQUIVO	https://maps.app.goo.gl/n6Jj6YzpqNfS8cHF7	1
	UNIDADE DESCENTRALIZADA 2	-	1
SMASC	SMASC - ALMOXARIFADO	https://maps.app.goo.gl/CZV2nUAkbYMhY6uq9	1
	SMASC - CASA BELBELITA	https://maps.app.goo.gl/DxddTbATc7X73Bns5	1
	SMASC - CASA DE PASSAGEM	https://maps.app.goo.gl/WrVThbciHZooSfgX6	1
	SMASC - CENTRO DE MULTIPLO USO	https://maps.app.goo.gl/Lz5UoPyGg42jrnUn8	1
	SMASC - CONSELHO TUTELAR	https://maps.app.goo.gl/tyQnNc8nTmMfQ3MW7	1
	SMASC - CRAS I	https://maps.app.goo.gl/xPiY5KnmduNnBgK49	1
	SMASC - CRAS II	https://maps.app.goo.gl/HPNPDMJ2U98R5tRm8	1
	SMASC - CREAS	https://maps.app.goo.gl/xoJqeaMyfF9Ds6g19	1
	SMASC - SAICA	https://maps.app.goo.gl/CCwLfifR6sWyhhdm7	1
	SMASC - GANHA TEMPO	https://maps.app.goo.gl/5AXCG6MYtbiF1gwV7	1
	UNIDADE DESCENTRALIZADA 3	-	1
SME	SME - SECRETARIA DE EDUCAÇÃO	https://maps.app.goo.gl/WbNKuCbpt1rDS5TE7	1
	SME - MERENDA	https://maps.app.goo.gl/byhFeQxucnAjkWfH8	1
	SME - CENTRO MUNICIPAL DE EDUCAÇÃO INFANTIL	https://maps.app.goo.gl/r9P3FHMDnqK3KTGUA	1
	SME - EM 16 DE MARÇO	https://goo.gl/maps/irEBgMynkLFUVdqDA	1
	SME - EM BRINCANDO E APRENDENDO	https://goo.gl/maps/qUYuASgJv5KN9z9v6	1
	SME - EM BURITI	https://goo.gl/maps/oJLMV4MMGaWkxdi7A	1
	SME - EM BUSCANDO O	https://maps.app.goo.gl/52UwvjnQcLHDWQ7k6	1

	SABER		
	SME - EM CENTRO EDUCACIONAL DOM MÁXIMO BIENNÉS	https://goo.gl/maps/BDNwB6uZWrEapfWx5	1
	SME - EM DES. GABRIEL PINTO DE ARRUDA	https://goo.gl/maps/BDCMfHEfwrEELscN9	1
	SME - EM DR. JOSÉ RODRIGUES FONTES	https://maps.app.goo.gl/gN8iVN15FtGRnxbB9	1
	SME - EM DUQUE DE CAXIAS	https://goo.gl/maps/s5PAoUDUNHedzdks6	1
	SME - EM FAZENDO ARTE	https://maps.app.goo.gl/kTP6RNoQeYxuAfPNA	1
	SME - EM GARCÊS	https://goo.gl/maps/3J1HfZuFZ9v5WEcj9	1
	SME - EM GOTINHAS DO SABER	https://goo.gl/maps/mYM52pa2QkFA2j2C9	1
	SME - EM JARDIM GUANABARA	https://goo.gl/maps/Rfg8wh2T7iw4NrbP6	1
	SME - EM JARDIM PARAÍSO	https://goo.gl/maps/kkyMp6LAXieSyvPW9	1
	SME - EM NOVO ORIENTE	https://maps.app.goo.gl/4gacByZXhJ48UMvt5	1
	SME - EM PEQUENO SÁBIO	https://goo.gl/maps/EMEBFPffRm6Tb62a8	1
	SME - EM PROF. EDUARDO BENEVIDES LINDOTE	https://goo.gl/maps/Y43ifBkKTAwNN1U86	1
	SME - EM PROFª ISABEL CAMPOS	https://goo.gl/maps/1MgqjESG46yCxwe88	1
	SME - EM PROFA. ERENICE SIMÃO ALVARENGA	https://goo.gl/maps/yo4E1htCJ5EJYWE48	1
	SME - EM RAQUEL RAMÃO DA SILVA	https://goo.gl/maps/ke1dUMYCGWqwve6P8	1
	SME - EM SANTOS DUMONT	https://goo.gl/maps/uyBXsZNDDszodCxk6	1
	SME - EM TANCREDO NEVES	https://goo.gl/maps/fKVomd6j3LZtfjkS8	1
	SME - EM VILA IRENE	https://goo.gl/maps/aGdb2PV6NF3Yoxhe7	1
	SME - EM VILA REAL	https://goo.gl/maps/dfKNaDkEfK2V8YiJ8	1
	SME - EM VITÓRIA RÉGIA	https://goo.gl/maps/vP5EUrdTiHhhw13y6	1
	SME - EMEI FREI GRIGNION	https://goo.gl/maps/LmB1VSuePV8FtSXHA	1
	SME - EMEI IRENE COELHO CRUZ	https://goo.gl/maps/BiLhvdeg1tRmiuR37	1
	SME - EMEI MADRE MARIA ESTEVÃO	https://goo.gl/maps/kRXo9FN7eFvufAaV8	1
	SME - EMEI PROFESSORA DULSÂNGELA DE ALMEIDA SOUZA	https://maps.app.goo.gl/QZKQCN7SU9D2qwgd8	1
	SME- LIMOEIRO	https://goo.gl/maps/nrqaUDmiZV3xDpUN9	1
	SME - NOSSA SENHORA APARECIDA	https://goo.gl/maps/uYpxYHJzCmm6Qo1w8	1
	SME - PAULO FREIRE	https://maps.app.goo.gl/DE7sbzdMQVbaQXS77	1
	SME - PROFª LÉA MARIA LARA SILVA	https://maps.app.goo.gl/pjrMdwiU6wSSn3Uf7	1
	SME - PROVÍNCIA DE AREZZO	https://goo.gl/maps/NSNEbdrq1cjknywX8	1

	SME - ROÇA VELHA	https://goo.gl/maps/fGfEoY7trAGZhmS9A	1
	SME - SANTA CATARINA	https://goo.gl/maps/VzU6r8C8TVQJc3RM7	1
	SME - SANTO ANTÔNIO DO CARAMUJO	https://goo.gl/maps/ducAKNjzSQXECMHj9	1
	SME - SOTECO	https://maps.app.goo.gl/P32RY2iPJR7VLC9p7	1
	SME - TRANSPORTE EDUCAÇÃO	https://maps.app.goo.gl/cQumZ9jvaygvLQ159	1
	SME - EM UNIÃO	https://goo.gl/maps/zxtNZfD4YSyKrDVk8	1
	SME - CLARINÓPOLIS	https://goo.gl/maps/ducAKNjzSQXECMHj9	1
	SME - INFRAESTRUTURA EDUCAÇÃO	https://maps.app.goo.gl/b3bCUzB8qwz7vRd77	1
	SME - LARANJEIRA I	https://goo.gl/maps/jB1SZ3za3cdYev4a6	1
	SME - SÃO FRANCISCO	https://maps.app.goo.gl/sxzj1LsfxkFEX7Zy6	1
	UNIDADE DESCENTRALIZADA 4	-	1
	UNIDADE DESCENTRALIZADA 5	-	1
	UNIDADE DESCENTRALIZADA 6	-	1
	UNIDADE DESCENTRALIZADA 7	-	1
SMMADE	SMMADE	https://maps.app.goo.gl/zYaMoX5jtfJ1VQ2h8	1
	UNIDADE DESCENTRALIZADA 8	-	1
SMEL	SMEL - CIE	https://maps.app.goo.gl/Kkk4g4zUipLG7RDw6	1
	SMEL - DIDI PROFETA	https://maps.app.goo.gl/wUmbU83AgrRCFAjy6	1
	UNIDADE DESCENTRALIZADA 9	-	1
SMIL	SMIL - AEROPORTO	https://maps.app.goo.gl/N6nKAp5k4TpbGE1n6	1
	UNIDADE DESCENTRALIZADA 10	-	1
SMS	SMS - SECRETARIA DE SAUDE	https://maps.app.goo.gl/VWf4EYS5mnNdMk85A	1
	SMS - CAPS, AMBULATÓRIO DERMATOLÓGICO, LABORATORIO MUNICIPAL, ALMOXARIFADO, CMS	https://maps.app.goo.gl/3YsQdJ4PJUVqd6nG7	1
	SMS - CAPSI INFANTO JUVENIL	https://maps.app.goo.gl/NRE6n76fGEMAzeyy9	1
	SMS - CENTRO DE ESPECIALIDADES MEDICAS CEM	https://maps.app.goo.gl/zkjGjchEE1wsL14r8	1
	SMS - CENTRO DE SAUDE REFERENCIAL	https://maps.app.goo.gl/Z5MEaMJi68dU5hrG6	1
	SMS - CENTRO REAB DOM AQUINO CORREA CACERES CER II	https://maps.app.goo.gl/VhCQc4YayPyXp7sj8	1
	SMS - CEO	https://maps.app.goo.gl/wZMwZd1mfqVrkuRW6	1
	SMS - CTA CENTRO DE TESTAGEM E ACONSELHAMENTO SAE CACERES	https://maps.app.goo.gl/QPC3oTbJjodwapDV7	1

	SMS - FARMACIA BASICA DA SMS	https://maps.app.goo.gl/YwUSzHzPiKE5h3Vy8	1
	SMS - FROTAS	https://maps.app.goo.gl/UQZEQZxDpudbq1wH7	1
	SMS - POSTO DE SAUDE DA PAIOL	https://maps.app.goo.gl/PHsDSTgdLW1CdkacA	1
	SMS - POSTO DE SAUDE DE VILA APARECIDA	https://maps.app.goo.gl/uGRnxEjReD6jHpJ9A	1
	SMS - POSTO DE SAUDE DO LIMAO	https://maps.app.goo.gl/CfPip6ysDGqhiWmT6	1
	SMS - POSTO DE SAUDE HORIZONTE DOESTE	https://maps.app.goo.gl/6bkzEYMH7wQsigL49	1
	SMS - POSTO DE SAUDE LARANJEIRAS	https://maps.app.goo.gl/XpkQdasWsWE86U9q6?g_st=aw	1
	SMS - POSTO DE SAUDE PROF VERA LYGIA BALDO FACAO	https://maps.app.goo.gl/f6PfkXjMQjTudKqZ8	1
	SMS - POSTO DE SAUDE SADIA	https://maps.app.goo.gl/H29oLsoimParvAwv8	1
	SMS - UNID DE SAUDE DA FAMILIA VISTA ALEGRE	https://maps.app.goo.gl/FirXbqEx2srZf787A	1
	SMS - UNID SAUDE DA FAMILIA VITORIA REGIA	https://maps.app.goo.gl/mZmvrRyEijHAnTFY7	1
	SMS - UNIDADE BASICA DE SAUDE DR ADEMAR ROCHA DE OLIVEIRA CAVALHADA	https://maps.app.goo.gl/8gjpYWP87HBqcoZ46	1
	SMS - UNIDADE BASICA DE SAUDE JARDIM DAS OLIVEIRAS	https://maps.app.goo.gl/tT5o6Y7N38AVLUkZ9	1
	SMS - UNIDADE BASICA DE SAUDE SANTA ISABEL	https://maps.app.goo.gl/kUwep6ZQ8h7MucdX7	1
	SMS - UNIDADE DE SAUDE DA FAMILIA COHAB NOVA	https://maps.app.goo.gl/2dwof9LpsMAPALtM7	1
	SMS - UNIDADE DE SAUDE DA FAMILIA DO CAIC	https://maps.app.goo.gl/oJAf3xrRqWLe5Jev8	1
	SMS - UNIDADE DE SAUDE DA FAMILIA DO RODEIO	https://maps.app.goo.gl/2jADTBF6EXEvx9Ew6	1
	SMS - UNIDADE DE SAUDE DA FAMILIA JD PARAISO	https://maps.app.goo.gl/TdhriFPJ8nPUpFVx6	1
	SMS - UNIDADE DE SAUDE DA FAMILIA VILA REAL	https://maps.app.goo.gl/E1nPn9mTybVmcB267	1
	SMS - UNIDADE DE SAUDE SANTOS DUMONT	https://maps.app.goo.gl/oZuia8p4RaSbPKzP7	1
	SMS - UNIDADE DE SAUDE UNIVERSITÁRIO	https://maps.app.goo.gl/vYJEuN1ufGKzoEeK7	1
	SMS - UNIDADE SAUDE FAMILIA DO CARAMUJO	https://maps.app.goo.gl/zhXa1oX3UQzTwcHj9	1
	SMS - UNIDADE SAUDE FAMILIA JARDIM	https://maps.app.goo.gl/bRE93W32464phEPJ7	1

	GUANABARA		
	SMS - UPA PRONTO ATENDIMENTO JOSE SOUTO FARIAS	https://maps.app.goo.gl/mgaRTmkRznLoMFrY7	1
	SMS - VIGILANCIA EM SAÚDE	https://maps.app.goo.gl/YJFGaUT4mc3VeFoV6	1
	UNIDADE DESCENTRALIZADA 11	-	1
	UNIDADE DESCENTRALIZADA 12	-	1
	UNIDADE DESCENTRALIZADA 13	-	1
	UNIDADE DESCENTRALIZADA 14	-	1
SMTC	SMTC	https://maps.app.goo.gl/sMPDMtU3poAP51LF7	1
	SMTC - CASA DAVERON	https://maps.app.goo.gl/fHqLcuW2X5nJCHBv6	1
	SMTC - BIBLIOTECA	https://maps.app.goo.gl/6cGeYMDAR1YMQXTX6	1
	SMTC - CLUBINHO 2000	https://maps.app.goo.gl/vaUxdTdcihpHVacH9	1
	SMTC - MUSEU	https://maps.app.goo.gl/kKvwGsx58CZmAqDfA	1
	UNIDADE DESCENTRALIZADA 15	-	1
TOTAL			**115**

7.2.1.3.3. **Praças Públicas**

SECRETARIA	PRAÇA	LOCALIZAÇÃO	QUANTIDADE
SMEAE	SMEAE - AROLDO FANAIA	https://maps.app.goo.gl/8J86ycmMgagCRjCb6	1
	SMEAE - COHAB VELHA	https://maps.app.goo.gl/ExPmvCxJtbZ6Tsxk6	1
	SMEAE - PRAÇA BENJAMIN CONSTANT	https://goo.gl/maps/Bp9fHEKnFKQ4shkB7	1
	SMEAE - PRAÇA CARAMUJO	https://maps.app.goo.gl/7h6GapqJ9cnAkc8T7	1
	SMEAE - PRAÇA CIDADE ALTA	https://goo.gl/maps/MxXmDgoFqVtZdNex8	1
	SMEAE - PRAÇA CIDADE NOVA	https://maps.app.goo.gl/W8wgiTyN45SChQ9d8	1
	SMEAE - PRAÇA COHAB NOVA	https://goo.gl/maps/7xNnbDpDas9VePnN9	1
	SMEAE - PRAÇA DA FEIRA - CENTRO	https://goo.gl/maps/sjqGYtg7KatQcwcZ8	1
	SMEAE - PRAÇA DNER - BOMBEIROS	https://goo.gl/maps/3tgxS4Uz2pnsdPxH9	1
	SMEAE - PRAÇA DO GERALDÃO	https://goo.gl/maps/iGDeEFGjFZqQ3ct79	1
	SMEAE - PRAÇA DO MONTE VERDE	https://goo.gl/maps/VDYK2HWXctL7tgmV6	1
	SMEAE - PRAÇA DOM MÁXIMO	https://goo.gl/maps/om21uh8nLLWQdJs1A	1
	SMEAE - PRAÇA DUQUE DE CAXIAS - CENTRO	https://goo.gl/maps/sjqGYtg7KatQcwcZ8	1
	SMEAE - PRAÇA HORIZONTE D'OESTE	https://maps.app.goo.gl/yNFf1xADWNWK6NkZ6	1
	SMEAE - PRAÇA JARDIM AEROPORTO	https://goo.gl/maps/W6oEg6qd6pwi7MwF9	1

	SMEAE - PRAÇA JARDIM DA OLIVEIRA (EMPA)	https://maps.app.goo.gl/Z1yuZWjrLsYP5jwP7	1
	SMEAE - PRAÇA JARDIM PARAISO	https://maps.app.goo.gl/pYiSUbjpqciUhE3N9	1
	SMEAE - PRAÇA JARDIM SÃO LUIZ	https://maps.app.goo.gl/nBF5xryfXZoMWjUQ9	1
	SMEAE - PRAÇA JARDIM UNIVERSITÁRIO III	https://goo.gl/maps/ofActSaScSGdXz4R6	1
	SMEAE - PRAÇA JOSÉ DE ANCHIETA	https://goo.gl/maps/A8WHwD7BX6NUWhJT6	1
	SMEAE - PRAÇA JUNCO	https://maps.app.goo.gl/qXAReBWJ7BQRPpkM9	1
	SMEAE - PRAÇA MAJOR JOÃO CARLOS	https://goo.gl/maps/Qcwdn4CXJdT5VCWQ6	1
	SMEAE - PRAÇA MEDEIROS	https://goo.gl/maps/HUThKqHzuPa6ABpEA	1
	SMEAE - PRAÇA NOVA ERA (CAMPO)	https://maps.app.goo.gl/YQKX7SBhzB9dcjcj9	1
	SMEAE - PRAÇA PANTANAL	https://goo.gl/maps/AUKWENW5iR2gENDT7	1
	SMEAE - PRAÇA RESIDENCIAL ANA PAULA	https://goo.gl/maps/pA2tyTfhq8jqo5Fk7	1
	SMEAE - PRAÇA SANTA CRUZ	https://maps.app.goo.gl/KFsn7XrjbpDGFV1X9	1
	SMEAE - PRAÇA SANTA ISABEL	https://maps.app.goo.gl/TBJYXELoqvGd7Lkm9	1
	SMEAE - PRAÇA SANTO ANTONIO	https://maps.app.goo.gl/Tu2hhrXUFw4rSABn6	1
	SMEAE - PRAÇA SÃO JORGE	https://goo.gl/maps/MxXmDgoFqVtZdNex8	1
	SMEAE - PRAÇA SÃO LOURENÇO (CAMPO)	https://maps.app.goo.gl/bouowePQbhfCzuRm7	1
	SMEAE - PRAÇA SÃO MIGUEL	https://goo.gl/maps/TeYnV6RyQdD3d4Zo8	1
	SMEAE - PRAÇA VALTER FIDELIS - VILA REAL	https://maps.app.goo.gl/PyeiqkA6niDZH3hE9	1
	SMEAE - PRAÇA VILA APARECIDA	https://maps.app.goo.gl/Cjpoxp8VnhRTkBMa9	1
	SMEAE - PRAÇA VILA REAL	https://maps.app.goo.gl/Yp8X21VytfkPPvgw6	1
	SMEAE - PRAÇA VITÓRIA RÉGIA	https://goo.gl/maps/mJXKjDVQASbukgY37	1
	SMEAE - RODOVIÁRIA	https://maps.app.goo.gl/8LyQniCzZ74f3oCC7	1
	SMEAE - SADIA	https://maps.app.goo.gl/tc1GB5cCztjYFNtm9	1
	PRAÇA MUNICIPAL 1		1
	PRAÇA MUNICIPAL 2		1
	PRAÇA MUNICIPAL 3		1
	PRAÇA MUNICIPAL 4		1
SMTC	SMTC - PALCO DE EVENTOS SEMATUR	https://maps.app.goo.gl/WsUtv8cTtAgazbeP9	1
	SMTC - PRAÇA BARÃO	https://maps.app.goo.gl/vP3qT3xGyzzbTkVf8	1
	PRAÇA MUNICIPAL 5		1
	PRAÇA MUNICIPAL 6		1
TOTAL			**46**

7.2.2. **Fase de Prestação de Serviço Mensal** (até 180 meses após a assinatura do contrato):

7.2.2.1. Após a implantação, será iniciada a fase de operação contínua da solução, garantindo a manutenção preventiva e corretiva dos equipamentos, suporte técnico especializado, monitoramento em tempo real da infraestrutura de segurança cibernética e otimização do tráfego de rede com a tecnologia SD-WAN. Essa fase inclui a prestação de serviços de segurança cibernética baseada em Inteligência Artificial Preditiva, bem como a consultoria contínua para aprimoramento da política de segurança da informação do município.

7.3. Além da estruturação física, a execução do contrato incluirá a implantação de links dedicados de internet para garantir alta disponibilidade, com redundância de ASN e rotas distintas, estabilidade para os serviços administrativos e operacionais e alternativa de contingência para evitar interrupções nos serviços

7.4. O serviço de Link de Internet para as localidades que serão contempladas com WI-FI Social deverá ser implantado impreterivelmente em até 30 (trinta) dias a partir da ordem de serviço emitida pelo Gestor do Contrato.

7.5. Para o **Lote único** a CONTRATADA deverá cumprir os eventos descritos na tabela a seguir, respeitando os prazos máximos estabelecidos

MARCOS DIA	PRAZOS MÁXIMOS (EM DIAS)	EVENTO	RESPONSÁVEL
D0		Assinatura do contrato entre o CONTRATANTE e a empresa licitante vencedora.	CONTRATANTE e a CONTRATADA
D1		Emissão da Ordem de Serviço pelo CONTRATANTE	CONTRATANTE
D2	D1+2	Entrega do projeto executivo	CONTRATADA
D3	D2+2	Aprovação do projeto executivo	CONTRATANTE
D4	D1+15	Entrega dos link de Internet e WI-FI nas praças, contemplando toda a solução de segurança de SDWAN e NGFW	CONTRATADA
D5	D4+3	Emissão do Termo de Recebimento provisório, para início da conferência do serviço entregue dos Links de Internet das praças	CONTRATANTE
D6	D5+5	Emissão do Termo de Recebimento Definitivo, autorização para emissão de faturamento e início do período de execução dos serviços dos Links de Internet das praças	CONTRATANTE
D7	D1+60	Conclusão da entrega, instalação e configuração dos equipamentos, capacitação e operacionalização de todos os links de comunicação, Firewall, IA Preditiva, sensores de cibersegurança, SDWAN, NGFW	CONTRATADA
D8	D7+3	Emissão do Termo de Recebimento provisório, para início da conferência do serviço entregue.	CONTRATANTE
D9	D8+5	Emissão do Termo de Recebimento Definitivo, autorização para emissão de faturamento e início do período de execução dos serviços de links de comunicação, Firewall, Sensores de Cibersegurança, SDWAN, NGFW	CONTRATANTE

7.6. A instalação da solução será realizada por uma empresa homologada e credenciada, com compromisso solidário ao fabricante, garantindo a fluidez da implantação dentro do prazo estipulado no edital. Para assegurar a operacionalidade da solução, serão promovidas capacitações técnicas para a equipe da Prefeitura, visando aprimorar a gestão e monitoramento dos sistemas implementados.

7.7. O modelo de execução do objeto visa garantir não apenas a segurança cibernética e a conectividade da administração pública municipal, mas também a eficiência na prestação de serviços essenciais à população, promovendo inovação, resiliência e modernização tecnológica.

8. MODELO DE GESTÃO DO CONTRATO

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

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

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

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

8.5. Após a assinatura do contrato ou instrumento equivalente~~,~~ o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

8.6. **Fiscalização**

8.6.1. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput), nos termos do Decreto nº 665 de 09 de outubro de 2024.

8.6.2. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração (Decreto nº 11.246, de 2022, art. 22, VI);

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

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

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

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

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

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

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

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

8.6.5. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

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

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

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

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

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

9. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

9.1. Forma de Acompanhamento da Garantia e Níveis de Serviço

9.1.1. Para cumprir com os níveis de disponibilidade a prestadora de serviços deve trabalhar com duas variáveis principais: o MTBF (Tempo médio entre falhas) da solução, e o MTTR (Tempo médio de reparação de falhas). Para aumentar a disponibilidade deve-se aumentar o MTBF e diminuir o MTTR, de forma que o sistema apresente falhas com menor frequência e que estas sejam recuperadas mais rapidamente.

Abaixo estão listados os valores de disponibilidade mensal para cada Item deste Termo:

LOTE	ITEM	SERVIÇO	DISPONIBILIDADE
1 (ÚNICO)	1	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)	99,8%
	2	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	99,8%
	3	Serviço de Link dedicado de Acesso à internet, bloco /29 e Banda Mínima de Acesso Garantida de 500Mbps (Alta Disponibilidade) SEDE (Dois Link de ASN e Rota Diferentes)	99,8%
	4 5	Serviço de Link de acesso à Internet Sites Remotos, aplica-se ao WIFI Social	99,2%

9.2. Nas planilhas abaixo estão detalhados todos os indicadores destinados à aferição dos níveis mínimos de serviço da contratação pretendida. Na apuração dos indicadores poderão ser confrontados os dados da solução de gerenciamento da CONTRATADA e do sistema de monitoramento da CONTRATANTE.

MÉTRICA 1 - DISPONIBILIDADE (IMR-01)	
Indicador de Qualidade	Índice de Disponibilidade.
Métrica	Indicador é calculado com a seguinte forma: **IDM=[(To - Ti)/To]*100** Onde: IDM = índice de disponibilidade mensal do LINK em % To = período de operação (um mês) em minutos. Ti = somatório dos tempos de inoperância durante o período de operação (1 mês) em minutos. No caso de inoperância reincidente num período inferior a 3 horas, contado a partir do restabelecimento

	do link da última inoperância, considerar-se-á como tempo de indisponibilidade do enlace o início da primeira inoperância até o final da última inoperância, quando o link estiver totalmente operacional. Os tempos de inoperância serão os tempos em que os links apresentarem problemas que serão obtidos dos chamados abertos no sistema de abertura de chamados técnicos (Trouble Ticket) e os tempos de indisponibilidade computados pela violação do indicador de Retardo. Somente serão desconsiderados os tempos de inoperância causados por manutenções programadas com o CONTRATANTE, ressalvados, contudo, os casos fortuitos e de força maior.
Periodicidade de Aferição	Mensal
Limiar de Qualidade	Vide Item 9.1 - Forma de Acompanhamento da Garantia e Níveis de Serviço
Pontos de Controle	A CONTRATADA realizará, por meio da sua solução de gerenciamento, a coleta e o armazenamento de informações a respeito de todos os serviços pelo tempo de duração do contrato.
Relatórios de Níveis de Serviço	A CONTRATADA deverá disponibilizar mensalmente à CONTRATANTE, relatórios com os índices apurados, totalizados e apresentados mensalmente por serviço. Nos relatórios citados deverão ser apresentados: o número do ticket, tempo de indisponibilidade (horas e minutos), o tempo de interrupções programadas, o tempo de interrupções de responsabilidade da CONTRATANTE. A CONTRATADA deverá disponibilizar, quando demandada pelo CONTRATANTE, relatório detalhando os tempos de falhas (com hora de início e fim da inoperância), minutos excedentes ao prazo máximo para reparo e disponibilidade no período (mês) e motivo(s) da(s) indisponibilidade(s) apurada(s). Após análise do fiscal técnico, poderá ser desconsiderado do período de inoperância, o tempo decorrente da impossibilidade da CONTRATADA acessar os equipamentos nas instalações da CONTRATANTE, comprovando a CONTRATADA que o problema estava nas dependências da CONTRATANTE.

MÉTRICA 2 - TAXA DE ERRO (IMR-02)	
Indicador de Qualidade	Percentual de erros nos enlaces.
Métrica	Indicador é calculado com a seguinte fórmula: $\mathbf{TER = (QEQ / TTQ)* 100}$ Sendo: TER = Indicador de taxa de erro; TTQ = Quantidade total de quadros enviados ou recebidos em um determinado período; QEQ = Quantidade de erros identificados em um determinado período. Para efeito de mensuração desta métrica utiliza-se as seguintes considerações: • Quadro é a unidade de transferência de dados na camada de enlace do modelo OSI, ou seja, o frame Ethernet; • Os erros devem ser reportados pelo roteador da CONTRATADA utilizado na conexão com a rede da CONTRATANTE; • Serão considerados os erros em ambas as interfaces de ingresso e egresso no roteador da CONTRATADA.
Periodicidade de Aferição	Esta métrica deverá ser aferida, ininterruptamente, em intervalos de 5 minutos.
Limiar de Qualidade	0,5%
Pontos de Controle	O período utilizado no cálculo da métrica e, quando for o caso, o período considerado como indisponível será o do intervalo entre as aferições

MÉTRICA 3 - LATÊNCIA (IMR-03)

Indicador de Qualidade	Tempo de latência de ida e volta do pacote através do link contratado
Métrica	A latência deve mensurar o tempo do trajeto de ida-e-volta (RTT - round trip time) de um pacote do tipo ICMP com tamanho de 1000 bytes. Para efeito de mensuração desta métrica utiliza-se as seguintes considerações: • Para os links Internet, as medições de latência devem ser feitas entre o Roteador Internet ou Appliance SD-WAN e o primeiro roteador da CONTATADA na Internet. • Pacote é a unidade de transferência de dados na camada de redes do modelo OSI, ou seja os datagramas TCP, UDP, ICMP e ARP; • O envio de pacotes para obtenção dos quantitativos utilizados no cálculo desta métrica deve ocorrer entre dois pontos distintos e remotos, um localizado no segmento de rede da CONTRATANTE onde estiver conectado o roteador da CONTRATADA, e outro localizado em segmento de rede de terceiros que estejam ligados a Internet por meio da rede da mesma CONTRATADA, ou em segmento de rede utilizado para troca de tráfego entre de operadoras de acesso à Internet (Pontos de Troca de Tráfego), podendo inclusive, tratar-se dos roteadores de borda da CONTRATADA conectados aos segmentos aqui mencionados. Serão desconsiderados os períodos em que os valores mensurados ultrapassem o limite aceitável desta métrica, caso a volume médio de utilização do link no mesmo período seja superior a 80% da velocidade do respectivo enlace.
Mínimo aceitável	Links de Internet: 65 ms
Periodicidade Aferição	Esta métrica deverá ser aferida, ininterruptamente, em intervalos de 5 minutos. O período utilizado no cálculo da métrica será o período do intervalo entre as aferições

MÉTRICA 4 – PERDA DE PACOTES (IMR-04)	
Indicador de Qualidade	Percentual de perda de pacotes IP ao longo da rede da CONTRATADA em um determinado período.
Métrica	Indicador é calculado com a seguinte forma: **TPP = (QPP / QTP)* 100** Sendo: TPP = Indicador de perda de pacotes QTP = Quantidade total de pacotes enviados ou recebidos em um determinado período QPP = Quantidade de pacotes perdidos em um determinado período Para efeito de mensuração desta métrica utiliza-se as seguintes considerações: • Pacote é a unidade de transferência de dados na camada de redes do modelo OSI, ou seja os datagramas TCP, UDP, ICMP e ARP; • O envio de pacotes para obtenção dos quantitativos utilizados no cálculo desta métrica deve ocorrer entre dois pontos distintos e remotos, um localizado no segmento de rede da CONTRATANTE onde estiver conectado o roteador da CONTRATADA, e outro localizado em segmento de rede de terceiros que estejam ligados a Internet por meio da rede da mesma CONTRATADA, ou em segmento de rede utilizado para troca de tráfego entre de operadoras de acesso à Internet (Pontos de Troca de Tráfego), podendo inclusive, tratar-se dos roteadores de borda da CONTRATADA conectados aos segmentos aqui mencionados. Serão desconsiderados os períodos em que os valores mensurados ultrapassem o limite aceitável desta métrica, caso a volume médio de utilização do link no mesmo período seja superior a 80% da velocidade do respectivo enlace.
Máximo aceitável	3% de perda
Periodicidade Aferição	Esta métrica deverá ser aferida, ininterruptamente, em intervalos de 5 minutos. O período utilizado no cálculo da métrica será o período do intervalo entre as aferições.

MÉTRICA 5 – PRAZO PARA ALTERAÇÃO DE CONFIGURAÇÃO DOS EQUIPAMENTOS SOLICITADOS PELO CONTRATANTE	
Indicador de Qualidade	Prazo, em horas, para a contratada alterar a configuração dos equipamentos solicitada pelo CONTRATANTE.
Métrica	Apuração mensal do tempo que a contratada executa e apresente uma alteração na configuração de equipamentos, a partir do momento do registro da solicitação de alteração da configuração na base de dados relativa à solução de gerenciamento do Provedor e de comparação com o valor do Limiar de Qualidade desta tabela. **PA = Taa – Tsa** onde: PA = Prazo de alteração da configuração de equipamentos Taa = Instante da aceitação pela da alteração Tsa = Instante da solicitação da alteração
Periodicidade de Aferição	Mensal
Limiar de Qualidade	Prazo máximo: 48 horas após a solicitação de alteração da configuração pela CONTRATANTE. Em caso de agendamento pelo CONTRATANTE este prazo ficará suspenso.
Pontos de Controle	De acordo com os registros na Central de Atendimento.
Relatórios de Níveis de Serviço	A CONTRATADA deverá disponibilizar mensalmente à CONTRATANTE, relatórios com os índices apurados, totalizados e apresentados mensalmente por serviço. Nos relatórios citados deverão ser apresentados: o número do ticket, tempo de indisponibilidade (horas e minutos), o tempo de interrupções programadas, o tempo de interrupções de responsabilidade da CONTRATANTE.
Descontos	Para cada 1 (uma) hora acima do Prazo para Alteração de Configuração de Equipamentos (PAC), será implicado à contratada desconto correspondente a 2,0% (dois por cento), calculado sobre o valor mensal do circuito afetado. O referido desconto deverá ser retratado nos relatórios de prestação dos serviços, junto ao faturamento, apresentados mensalmente por enlace.

9.3. **Recebimento do Objeto**

9.3.1. A emissão do Termo de Recebimento Definitivo é o marco inicial da efetiva prestação do serviço contratado, nas condições em que foram definidas pela CONTRATANTE neste instrumento.

9.3.2. Os serviços serão recebidos provisoriamente, no prazo de até 3 (três) dias, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. (Art. 140, I, a , da Lei nº 14.133 e Arts. 22, X e 23, X do Decreto nº 11.246, de 2022);

9.3.2.1. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda do contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.

9.3.2.2. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico. (Art. 22, X, Decreto nº 11.246, de 2022);

9.3.2.3. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo. (Art. 23, X, Decreto nº 11.246, de 2022)

9.3.2.4. O fiscal setorial do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo.

9.3.3. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato:

9.3.3.1. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

9.3.3.2. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório. (Art. 119 c/c art. 140 da Lei nº 14133, de 2021)

9.3.3.3. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

9.3.3.4. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

9.3.4. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

9.3.5. Os serviços serão recebidos definitivamente no prazo de 7(sete) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

9.3.5.1. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento (art. 21, VIII, Decreto nº 11.246, de 2022).

9.3.5.2. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções;

9.3.5.3. Emitir Termo Circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e

9.3.5.4. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

9.3.5.5. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão

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

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

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

9.3.9. Será permitido a emissão do Termo de Recebimento Definitivo, de forma individual, para serviço de Link de Internet WI-FI nas praças.

9.4. **Sanções Administrativas e Procedimentos Para Retenção ou Glosa no Pagamento**

9.4.1. **Descontos Aplicáveis em Caso de Descumprimento do IMR**

9.4.1.1. Durante a vigência do contrato poderão ser aplicados descontos na fatura, em caso de eventual descumprimento do Instrumento de Medição de Resultado (IMR), a título de glosa, limitando-se cada um ao limite do valor mensal do contrato.

9.4.1.2. Para fins de cálculo do valor do desconto de glosa contratual serão observados os critérios do **Item 9.1. Forma de Acompanhamento da Garantia e Níveis de Serviço**, nos termos do Instrumento de Medição de Resultado - IMR, aplicando os descontos correspondentes à disponibilidade mensal aferida, conforme a tabela abaixo:

LOTE	ITEM	SERVIÇO	FAIXA ATÉ 24H	FAIXA 24H ATÉ 48H	FAIXA ACIMA 48 H
1 (ÚNICO)	1	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN Sede (Alta Disponibilidade)	0,01% /min	0,02% /min	0,02% /min + multa moratória prevista no subitem 9.4.3.1
	2	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	0,01% /min	0,02% /min	0,02% /min + multa moratória prevista no subitem 9.4.3.1
	3	Serviço de Link dedicado de Acesso à internet, bloco /29 e Banda Mínima de Acesso Garantida	0,01% /min	0,02% /min	0,02% /min + multa moratória prevista

		de 500Mbps (Alta Disponibilidade) SEDE (Dois Link de ASN e Rota Diferentes)			no subitem 9.4.3.1
	45	Serviço de Link de acesso à Internet Sites Remotos, aplica-se ao WIFI Social	0,009% /min	0,025% /min	0,025% /min

9.4.1.3. Em caso do não cumprimento da Métrica 5 do IMR o desconto será aplicado conforme abaixo:

MÉTRICA	FAIXA ATÉ 48H	FAIXA 48H ATÉ 72H	FAIXA ACIMA 72H
MÉTRICA 5 - Solicitação de alteração de configuração dos equipamentos - Prazo 48 horas	2,0% /hora	2,5% /hora	2,5% /hora + multa moratória prevista no subitem 9.4.3.1

9.4.1.4. Nos cálculos de desconto, em que a faixa for ultrapassada, todo o cálculo deverá ser feito na faixa posterior.

9.4.1.5. O valor do desconto será aplicado no mês imediatamente subsequente ao mês em que ocorreram os fatos causadores dos descontos, tendo como base o valor vigente do acesso do mês da ocorrência da interrupção.

9.4.1.6. Os descontos não poderão ultrapassar o valor do item do serviço prestado.

9.4.2. **Sanções Aplicáveis Fase de Instalação**

9.4.2.1. O atraso injustificado no cumprimento do objeto sujeitará a CONTRATADA às seguintes penalidades:

- Advertência;
- Multa moratória no valor de 1% do valor anual do contrato para o enlace, por dia de atraso, limitado a 10 dias, pelo atraso injustificado na entrega do projeto executivo, podendo ser adotadas medidas administrativas para rescisão contratual por inexecução total da obrigação. Entende-se por enlace/circuito como qualquer link Internet nos Sites Remotos e na Sede do CONTRATANTE;
- Multa moratória no valor de 1% do valor anual do contrato para o enlace, por dia de atraso, limitado a 30 dias, pelo atraso injustificado na instalação e configuração dos enlaces contratados, podendo ser adotadas medidas administrativas para rescisão contratual por inexecução total da obrigação. Entende-se por enlace/circuito como qualquer link Internet nos Sites Remotos e na Sede do CONTRATANTE.

9.4.3. **Sanções Aplicáveis Fase de Operação**

9.4.3.1. Caso a CONTRATADA ultrapasse a última faixa dos descontos aplicáveis, além da aplicação dos descontos, será imposta multa moratória de 1% do valor mensal do serviço não atendido no IMR, limitada a 10 dias.

9.4.3.2. A não manutenção das condições de habilitação da empresa ao longo da execução do contrato poderá ensejar sua rescisão unilateral pelo CONTRATANTE, após devido processo administrativo, assegurados o contraditório e a ampla defesa, além da aplicação de multa de 30% sobre o valor da parcela inadimplida.

9.4.3.3. A multa poderá ser aplicada cumulativamente com outras penalidades previstas no contrato ou na legislação vigente.

9.4.3.4. A inexecução total ou parcial do contrato poderá resultar em rescisão, nos termos deste instrumento e dos arts. 155 e 156 da Lei nº 14.133/21, incluindo indenização por eventuais prejuízos causados ao CONTRATANTE.

9.4.3.5. A aplicação das sanções será realizada mediante processo administrativo específico, assegurados o contraditório e a ampla defesa, com comunicação formal da penalidade à CONTRATADA.

9.4.3.5.1. A critério da autoridade competente, com base nos princípios da proporcionalidade e razoabilidade, as penalidades poderão ser atenuadas ou relevadas mediante comprovação fundamentada, desde que requeridas por escrito no prazo de 5 dias úteis a contar da notificação.

9.4.3.6. O atraso no pagamento de multas será corrigido pelo IPCA, divulgado pelo IBGE.

9.4.3.7. O CONTRATANTE registrará no SICAF todas as penalidades aplicadas à CONTRATADA.

9.4.4. **Sanções Administrativas**

9.4.4.1. Comete infração administrativa, nos termos da Lei nº 14.133/2021, a CONTRATADA que:

9.4.4.1.1. Der causa à inexecução parcial ou total do contrato, especialmente quando causar grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

9.4.4.1.2. Deixar de entregar documentação exigida no certame ou para a contratação;

9.4.4.1.3. Não manter a proposta, salvo por fato superveniente devidamente justificado;

9.4.4.1.4. Ensejar o retardamento injustificado da execução do objeto;

9.4.4.1.5. Apresentar declaração ou documentação falsa durante a licitação ou execução do contrato;

9.4.4.1.6. Fraudar a licitação ou praticar atos fraudulentos na execução do contrato;

9.4.4.1.7. Adotar comportamento inidôneo, praticar fraudes ou atos ilícitos visando frustrar os objetivos da licitação;

9.4.4.1.8. Praticar ato lesivo conforme o art. 5º da Lei nº 12.846/2013.

9.4.4.2. Pela inexecução total ou parcial do contrato, poderão ser aplicadas as seguintes sanções:

9.4.4.2.1. Advertência, quando não se justificar penalidade mais grave;

9.4.4.2.2. Multa, variando entre 0,5% e 30% do valor do contrato, conforme art. 155 da Lei nº 14.133/2021;

9.4.4.2.3. Impedimento de licitar e contratar, pelo prazo máximo de 3 anos, nos casos de infrações previstas nos incisos II a VII do art. 155 da Lei nº 14.133/2021, quando não for cabível penalidade mais severa;

9.4.4.2.4. Declaração de inidoneidade para licitar e contratar, pelo prazo de 3 a 6 anos, nos casos das infrações previstas nos incisos VIII a XII do art. 155 da Lei nº 14.133/2021, bem como naquelas previstas nos incisos II a VII que justifiquem penalidade mais grave.

9.4.4.3. Na aplicação das sanções, serão considerados:

9.4.4.3.1. A natureza e a gravidade da infração;

9.4.4.3.2. As peculiaridades do caso concreto;

9.4.4.3.3. Circunstâncias agravantes ou atenuantes;

9.4.4.3.4. Os danos causados à Administração Pública;

9.4.4.3.5. A existência de programa de integridade na empresa.

9.4.4.4. A sanção prevista no item 9.4.4.2.4. será precedida de análise jurídica observando as seguintes regras:

9.4.4.4.1. Quando aplicada por órgão do Poder Executivo, será de competência exclusiva de Ministro de Estado, Secretário Estadual ou Municipal, ou da autoridade máxima da autarquia ou fundação responsável;

9.4.4.4.2. Quando aplicada por órgãos dos Poderes Legislativo e Judiciário, Ministério Público ou Defensoria Pública, será de competência exclusiva de autoridade equivalente às referidas no item 9.4.4.4.1, conforme regulamento.

9.4.4.5. As sanções previstas nos itens 9.4.4.2.1., 9.4.4.2.3. e 9.4.4.2.4. poderão ser aplicadas cumulativamente com a prevista no item 9.4.4.2.2.

9.4.4.6. Se o valor das multas e indenizações exceder eventuais créditos da CONTRATADA junto à Administração, a diferença será descontada da garantia prestada ou cobrada judicialmente.

9.4.4.7. A aplicação das sanções previstas nos itens 9.4.4.2.1., 9.4.4.2.2., 9.4.4.2.3. e 9.4.4.2.4. não exclui a obrigação de reparação integral dos danos causados à Administração.

9.4.4.8. A defesa quanto à aplicação das sanções previstas no item 9.4.4.2.2., poderá ser apresentada no prazo de 15 dias úteis a contar da intimação.

9.4.4.9. Para a aplicação das sanções previstas nos itens 9.4.4.2.3. e 9.4.4.2.4. será instaurado processo de responsabilização conduzido por comissão composta por, no mínimo, dois servidores estáveis, garantindo-se o direito à defesa no prazo de 15 dias úteis, nos termos do art. 158 da Lei nº 14.133/2021.

9.5. **Liquidação**

9.5.1. O faturamento mensal terá início somente após a emissão do Termo de Recebimento Definitivo, não sendo contada a fase de implantação do Item.

9.5.2. Para o serviço de Link de Internet nas localidades praças será permitido o faturamento após o Termo de Recebimento Definitivo de cada uma das unidades.

9.5.3. Durante a fase de prestação mensal a CONTRATANTE deverá validar minuciosamente as planilhas de memória de cálculo fornecidas pela CONTRATADA a fim de apurar os valores a serem faturados e os descontos aplicados, às planilhas de memória de cálculo deverão ser enviadas até o quinto dia após o fechamento do período de apuração.

9.5.4. CONTRATADA poderá optar por emitir a nota fiscal/fatura após a validação da memória de cálculo pela CONTRATANTE que terá prazo de 5 dias úteis para validação.

9.5.5. A CONTRATADA poderá emitir a nota fiscal/fatura com descontos apurados pela CONTRATADA e em caso de discordância dos descontos apurados por parte da CONTRATANTE, os descontos poderão ser aplicados na fatura do mês posterior.

9.5.6. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de 5 dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 6º, §1º do Decreto nº089/2024 .

9.5.6.1. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

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

a) o prazo de validade;
b) a data da emissão;
c) os dados do contrato e do órgão contratante;
d) o período respectivo de execução do contrato;
e) os descontos com mês referência;
f) o valor a pagar;
g) dados bancários para o recebimento do montante; e
h) eventual destaque do valor de retenções tributárias cabíveis.

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

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

9.5.10. A Administração deverá realizar consulta ao SICAF para:

a) verificar a manutenção das condições de habilitação exigidas no edital;
b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

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

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

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

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

9.6. **Prazo de pagamento**

9.6.1. O pagamento será efetuado no prazo de até 15 (quinze) dias úteis contados da finalização da liquidação da despesa, nos termos do art. 6º, §1º do Decreto nº089/2024.

9.7. **Forma de pagamento**

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

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

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

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

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

9.8. **Reajuste**

9.8.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do Orçamento.

9.8.2. Após o interregno de um ano do orçamento estimado, mediante pedido expresso do contratado, os preços iniciais serão reajustados pelo contratante, mediante a aplicação do índice IPCA ou outro que reflita a inflação e seja mais vantajoso à Administração Pública Municipal, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

10. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

10.1. **Forma de seleção e critério de julgamento da proposta**

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

10.1.2. A presente aquisição adotará como regime de execução por preço unitário, a ser contratado mediante licitação, na modalidade Pregão Eletrônico, com lances abertos com intervalos mínimos entre lances de R$ 0,01 (um centavo) com valor de referência sigilos, levando em conta o objetivo da promoção de uma maior disputa entre os licitantes, com resultados satisfatórios para as empresas e o órgão público, considerando que o valor ultimado pelo mercado é variável, já que o referido objeto depende de tecnologias cada vez mais avançadas.

10.1.3. A presente licitação será julgada pelo critério de menor valor global, tendo em vista que o objeto consiste na contratação de empresa especializada para prestação de serviços de segurança cibernética com Inteligência Artificial Preditiva, garantindo alta disponibilidade, segurança, eficiência e sustentabilidade no atendimento às demandas do Município de Cáceres. Considerando a natureza integrada dos serviços, que envolvem soluções tecnológicas interdependentes, como conectividade segura, monitoramento preditivo, suporte técnico especializado e infraestrutura crítica de proteção de dados, a execução por um único fornecedor assegura a compatibilidade entre os componentes, a uniformidade dos padrões técnicos, a continuidade do serviço e a racionalização dos custos operacionais. Assim, a adoção do julgamento por valor global mostra-se técnica e economicamente mais vantajosa para a Administração Pública, promovendo a otimização dos recursos públicos e garantindo a eficiência na implementação da solução proposta.

10.1.4. É lícito o agrupamento em lotes de itens a serem contratados por meio de pregão, desde que possuam mesma natureza e que guardem relação entre si (Acórdão TCU nº 5.260/2011 – 1ª Câmara);

10.2. **Exigências de habilitação**

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

10.2.1.1. **Habilitação jurídica**

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

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

10.2.1.1.3. **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;

10.2.1.1.4. **Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada**

rio - 029/2025 (112/232)

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;

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

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

10.2.1.1.7. **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

10.2.1.1.8. **Sociedade cooperativa:** ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

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

10.2.1.2. **Habilitação fiscal, social e trabalhista**

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

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

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

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

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

10.2.1.2.6. Prova de regularidade com a Fazenda [Estadual/Distrital] e [Municipal/Distrital] do domicílio e sede do fornecedor, relativa à atividade em cujo exercício contrata e concorre;

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

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

10.2.1.3. **Qualificação Econômico-Financeira**

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

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

10.2.1.3.3. Índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC) superiores a 1 (um), comprovados mediante a apresentação pelo licitante de balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais e obtidos pela aplicação das seguintes fórmulas:

I) Liquidez Geral (LG) = (Ativo Circulante + Realizável a Longo Prazo) / (Passivo Circulante + Passivo Não Circulante);

II) Solvência Geral (SG)= (Ativo Total) / (Passivo Circulante +Passivo não Circulante); e

III) Liquidez Corrente (LC) = (Ativo Circulante) / (Passivo Circulante).

10.2.1.3.4. 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] OU [patrimônio líquido mínimo] de 5% do valor total estimado do item.

10.2.1.4. **Qualificação Econômico-Financeira. (Justificativa)**

10.2.1.4.1. Ressalta-se que as exigências de habilitação relativas à qualificação econômico-financeira acima previstas e de acordo com o artigo 69 da Lei nº 14.133/21, têm a finalidade de viabilizar a aferição da situação financeira dos licitantes pela Administração. Dessa forma, será possível verificar se o interessado reúne condições indispensáveis para suportar as despesas relativas à satisfatória execução do objeto contratual, como dado objetivo de comprovação da qualificação econômico-financeira dos licitantes e para efeito de garantia ao adimplemento do contrato a ser ulteriormente celebrado, visando assegurar que a empresa contratada possa cumprir suas obrigações de curto e longo prazo, cumprindo as obrigações previstas no Edital e contrato, por se tratar de registro de preço o índice de 5% do valor de cada item, a Administração escolheu este valor por entender ser o mínimo a exigir de uma empresa para se manter um contrato, dentro de um nível de segurança e equilíbrio. Ademais, com o objetivo de não restringir o universo de concorrentes, resolveu não exigir valor acima da unidade. Ante o exposto, a exigência do Edital nada mais fez que traduzir em critérios objetivos o disposto no art. 37, XXI, da Constituição Federal, ademais, os índices escolhidos foram democráticos, na medida em que estabelecem um "mínimo" de segurança na contratação. Desta forma, atende plenamente a Lei Federal nº 14.133/21 limitando-se a exigir índices que demonstrem a capacidade financeira dos licitantes com vistas ao compromisso a ser assumido para plena execução do contrato.

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

10.2.1.4.3. O balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos. (Lei nº 14.133, de 2021, art. 69, §6º)

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

10.2.1.5. **Qualificação Técnica**

10.2.1.5.1. Será exigida a comprovação da capacidade técnico-operacional da licitante, mediante a apresentação de atestados emitidos por pessoa jurídica de direito público ou privado, que comprovem a execução de serviços compatíveis em características, quantidades e prazos com o objeto deste contrato, incluindo o fornecimento e a instalação de equipamentos correlatos aos ofertados, bem como a prestação de serviços de instalação, configuração e suporte técnico. A licitante deverá comprovar, no mínimo, experiência prévia correspondente a **30% (trinta por cento)** do quantitativo estimado do **item 1 – Solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)**, considerado de maior relevância técnica para a consecução do objeto. Tal exigência encontra amparo no inciso III do art. 67 da Lei nº 14.133/2021, sendo justificada pela complexidade e especificidade do objeto, que demanda experiência comprovada na execução de soluções integradas de segurança cibernética, com destaque para componentes baseados em Inteligência Artificial Preditiva, visando garantir a eficiência, a continuidade dos serviços e a mitigação de riscos operacionais, em observância aos princípios da legalidade, razoabilidade, eficiência e interesse público.

10.2.1.5.1.1. A comprovação poderá ser feita por meio de um ou mais atestados que, **conjuntamente**, demonstrem a experiência da licitante de forma compatível com o objeto contratado, especialmente no que se refere ao atendimento do percentual mínimo de 30% do item de maior relevância técnica, vedada a exigência de comprovação integral do quantitativo estimado.

10.2.1.5.1.2. Os atestados deverão conter, no mínimo:

10.2.1.5.1.2.1. Identificação completa do emitente, com razão social, CNPJ, endereço e dados de contato;

10.2.1.5.1.2.2. Descrição detalhada dos serviços executados, permitindo aferir a compatibilidade em características com o objeto, incluindo fornecimento e instalação de equipamentos, implantação de soluções de segurança cibernética, configuração e suporte técnico;

10.2.1.5.1.2.3. Indicação de que os serviços foram executados em quantidades compatíveis, com destaque para a experiência mínima equivalente a 30% do quantitativo estimado do item de maior relevância técnica, conforme avaliação da Administração.

vedada a exigência de quantidades idênticas ou desproporcionais, nos termos do art. 67, §§ 1º, 2º e 5º, da Lei nº 14.133/2021;

10.2.1.5.1.2.4. Período de execução dos serviços, com datas de início e de conclusão ou, se for o caso, vigência atual, para fins de comprovação da compatibilidade em prazos;

10.2.1.5.1.2.5. Declaração de que os serviços foram prestados de forma satisfatória, assinada por representante legal da entidade emitente;

10.2.1.5.1.2.6. Assinatura e identificação do responsável pela emissão, com nome legível, cargo e meios de contato.

10.2.1.5.2. A licitante deve comprovar que dispõe de, no mínimo, dois (02) técnicos certificados pelo fabricante da solução proposta, os quais participarão diretamente da execução dos serviços previstos.

10.2.1.5.3. As certificações devem ser reconhecidas pelo fabricante e estar atualizadas, garantindo conhecimento técnico adequado às demandas do projeto.

10.2.1.5.4. O fornecedor deve fornecer todas as informações e documentos necessários para validar a legitimidade dos atestados apresentados, incluindo:

- Cópia do contrato que deu origem à prestação dos serviços mencionados nos atestados;
- Endereço atual da contratante que emitiu o atestado;
- Local onde os serviços foram executados;
- Outros documentos complementares, se solicitados pela Administração.

10.2.1.5.5. A licitante deve comprovar experiência em projetos de complexidade e escopo semelhantes, preferencialmente na área pública ou em ambientes corporativos de grande porte, apresentando histórico de projetos realizados com soluções NGFW, SD-WAN e links de redundância.

10.2.1.5.6. A licitante deverá demonstrar a capacidade técnica necessária para atender aos requisitos específicos do projeto, incluindo:

- Disponibilidade de suporte técnico especializado durante todo o período contratual;
- Experiência em integrar soluções de segurança em redes heterogêneas e complexas;

- Conhecimento comprovado em tecnologias de alta disponibilidade, criptografia e gestão de redes com políticas de segurança.

10.2.1.5.7. Sempre que solicitado pela Administração, a licitante deverá apresentar documentação adicional que comprove a qualificação técnica e a capacidade operacional para executar o objeto contratado, garantindo transparência e segurança no processo de contratação.

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

11.1. O custo estimado da contratação possui caráter sigiloso e será tornado público apenas e imediatamente após o julgamento das propostas nos termos do Art. 9º do Decreto municipal 240/23.

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

12. DA PARTICIPAÇÃO DE CONSORCIO

12.1. Trata-se da vedação da participação de consórcios quanto ao registro de preços para CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA PRESTAÇÃO DE SERVIÇOS DE SEGURANÇA CIBERNÉTICA COM INTELIGÊNCIA ARTIFICIAL PREDITIVA, GARANTINDO ALTA DISPONIBILIDADE, SEGURANÇA, EFICIÊNCIA E SUSTENTABILIDADE NO ATENDIMENTO ÀS DEMANDAS DO MUNICÍPIO DE CÁCERES.

12.2. Art. 14 da Lei 14.133/21, conferiu a discricionaridade à Administração para permitir ou vetar a formação de consórcio em certame licitatório. É sabido que, em regra, a formação de consórcio é admitida quando o objeto a ser licitado envolve questões de alta complexidade técnica ou de relevante vulto, em que, isoladamente, as empresas não teriam condições de suprir os requisitos de habilitação do edital.

12.3. Tratando-se do objeto em questão, a ausência de consórcio não trará prejuízos à competitividade do certame por se tratar de um registro de preços, de serviços comuns, a ser executado ao longo de 12 (doze) meses em sua totalidade ou não, que não demandam especialidades diferentes entre as empresas, as quais poderiam impedir a execução dos serviços por uma única empresa. É nítido, neste caso também que, a reunião de empesas em consórcio, ao invés de estabelecer uma disputa entre as empresas, as mesmas formalizariam acordo para eliminar a competição caso estivessem reunidas em consórcio.

12.4. Diante de todo o exposto e, considerando que existem diversas empresas com capacidade para fornecer os serviços a serem contratados facilmente comprovados através do número de cotações inseridas no processo, fica vedada à participação de consórcios na licitação.

13. ADESÃO A ATA DE REGISTRO DE PREÇO

13.1. Em conformidade com a Lei nº 14.133/2021, a Lei nº 14.770/2023 e demais regulamentos aplicáveis, a adesão à Ata de Registro de Preços (ARP) configura-se como mecanismo de cooperação interfederativa, baseado na manifestação de interesse mútuo entre os entes públicos. Tal procedimento visa proporcionar maior eficiência administrativa e econômica, especialmente diante das dificuldades enfrentadas por órgãos e entidades para realizar processos licitatórios frequentes, seja por limitações de pessoal, infraestrutura ou outras razões justificáveis.

13.2. A adesão à ARP pelos demais entes federados será viabilizada desde que respeitados os limites quantitativos previstos no instrumento convocatório e nas legislações mencionadas, bem como observadas as condições estabelecidas neste Termo de Referência. A formalização da adesão deverá ocorrer mediante solicitação formal do ente interessado, acompanhada da anuência do órgão gerenciador e da CONTRATADA, conforme exigido pela legislação vigente.

13.3. A adesão não poderá resultar em prejuízo ao fornecimento ou à prestação dos serviços destinados ao órgão gerenciador e demais participantes da ARP. Caso o volume decorrente das adesões comprometa o atendimento das quantidades inicialmente previstas, a CONTRATADA deverá priorizar o fornecimento ao órgão gerenciador e aos participantes originais, conforme os prazos e condições estabelecidos neste instrumento.

13.4. Os entes federados que aderirem à ARP assumem integral responsabilidade pela gestão e fiscalização dos contratos celebrados diretamente com a CONTRATADA, sem qualquer interferência ou solidariedade do órgão gerenciador. Caberá ao ente aderente zelar pelo cumprimento das obrigações pactuadas, inclusive no que se refere às condições de pagamento, prazos de entrega e demais cláusulas contratuais.

13.5. O órgão gerenciador poderá, a qualquer tempo, solicitar relatórios à CONTRATADA para acompanhar as adesões realizadas, garantindo o cumprimento dos limites quantitativos e demais disposições legais aplicáveis. Eventuais irregularidades deverão ser comunicadas ao órgão gerenciador, que adotará as providências cabíveis em conformidade com a legislação vigente.

14. ADEQUAÇÃO ORÇAMENTÁRIA

14.1. As despesas oriundas da presente aquisição correrão por conta de todas as dotações vigentes, conforme especificado pelas Secretarias no momento do empenho.

ÓRGÃO/ UNIDADE	FUNCIONAL-PROGRAMÁTICA	NATUREZA DA DESPESA	FONTE DE RECURSOS	SECRETARIA
021301	04.129.1002.2109	3.3.90.	1.1.500	SMFAZ
021201	27.122.1009.2107	3.3.90.	1.1.500	SMFAZ
020501	10.122.1003.2021	33.90.	1.1.500	SMS
020502	10.304.1003.2030	33.90.	1.600	SMS
020901	04.121.1002.2071	3.3.90.	1.1.500	SMPLAN

020901	04.127.1002.2071	3.3.90.	1.1.500	SMPLAN
021101	08.122.1008.2074	3.3.90.	1.1.500	SMASC
021102	08.244.1008.2082	3.3.90.	4.1.660	SMASC
021102	08.244.1008.2083	3.3.90.	1.1.500	SMASC
021102	08.244.1008.2083	3.3.90.	4.1.660	SMASC
021102	08.244.1008.2086	3.3.90.	4.1.660	SMASC
021102	08.244.1008.2091	3.3.90.	1.1.500	SMASC
020601	12.122.1004.2046	3.3.90.	2.1.500	SME
020401	04.123.1002.2019	3.3.90.	1.1.500	SMFIN
020701	15.122.1005.2061	3.3.90.	1.1.500	SMIL
021401	18.122.1010.2111	3.3.90.	1.1.500	SMMADE
021001	20.122.1007.2072	3.3.90.	1.1.500	SMAGRI
020101	04.122.1002.2004	3.3.90.	1.1.500	GABINETE
020201	04.122.1002.2012	3.3.90.	1.1.500	SMEAE
020801	04.122.1006.2066	3.3.90.	1.1.500	SMTC
021201	27.122.1009.2.107	3.3.90.	1.1.500	SMEL
020201	04 126 1002 2014 0000	3.3.90	1.1.500	SMEAE
020201	04 122 1002 2012 0000	3.3.90	1.1.500	SMEAE
020301	04 122 1002 2018 0000	3.3.90	1.1.500	SMA

Cáceres-MT, 13 de junho 2025.

WELLYNGTON DE BARROS MACIEL
Coordenador de Informações Sistêmicas e Tecnologia de Informação em Substituição
Decreto nº. 392 de 11 de junho de 2025

JEREMIAS PEREIRA LEITE
Secretário Municipal Especial de Assuntos Estratégicos

CONTRATADA
Empresa: CNPJ:
Representante: CPF:
RG:

Assinado por 2 pessoas: WELLYNGTON DE BARROS MACIEL e JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/7BE7-17D2-35C8-081E e informe o código 7BE7-17D2-35C8-081E

ANEXO II – TERMO DA ATA DE REGISTRO DE PREÇO

O (A). PREFEITURA MUNICIPAL DE CÁCERES, com sede no(a) na Av. Brasil,119,COC, Bairro Jardim Celeste, na cidade de Cáceres-MT, inscrito(a) no CNPJ/MF sob o nº 03214145/0001-83, neste ato representado(a) pelo(a) ...... (cargo e nome), nomeado(a) pela Portaria nº ...... de ..... de ...... de 200..., publicada no .... de ..... de .... de , portador
da matrícula funcional nº ....,, considerando o julgamento da licitação na modalidade de pregão, na forma eletrônica, para REGISTRO DE PREÇOS nº ..../2024..., publicada no ...... de ...../...../200. , processo administrativo
n.º ...., RESOLVE registrar os preços da(s) empresa(s) indicada(s) e qualificada(s) nesta ATA, de acordo com a classificação por ela(s) alcançada(s) e na(s) quantidade(s) cotada(s), atendendo as condições previstas no edital, sujeitando-se as partes às normas constantes na Lei nº 14.133, de 1º de abril de 2021.

1. DO OBJETO

1.1. Registro de Preço para futura e eventual contratação de empresa especializada para prestação de serviços de segurança cibernética com Inteligência Artificial Preditiva, garantindo alta disponibilidade, segurança, eficiência e sustentabilidade no atendimento às demandas do Município de Cáceres, conforme condições e exigências estabelecidas neste instrumento.

2. DOS PREÇOS, ESPECIFICAÇÕES E QUANTITATIVOS.

2.1. O preço registrado, as especificações do objeto, a quantidade, fornecedor (es) e as demais condições ofertadas na(s) proposta(s) são as que seguem:

ITEM	Fornecedor *(razão social, CNPJ/MF, endereço, contatos, representante)*						
X	Especificação	*Marca (se exigida no edital)*	*Modelo (se exigido no edital)*	Unidade	Quantidade Máxima	Quantidade Mínima	Valor Un
1	Serviço de provimento de solução de Firewall de Nova Geração e SD- WAN (Alta Disponibilidade)						

2	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva						
3	Serviço de Link dedicado de Acesso à internet, bloco /29 e Banda Mínima de Acesso						

	Garantida de 500Mbps (Alta Disponibilidade) SEDE (Link de ASN e Rota Diferentes)						
4	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 150Mbps Sites Remotos (Fibra Óptica)						
5	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G)						
6	Implantação da Solução						

rio - 029/2025 (123/232)

7	Capacitação especializada da equipe com emissão de certificação.						
8	Consultoria Política de Segurança						

3. DA ADESÃO À ATA DE REGISTRO DE PREÇOS

3.1. Será admitida a adesão à ata de registro de preços decorrente desta licitação , conforme lei 14.133/2021.

4. VALIDADE DA ATA , FORMALIZAÇÃO DA ATA DE REGISTRO DE PREÇOS E CADASTRO RESERVA

4.1 A validade da Ata de Registro de Preços será de 1 (um) ano, contado a partir do primeiro dia útil subsequente à data de divulgação da ata do registro de preço, podendo ser prorrogada por igual período, mediante a anuência do fornecedor, desde que comprovado o preço vantajoso.

4.1.1. O contrato decorrente da ata de registro de preços terá sua vigência estabelecida no próprio instrumento contratual e observará 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.

4.1.2. Na formalização do contrato ou do instrumento substituto deverá haver a indicação da disponibilidade dos créditos orçamentários respectivos.

4.2 A contratação com os fornecedores registrados na ata será formalizada pelo órgão ou pela entidade interessada por intermédio de instrumento contratual, emissão de nota de empenho de despesa, autorização de compra ou outro instrumento hábil, conforme o art. 95 da Lei nº 14.133, de 2021.

4.2.1. O instrumento contratual de que trata deste processo. deverá ser assinado no prazo de validade da ata de registro de preços.

4.3 Os contratos decorrentes do sistema de registro de preços poderão ser alterados, observado o art. 124 da Lei nº 14.133, de 2021.

4.4 Após a homologação da licitação ou da contratação direta, deverão ser observadas as seguintes condições para formalização da ata de registro de preços:

4.4.1 Serão registrados na ata os preços e os quantitativos do adjudicatário.

4.4.2 Será incluído na ata, na forma de anexo, o registro dos licitantes ou dos fornecedores que:

4.4.2.1 Aceitarem cotar os bens, as obras ou os serviços com preços iguais aos do adjudicatário, observada a classificação da licitação; e

4.4.2.2 Mantiverem sua proposta original.

4.4.3 Será respeitada, nas contratações, a ordem de classificação dos licitantes ou dos fornecedores registrados na ata.

4.5 O registro a que se refere a este termo tem por objetivo a formação de cadastro de reserva para o caso de impossibilidade de atendimento pelo signatário da ata.

4.6 Para fins da ordem de classificação, os licitantes ou fornecedores que aceitarem reduzir suas propostas para o preço do adjudicatário antecederão aqueles que mantiverem sua proposta original.

4.7 A habilitação dos licitantes que comporão o cadastro de reserva a que se refere a este processo somente será efetuada quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:

4.7.1 Quando o licitante vencedor não assinar a ata de registro de preços, no prazo e nas condições estabelecidos *no edital*.

4.7.2 Quando houver o cancelamento do registro do licitante ou do registro de preços nas hipóteses previstas no edital.

4.8 O preço registrado com indicação dos licitantes e fornecedores será divulgado a ata de registro de preços e ficará disponibilizado durante a vigência da ata de registro de preços.

4.9 Após a homologação da licitação ou da contratação direta, o licitante mais bem classificado ou o fornecedor, no caso da contratação direta, será convocado para assinar a ata de registro de preços, no prazo e nas condições estabelecidos no edital de licitação ou no aviso de contratação direta, sob pena de decair o direito, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021.

4.9.1. O prazo de convocação poderá ser prorrogado 1 (uma) vez, por igual período, mediante solicitação do licitante ou fornecedor convocado, desde que apresentada dentro do prazo, devidamente justificada, e que a justificativa seja aceita pela Administração.

4.10 A ata de registro de preços será assinada por meio de assinatura digital e disponibilizada no Sistema de Registro de Preços.

4.11 Quando o convocado não assinar a ata de registro de preços no prazo e nas condições estabelecidos no edital ou no aviso de contratação, e observado o disposto no edital, observando o edital e seu anexo subitens, fica facultado à Administração convocar os licitantes remanescentes do cadastro de reserva, na ordem de classificação, para fazê-lo em igual prazo e nas condições propostas pelo primeiro classificado.

4.12 Na hipótese de nenhum dos licitantes que trata a ata de registro de preço, aceitar a contratação nos termos do item anterior, a Administração, observados o valor estimado e sua eventual atualização nos termos *do edital*, poderá:

4.12.1 Convocar para negociação os demais licitantes ou fornecedores remanescentes cujos preços foram registrados sem redução, observada a ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário; ou

4.12.2 Adjudicar e firmar o contrato nas condições ofertadas pelos licitantes ou fornecedores remanescentes, atendida a ordem classificatória, quando frustrada a negociação de melhor condição.

4.13. A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente justificada

5. ALTERAÇÃO OU ATUALIZAÇÃO DOS PREÇOS REGISTRADOS

5.1 Os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, nas seguintes situações:

5.2 Em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução de ata tal como pactuada, mediante pedido formal do interessado, nos termos da alínea "d" do inciso II do caput do art. 124 da lei n.º 14.133, de 2021", quando o ônus de prova incumbe ao contratante via requerimento fundamentado, que será analisado, se possível, em até 30 dias pela Administração Municipal.

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

5.2.2. Na hipótese de previsão no edital de cláusula de reajustamento ou repactuação sobre os preços registrados, nos termos da Lei nº 14.133, de 2021.

5.2.2.1. No caso do reajustamento, deverá ser respeitada a contagem da anualidade e
. o índice previstos para a contratação;

5.2.2.2. No caso da repactuação, poderá ser a pedido do interessado, conforme critérios definidos para a contratação.

5.2.2.3. No caso da repactuação, poderá ser a pedido do interessado, conforme critérios definidos para a contratação.

5.3. O requerimento de reequilíbrio da equação econômico-financeira deverá demonstrar o desequilíbrio havido minuciosamente por meio de memória de cálculo e a modificação dos encargos ser proporcional ao mesmo, e ser documentalmente comprovada.

6. NEGOCIAÇÃO DE PREÇOS REGISTRADOS

6.1. Na hipótese de o preço registrado tornar-se superior ao preço praticado no mercado por motivo superveniente, o órgão ou entidade gerenciadora convocará o fornecedor para negociar a redução do preço registrado.

6.1.1 Caso não aceite reduzir seu preço aos valores praticados pelo mercado, o fornecedor será liberado do compromisso assumido quanto ao item registrado, sem aplicação de penalidades administrativas.

6.2. Na hipótese prevista no item anterior, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam reduzir seus preços aos valores de mercado e não convocará os licitantes ou fornecedores que tiverem seu registro cancelado.

6.2.1 Se não obtiver êxito nas negociações, o órgão ou entidade gerenciadora procederá ao cancelamento da ata de registro de preços, adotando as medidas cabíveis para obtenção de contratação mais vantajosa.

6.2.2 Na hipótese de redução do preço registrado, o gerenciador comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços para que avaliem a conveniência e a oportunidade de diligenciarem negociação com vistas à alteração contratual, observado o disposto no art. 124 da Lei nº 14.133, de 2021.

6.3 Na hipótese de o preço de mercado tornar-se superior ao preço registrado e o fornecedor não poder cumprir as obrigações estabelecidas na ata, será facultado ao fornecedor requerer ao gerenciador a alteração do preço registrado, mediante comprovação de fato superveniente que supostamente o impossibilite de cumprir o compromisso.

6.3.1 Neste caso, o fornecedor encaminhará, juntamente com o pedido de alteração, a documentação comprobatória ou à planilha de custos que demonstre a inviabilidade do preço registrado em relação às condições inicialmente pactuadas.

6.3.2 Não hipótese de não comprovação da existência de fato superveniente que inviabilize o preço registrado, o pedido será indeferido pelo órgão ou entidade gerenciadora e o fornecedor deverá cumprir as obrigações estabelecidas na ata, sob pena de cancelamento do seu registro, nos termos do edital, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021, e na legislação aplicável.

6.3.3 Na hipótese de cancelamento do registro do fornecedor, nos termos do item anterior, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam manter seus preços registrados, observado o disposto no edital.

6.3.4 Se não obtiver êxito nas negociações, o órgão ou entidade gerenciadora procederá ao cancelamento da ata de registro de preços, nos termos do edital, e adotará as medidas cabíveis para a obtenção da contratação mais vantajosa.

6.3.5 Na hipótese de comprovação da majoração do preço de mercado que inviabilize o preço registrado, conforme previsto no edital, o órgão ou entidade gerenciadora atualizará o preço registrado, de acordo com a realidade dos valores praticados pelo mercado.

6.3.6 O órgão ou entidade gerenciadora comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços sobre a efetiva alteração do preço registrado, para que avaliem a necessidade de alteração contratual, observado o disposto no art. 124 da Lei nº 14.133, de 2021.

7. REVISÃO E CANCELAMENTO.

7.1. O registro do fornecedor será cancelado pelo gerenciador, quando o fornecedor:

7.1.1. Descumprir as condições da ata de registro de preços, sem motivo justificado;

7.1.2. Não retirar a nota de empenho, ou instrumento equivalente, no prazo estabelecido pela Administração sem justificativa razoável;

7.1.3. Não aceitar manter seu preço registrado, na hipótese prevista no edital.

7.1.4. Sofrer sanção prevista nos incisos III ou IV do caput do art. 156 da Lei nº 14.133, de 2021. Na hipótese de aplicação de sanção prevista nos incisos III ou IV do caput do art. 156 da Lei nº 14.133, de 2021, caso a penalidade aplicada ao fornecedor não ultrapasse prazo de vigência da ata de registro de preços, poderá o órgão ou a entidade gerenciadora poderá, mediante decisão fundamentada, decidir pela manutenção do registro de preços, vedadas contratações derivadas da ata enquanto perdurarem os efeitos da sanção.

7.2. O cancelamento de registros nas hipóteses previstas deste instrumento será formalizado por despacho do órgão ou da entidade gerenciadora, garantidos os princípios do contraditório e da ampla defesa.

7.3. Na hipótese de cancelamento do registro do fornecedor, o órgão ou a entidade gerenciadora poderá convocar os licitantes que compõem o cadastro de reserva, observada a ordem de classificação.

7.4. O cancelamento dos preços registrados poderá ser realizado pelo gerenciador, em determinada ata de registro de preços, total ou parcialmente, nas seguintes hipóteses, desde que devidamente comprovadas e justificadas:

7.4.1. Por razão de interesse público;

7.4.2. A pedido do fornecedor, decorrente de caso fortuito ou força maior; ou

7.4.3. Se não houver êxito nas negociações, nas hipóteses em que o preço de mercado se tornar superior ou inferior ao preço registrado.

8. DAS PENALIDADES

8.1. O descumprimento da Ata de Registro de Preços ensejará aplicação das penalidades estabelecidas *no edital.*

8.2. As sanções também se aplicam aos integrantes do cadastro de reserva no registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente após terem assinado a ata.

9. CONDIÇÕES GERAIS

9.1. As condições gerais de execução do objeto, tais como os prazos para entrega e recebimento, as obrigações da Administração e do fornecedor registrado, penalidades e demais condições do ajuste encontram-se definidos no Termo de Referência, ANEXO *AO EDITAL.*

9.2. Para firmeza e validade do pactuado, a presente Ata foi lavrada em 2 (duas) vias de igual teor, que depois de lida e achada em ordem, vai assinada pelas partes.

Cáceres - MT, de__________2025. CONTRATANTE:

____

MUNICIPIO DE CÁCERES – MT

Secretário Municipal Especial de Assuntos Estratégicos.
CONTRATADA

Empresa: CNPJ:
Represente: CPF: RG:

ANEXO III - TERMO DE CONTRATO

TERMO DE CONTRATO DE COMPRA Nº ..../...., QUE FAZEM ENTRE SI O(A)... E A EMPRESA ....

A Prefeitura Municipal de Cáceres, por intermédio do(a).....................................(órgão) contratante), com sede no(a) ...., na cidade de .... /Estado ..., inscrito(a) no CNPJ sob o nº ...., neste ato representado(a) pelo(a)..........................(cargo e nome), nomeado(a) pela Portaria nº ......, de ..... de .... de 20..., publicada no DOU de ..... de .... de ...., portador da matrícula funcional nº ....,., doravante denominada CONTRATANTE, e o(a) .... inscrito(a) no CNPJ/MF sob o nº ...., sediado(a) na ...., em .... doravante designada CONTRATADA, neste ato representada pelo(a) Sr.(a) ...., portador(a) da Carteira de Identidade nº ...., expedida pela (o) ...., e CPF nº ...., tendo em vista o que consta no Processo nº .... e em observância às disposições da LEI 14.133/2021.

1. CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto do presente instrumento é a contratação de empresa especializada para prestação de serviços de segurança cibernética com Inteligência Artificial Preditiva, garantindo alta disponibilidade, segurança, eficiência e sustentabilidade no atendimento às demandas do Município de Cáceres, conforme condições e exigências estabelecidas no Termo de Referência.

1.2. Objeto da contratação:

ITEM	CÓDIGO TCE- MT	CÓDIGO CATMAT	ESPECIFICAÇÃO	UNIDADE	QUANTIDADE	QUANTIDADE ANUAL
1	257560-4	609340	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)	Serviço	173	2076

2	152969	481647	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	Serviço	2	24
3	00065206	26174	Serviço de Link dedicado de Acesso à internet, bloco /29 e Banda Mínima de Acesso Garantida de 500Mbps (Alta Disponibilidade) SEDE (Link de ASN e Rota Diferentes)	Serviço	2	24
4	152970	26484	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 150Mbps Sites	Serviço	171	2052
			Remotos (Fibra Óptica)			
5	152972	26557	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G)	Serviço	171	2052
6	339905-2	1988	Implantação da Solução	Serviço	1	1

rio - 029/2025 [illegible] (130/232) [illegible]

7	404876-8	16837	Capacitação especializada da equipe com emissão de certificação.	Treinamento	1	1
8	332679-9	27340	Consultoria Política de Segurança	Serviço	1	1

1.3. Vinculam esta contratação, independentemente de transcrição:

1.3.1. O Termo de Referência;

1.3.2. O Edital da Licitação;

1.3.3. A Proposta do contratado;

1.3.4. Eventuais anexos dos documentos supracitados.

1.4. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

1.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

1.6. 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.

1.7. 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.

1.8. O reajuste será realizado por apostilamento.

1.9. o prazo para resposta ao pedido de repactuação de preços será preferencialmente de 1 (um) mês, contado da data do fornecimento da documentação prevista no § 6º do art.

2. CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1. O prazo de vigência da contratação é de 12 (doze) meses contados do(a), prorrogável sucessivamente, na forma do artigo 114 da Lei n° 14.133, de 2021.

2.2. A prorrogação de que trata este item é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o contratado, atentando, ainda, para o cumprimento dos seguintes requisitos:

a) Estar formalmente demonstrado no processo que a forma de prestação dos serviços tem natureza continuada;

b) Seja juntado relatório que discorra sobre a execução do contrato, com informações de que os serviços tenham sido prestados regularmente;

c) Seja juntada justificativa e motivo, por escrito, de que a Administração mantém interesse na realização do serviço;

d) Haja manifestação expressa do contratado informando o interesse na prorrogação;

e) Seja comprovado que o contratado mantém as condições iniciais de habilitação.

2.3. O contratado não tem direito subjetivo à prorrogação contratual.

2.4. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

2.5. Nas eventuais prorrogações contratuais, os custos não renováveis já pagos ou amortizados ao longo do primeiro período de vigência da contratação deverão ser reduzidos ou eliminados como condição para a renovação.

2.6. O contrato não poderá ser prorrogado quando o contratado tiver sido penalizado nas sanções de declaração de inidoneidade ou impedimento de licitar e contratar com poder público, observadas as abrangências de aplicação.

3. CLÁUSULA QUARTA – DOTAÇÃO ORÇAMENTÁRIA

3.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União deste exercício, na dotação abaixo discriminada:

Gestão/Unidade:
Fonte de Recursos:
Programa de Trabalho:
Elemento de Despesa:
Plano Interno:
Nota de Empenho

3.2. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

4. CLÁUSULA QUINTA – PAGAMENTO

4.1. O prazo para pagamento e demais condições a ele referentes encontram-se no Termo de Referência.

V - O preço e as condições de pagamento, os critérios, a data-base e a periodicidade do reajustamento de preços e os critérios de atualização monetária entre a data do adimplemento das obrigações e a do efetivo pagamento;

VI - os critérios e a periodicidade da medição, quando for o caso, e o prazo para liquidação e para pagamento; VII - os prazos de início das etapas de execução, conclusão, entrega, observação e recebimento definitivo, quando for o caso; da prestação do serviço aos ditames da Lei Federal nº 8.078/1990.

5. CLÁUSULA SEXTA – REAJUSTE

5.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do Orçamento.

5.2. Após o interregno de um ano do orçamento estimado, mediante pedido expresso do contratado, os preços iniciais serão reajustados pelo contratante, mediante a aplicação do índice IPCA ou outro que reflita a inflação e seja mais vantajoso à Administração Pública Municipal, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

5.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

5.4. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

5.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

5.6. 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.

5.7. 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.

5.8.O reajuste será realizado por apostilamento.

5.9. o prazo para resposta ao pedido de repactuação de preços será preferencialmente de 1 (um) mês, contado da data do fornecimento da documentação prevista no § 6º do art.

6. CLÁUSULA OITAVA - ENTREGA E RECEBIMENTO DO OBJETO

6.1. As condições de entrega e recebimento do objeto são aquelas previstas no Termo de Referência, anexo ao Edital.

7. CLAÚSULA NONA – FISCALIZAÇÃO

7.1. A fiscalização da execução do objeto será efetuada por Comissão/Representante designado pela CONTRATANTE, na forma estabelecida no Termo de Referência, anexo do Edital.

8. CLÁUSULA DÉCIMA – OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

8.1. As obrigações da CONTRATANTE e da CONTRATADA são aquelas previstas no Termo de Referência, anexo do Edital.

9. CLÁUSULA DÉCIMA PRIMEIRA – SANÇÕES ADMINISTRATIVAS

9.1. As sanções referentes à execução do contrato são aquelas previstas no Termo de Referência, anexo do Edital.

10. CLÁUSULA DÉCIMA SEGUNDA – RESCISÃO

10.1. O contrato será extinto quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes.

10.2. O contrato poderá ser extinto antes do prazo nele fixado, sem ônus para o contratante, quando este não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

10.3. A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação do contratado pelo contratante nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia.

10.4. Caso a notificação da não-continuidade do contrato de que trata este subitem ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação.

10.5. O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

10.6. Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

10.7. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a extinção se não restringir sua capacidade de concluir o contrato.

10.8. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

10.9. O termo de extinção, sempre que possível, será precedido:

10.9.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

10.9.2. Relação dos pagamentos já efetuados e ainda devidos;

10.9.3. Indenizações e multas.,

10.10. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório (art. 131, *caput,* da Lei n.º 14.133, de 2021).

10.11. O não pagamento dos salários e das verbas trabalhistas, e o não recolhimento das contribuições sociais, previdenciárias e para com o FGTS poderá dar ensejo à extinção do contrato por ato unilateral e escrito do contratante e à aplicação das penalidades cabíveis.

10.12. O contratante poderá conceder prazo para que o contratado regularize suas obrigações trabalhistas ou suas condições de habilitação, sob pena de extinção contratual, quando não identificar má-fé ou a incapacidade de correção.

10.13. Quando da extinção, o fiscal administrativo deverá verificar o pagamento pelo contratado das verbas rescisórias ou os documentos que comprovem que os empregados serão realocados em outra atividade de prestação de serviços, sem que ocorra a interrupção do contrato de trabalho.

10.14. Até que o contratado comprove o disposto no item anterior, o contratante reterá:

10.14.1. A garantia contratual - prestada com cobertura para os casos de descumprimento das obrigações de natureza trabalhista e previdenciária, incluídas as verbas rescisórias -, a qual será executada para reembolso dos prejuízos sofridos pela Administração, nos termos da legislação que rege a matéria (art. 121,

§ 3º, I, e art. 139, III, b, da Lei n.º 14.133/2021); e

10.14.2. Os valores das Notas fiscais ou Faturas correspondentes em valor proporcional ao inadimplemento, até que a situação seja regularizada.

10.15. Na hipótese do subitem anterior, não havendo quitação das obrigações por parte do contratado no prazo de 15 (quinze) dias, o contratante poderá efetuar o pagamento das obrigações diretamente aos empregados que tenham participado da execução dos serviços objeto do contrato, deduzindo o respectivo valor do pagamento devido ao contratado (art. 121, §3º, inciso II, da Lei nº 14.133/2021).

10.16. O contratante poderá ainda:

10.16.1. nos casos de obrigação de pagamento de multa pelo contratado, reter a garantia prestada a ser executada (art. 139, III, “c”, da Lei n.º 14.133/2021), conforme legislação que rege a matéria; e

10.16.2. nos casos em que houver necessidade de ressarcimento de prejuízos causados à Administração, nos termos do inciso IV do art. 139 da Lei n.º 14.133, de 2021, reter os eventuais créditos existentes em favor do contratado decorrentes do contrato.

10.17. O contrato poderá ser extinto caso se constate que o contratado mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que tenha desempenhado função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau (art. 14, inciso IV, da Lei n.º 14.133, de 2021).

11. CLÁUSULA DÉCIMA TERCEIRA – VEDAÇÕES

11.1. É vedado à CONTRATADA:

11.1.1. caucionar ou utilizar este Termo de Contrato para qualquer operação financeira;

rio - 029/2025 [illegible] (134/232) [illegible]

11.1.2. interromper a execução contratual sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

12. CLÁUSULA DÉCIMA QUARTA – ALTERAÇÕES

12.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

12.2. O contratado é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

12.3. As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da consultoria jurídica do contratante, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês (art. 132 da Lei nº 14.133, de 2021).

12.4. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

13. CLÁUSULA DÉCIMA QUINTA - DOS CASOS OMISSOS.

13.1. Os casos omissos serão decididos pelo contratante, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor

14. CLÁUSULA DÉCIMA SEXTA – PUBLICAÇÃO

14.1. Incumbirá ao contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, *caput*, da Lei n.º 14.133, de 2021, e ao art. 8º, §2º, da Lei n. 12.527, de 2011, c/c art. 7º, §3º, inciso V, do Decreto n. 7.724, de 2012.

15. CLÁUSULA DÉCIMA SÉTIMA – FORO

15.1. Fica eleito o Foro da Justiça Federal em ......, Seção Judiciária de ...... para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme art. 92, §1º, da Lei nº 14.133/21.

16. MATRIZ DE RISCO

16.1. Por se tratar de objeto rotineiro, sem aferição de riscos aparentes para a Administração Pública, dispensa a elaboração da matriz de risco.

...., ... de... de 20.....

____

Responsável legal da CONTRATANTE

____

Responsável legal da CONTRATADA TESTEMUNHAS:

1-

2-

TERMO DE REFERÊNCIA 01/2025

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Registro de Preço para futura e eventual contratação de empresa especializada para prestação de serviços de segurança cibernética com Inteligência Artificial Preditiva, garantindo alta disponibilidade, segurança, eficiência e sustentabilidade no atendimento às demandas do Município de Cáceres, conforme condições e exigências estabelecidas neste instrumento.

1.1.1. O serviço a ser prestado engloba, fornecimento em regime de comodato, instalação e configuração de Next Generation Firewall (NGFW) e SD-WAN, redundância composta por links primário e secundário de ASN e rotas diferentes, manutenção contínua, suporte técnico, software de gerenciamento, conectividade segura para unidades externas e praças públicas, capacitação certificada da equipe e atendimento técnico especializado.

LOTE	ITEM	CÓDIGO TCE-MT	CÓDIGO CAT MAT	ESPECIFICAÇÃO	UNIDADE	QUANTIDADE	QUANTIDADE ANUAL
1 (ÚNICO)	1	257560-4	609340	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)	Serviço	173	2076
	2	152969	481647	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	Serviço	2	24
	3	00065206	26174	Serviço de Link dedicado de Acesso à internet, bloco /29 e Banda Mínima de Acesso Garantida de 500Mbps (Alta Disponibilidade) SEDE (Link de ASN e Rota Diferentes)	Serviço	2	24
	4	152970	26484	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 150Mbps Sites Remotos (Fibra Óptica)	Serviço	171	2052
	5	152972	26557	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G)	Serviço	171	2052
	6	339905-2	1988	Implantação da Solução	Serviço	1	1
	7	404876-8	16837	Capacitação especializada da equipe com emissão de certificação.	Treinamento	1	1
	8	332679-9	27340	Consultoria Política de Segurança	Serviço	1	1

1.2. A licitação será realizada por meio de um único lote, contendo diversos itens, conforme especificado no Termo de Referência. O licitante deverá apresentar uma proposta para todos os itens dentro do lote, sendo vedada a oferta parcial.

1.3. A análise da documentação terá por finalidade verificar a habilitação da empresa, bem como sua capacidade de operar um projeto dessa complexidade.

1.3.1. Caso as exigências não sejam atendidas, será convocada a empresa subsequente que tenha apresentado o preço global imediatamente superior, observadas as regras de negociação.

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

1.5. O prazo de vigência da contratação será de 12 (doze) meses, contados a partir da assinatura do contrato, podendo ser prorrogado por períodos iguais e consecutivos, desde que, durante o planejamento e toda a execução do contrato, sejam observadas as seguintes condições:

a) seja emitido ateste da autoridade competente do órgão ou entidade contratante, confirmando que a contratação representa a alternativa mais vantajosa do ponto de vista econômico, em razão de sua natureza plurianual;

b) haja previsão e disponibilidade de créditos orçamentários vinculados à contratação e justificativa quanto à conveniência de sua manutenção; e

c) a Administração possa rescindir o contrato, sem ônus, caso não disponha dos recursos orçamentários necessários à sua continuidade ou caso entenda que a contratação deixou de atender ao interesse público.

Esse prazo poderá se estender até o limite de 15 (quinze) anos, conforme estabelecido no artigo 114 da Lei nº 14.133/2021, diante da natureza continuada da operação e da sua caracterização como sistema estruturante de tecnologia da informação, conforme demonstrado no Estudo Técnico Preliminar.

1.6. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico do Estudo Técnico Preliminar, apêndice deste Termo de Referência.

3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

3.1. A Fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada em tópico específico do Estudo Técnico Preliminar, apêndice deste Termo de Referência.

3.2. O objeto da contratação está previsto no Plano de Contratações Anual [2025], conforme detalhamento a seguir:

I) ID PCA no PNCP: 03214145000183-0-000001/2025;

II) Data de publicação no PNCP: 28/01/2025;

III) Id do item no PCA: 166;

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

4.1. A solução tem por objetivo proporcionar uma infraestrutura robusta, segura e eficiente para o ambiente de tecnologia da informação da Prefeitura Municipal de Cáceres, assegurando a continuidade dos serviços públicos e a proteção dos dados institucionais. O ciclo de vida da solução contempla todas as fases essenciais, desde a implantação até a operação contínua, manutenção e eventuais atualizações tecnológicas, garantindo um alto padrão de qualidade e desempenho ao longo da vigência do contrato.

4.2. A solução contempla segurança cibernética avançada, conectividade de alto desempenho e suporte especializado, alinhando-se às melhores práticas de governança digital e proteção de ativos públicos.

4.3. A implantação e execução do contrato seguem um modelo estruturado em duas fases principais:

4.3.1. **Fase de Implantação**, com prazo de até 60 dias após a assinatura do contrato, abrangendo a instalação dos equipamentos, ativação dos links, integração das unidades externas e capacitação da equipe técnica.

4.3.2. **Fase de Prestação de Serviço Mensal**, com duração de até 180 meses, garantindo manutenção contínua, suporte técnico especializado, atualizações tecnológicas e otimização da infraestrutura de segurança e comunicação de dados.

4.4. O ciclo de vida da solução envolve etapas bem definidas, assegurando que a infraestrutura implementada esteja sempre atualizada e alinhada com as necessidades da Prefeitura.

4.4.1. **Planejamento e Implantação**

4.4.1.1. Na fase inicial, serão executadas as atividades necessárias para a estruturação da solução contratada, garantindo que todos os componentes sejam devidamente configurados e operacionalizados. Essa etapa inclui:

4.4.1.1.1. Instalação e configuração dos equipamentos de segurança cibernética, incluindo Next Generation Firewall (NGFW) e SD-WAN, visando a proteção contra ameaças digitais e a otimização do tráfego de rede.

4.4.1.1.2. Implementação de serviços de segurança cibernética baseados em Inteligência Artificial Preditiva, permitindo a detecção e resposta antecipada a incidentes.

4.4.1.1.3. Ativação dos links dedicados de internet, garantindo 500 Mbps na sede, 150 Mbps nos sites remotos e 35 Mbps como link de contingência, assegurando conectividade estável para as operações administrativas e serviços públicos digitais.

4.4.1.1.4. Integração das unidades externas e praças públicas à infraestrutura de rede segura, possibilitando um acesso seguro e confiável aos sistemas municipais.

4.4.1.1.5. Capacitação certificada da equipe técnica da Prefeitura, garantindo a qualificação necessária para a gestão e monitoramento da solução implementada.

4.4.2. **Operação e Manutenção**

4.4.2.1. Após a implantação, a solução entrará em operação contínua, garantindo que os serviços contratados sejam entregues de forma eficiente e dentro dos padrões de qualidade exigidos. Esta fase inclui:

4.4.2.1.1. Monitoramento contínuo da infraestrutura, com análises preditivas para detecção de ameaças e otimização do desempenho dos sistemas.

4.4.2.1.2. Suporte técnico especializado, disponível para resolver quaisquer incidentes ou necessidades de ajustes na configuração da solução.

4.4.2.1.3. Gestão e atualização dos equipamentos e software, garantindo que os firewalls, SD-WAN e demais componentes tecnológicos operem sempre com as versões mais recentes e seguras.

4.4.2.1.4. Consultoria contínua para aprimoramento da política de segurança da informação, com foco na proteção de dados, conformidade regulatória e mitigação de riscos cibernéticos.

4.4.2.1.5. Garantia de alta disponibilidade, com suporte a redundância de links e contingência operacional para evitar interrupções nos serviços municipais.

4.4.3. **Evolução e Sustentabilidade da Solução**

4.4.3.1. Ao longo do ciclo de vida da solução, serão adotadas práticas que garantam sua evolução tecnológica e sustentabilidade, permitindo que o investimento realizado permaneça eficiente e alinhado às necessidades do município. Entre essas práticas, destacam-se:

4.4.3.1.1. Adoção de tecnologias emergentes para otimizar a performance e segurança da infraestrutura de TIC.

4.4.3.1.2. Revisão periódica da estratégia de segurança cibernética, considerando as tendências de ameaças digitais e as melhores práticas do setor.

4.4.3.1.3. Expansão escalável da solução, permitindo a incorporação de novas unidades e serviços de forma ágil e estruturada.

4.4.3.1.4. Otimização do consumo de recursos tecnológicos, garantindo um uso eficiente da infraestrutura contratada e contribuindo para a sustentabilidade financeira e operacional do município.

4.5. **Especificação do Produto**

4.5.1. **Funcionamento Geral da Solução**

4.5.1.1. A contratação deverá englobar além das soluções de defesa cibernética a prestação de serviços de rede de longa distância (WAN) para manter a interligação da Sede da Prefeitura de Cáceres aos Sites Remotos, localizados no interior do Município e fora dele.

4.5.1.2. A contratação também inclui a prestação de serviço de acesso à internet nos Sites Remotos e na sede da Prefeitura Municipal de Cáceres MT.

4.5.1.3. A contratação deverá englobar o fornecimento de um conjunto de equipamentos de redes incluindo recursos de IP para trabalhar em alta disponibilidade na Sede e cada equipamento deverá permitir no mínimo 4(quatro) conexões à Internet.

4.5.1.4. A nova solução de comunicação de dados entre os Sites Remotos e a Sede utilizará equipamentos com a tecnologia SD-WAN com o objetivo de balancear o tráfego de forma inteligente para otimizar o uso da rede. Para que o tráfego corporativo seja protegido quando trafegar pela internet, serão configurados túneis VPN IPSEC entre os equipamentos SD-WAN da Sede da Prefeitura e dos Sites Remotos.

4.5.1.5. Os equipamentos SD-WAN da Sede deverão trabalhar em alta disponibilidade.

4.5.1.6. A relação dos Sites Remotos e da Central nos quais os serviços serão prestados encontra-se descrita no item 7.2.1.3 deste Termo de Referência.

4.5.1.7. Em situações normais, os tráfegos de sistemas da prefeitura sobretudo os administrativos, além do tráfego de telefonia IP, devem ser encaminhados pela via IPSEC pelo melhor link. Por outro lado, os serviços de videoconferência das Plataformas Zoom, Google, Webex e Microsoft Teams devem ser acessados diretamente sem a necessidade de utilização deste túnel, além da navegação de Internet das redes dos assessores, colaboradores e cidadãos que acessam a rede social da Prefeitura.

4.5.1.8. Em situações de falha ou de uso intenso da rede, alternativamente os tráfegos corporativos devem ser encaminhados entre os Sites Central e remotos utilizando também túnel VPN IPSEC pelo link secundário estabelecidos pela Internet. Os túneis VPN devem utilizar a topologia hub-and-spoke, com centralização nos equipamentos SD-WAN na Sede.

4.5.1.9. Em situações de falha de um dos links de Internet dos Sites remotos, o tráfego deve ser encaminhado pela conexão de internet secundária até o Site Central da Prefeitura.

4.5.1.10. A configuração do encaminhamento do tráfego e da contingência em casos de falha deve ser feita utilizando tecnologia SD-WAN em que o encaminhamento de tráfego é feito com base no perfil de tráfego em vez da utilização de rotas.

4.5.1.11. A prestação dos serviços descritos em cada ITEM deverá ser considerada como entregue, a partir da assinatura do Termo de Recebimento Definitivo.

4.5.1.12. A prestação dos serviços será baseada no modelo de remuneração em função dos resultados apresentados, em que os pagamentos serão feitos após mensuração e verificação de métricas quantitativas e qualitativas, contendo indicadores de desempenho e metas, com Instrumento de Medição de Resultado (IMR) definido em contrato, de modo a resguardar a eficiência e a qualidade na prestação dos serviços.

4.5.1.13. Os serviços a serem prestados incluem, ainda, a elaboração prévia de um Projeto Executivo de rede, a ser analisado pela equipe técnica da Prefeitura para aprovação, conforme especificações incluídas neste documento. Esse documento deverá conter, no mínimo:

a) Definição de topologias físicas e lógicas;

b) Plano de Endereçamento;

c) Plano de balanceamento do tráfego;

d) Parâmetros de qualidade de serviço;

e) Dimensionamento de enlaces e interfaces de comunicação;

f) Documentação dos últimos 1000 metros de passagem das fibras ópticas.

4.5.1.14. Não haverá aquisição de equipamentos, incluindo roteadores, modens, appliances SD- WAN e demais ativos de rede. Contudo, deverão ser fornecidos equipamentos juntamente com a prestação dos serviços de tecnologia da informação e comunicações como parte integrante da solução contratada.

4.5.1.15. O CONTRATANTE poderá solicitar a desativação do serviço prestado a qualquer sítio, bem como mudança de local de prestação dos serviços. Entende-se por mudanças de local de prestação dos serviços a mudança de endereços de instalação dos equipamentos e acessos dentro da cidade.

4.5.1.16. Após a conclusão da etapa de instalação dos serviços, a CONTRATADA deverá apresentar documentação técnica da solução (As Built), contendo: topologia física e lógica da rede, descrição de equipamentos e circuitos de comunicação de dados, descrição dos níveis mínimos de serviços contratados, dados para acesso ao portal de monitoramento dos serviços e dados para abertura de chamados de suporte técnico.

4.5.1.17. A CONTRATADA deverá também realizar repasse de conhecimento na modalidade presencial para a equipe técnica do CONTRATANTE sobre a solução implantada, conforme descrito no item 5.2 deste Termo de Referência.

4.5.2. **Topologia Da Solução**

4.5.2.1. A solução foi estruturada com base nas necessidades específicas da Prefeitura Municipal de Cáceres, visando garantir conectividade segura, eficiente e de alta disponibilidade para todas as unidades envolvidas. A infraestrutura foi projetada para suportar um volume significativo de acessos simultâneos, assegurando a qualidade da comunicação de dados, a integridade das informações e a segurança cibernética dos sistemas institucionais.

4.5.2.1.1. Estruturação dos Sites e Capacidade dos Links

4.5.2.1.1.1. A topologia da solução foi desenhada considerando a divisão dos Sites Remotos e do Site Central em dois tipos distintos de tecnologia e capacidade de conexão, com base na demanda estimada de usuários simultâneos e nos requisitos operacionais de cada localidade.

4.5.2.1.1.1.1. **Sites Remotos:** A estrutura contempla unidades como Postos de Saúde, Centros de Saúde e espaços públicos, onde os serviços de tecnologia da informação serão utilizados para fins administrativos e sociais. A demanda estimada para os Postos de Saúde varia entre 7 e 10 usuários simultâneos, enquanto os Centros de Saúde podem atender de 15 a 30 usuários simultaneamente. O tráfego nesses locais incluirá tanto o acesso aos sistemas institucionais da Prefeitura quanto a utilização de serviços públicos digitais pelos cidadãos.

4.5.2.1.1.1.2. **Site Central:** A Sede da Prefeitura concentra entre 400 e 500 usuários simultâneos, entre servidores e colaboradores, acessando tanto recursos internos quanto externos. Devido ao alto volume de tráfego e à criticidade dos serviços processados, a conexão do Site Central conta com dois links dedicados de alta capacidade (500 Mbps cada), providos por ASN distintos e rotas diferentes, garantindo redundância e continuidade operacional.

4.5.2.1.1.2. A configuração dos links de internet e a implementação da tecnologia SD-WAN asseguram balanceamento inteligente do tráfego, priorização de pacotes críticos e segurança reforçada para as comunicações entre as unidades.

4.5.2.1.2. **Topologia Lógica da Solução**

4.5.2.1.2.1. A topologia lógica da solução foi elaborada para representar a interconexão dos elementos envolvidos e demonstrar o produto final desta contratação. A arquitetura contempla os seguintes componentes essenciais:

4.5.2.1.2.1.1. Next Generation Firewalls (NGFW) instalados no Site Central, atuando como pontos de controle de segurança cibernética, prevenindo ataques e garantindo a integridade dos dados trafegados entre as unidades.

4.5.2.1.2.1.2. Solução de segurança cibernética com utilização de Inteligência Preditiva.

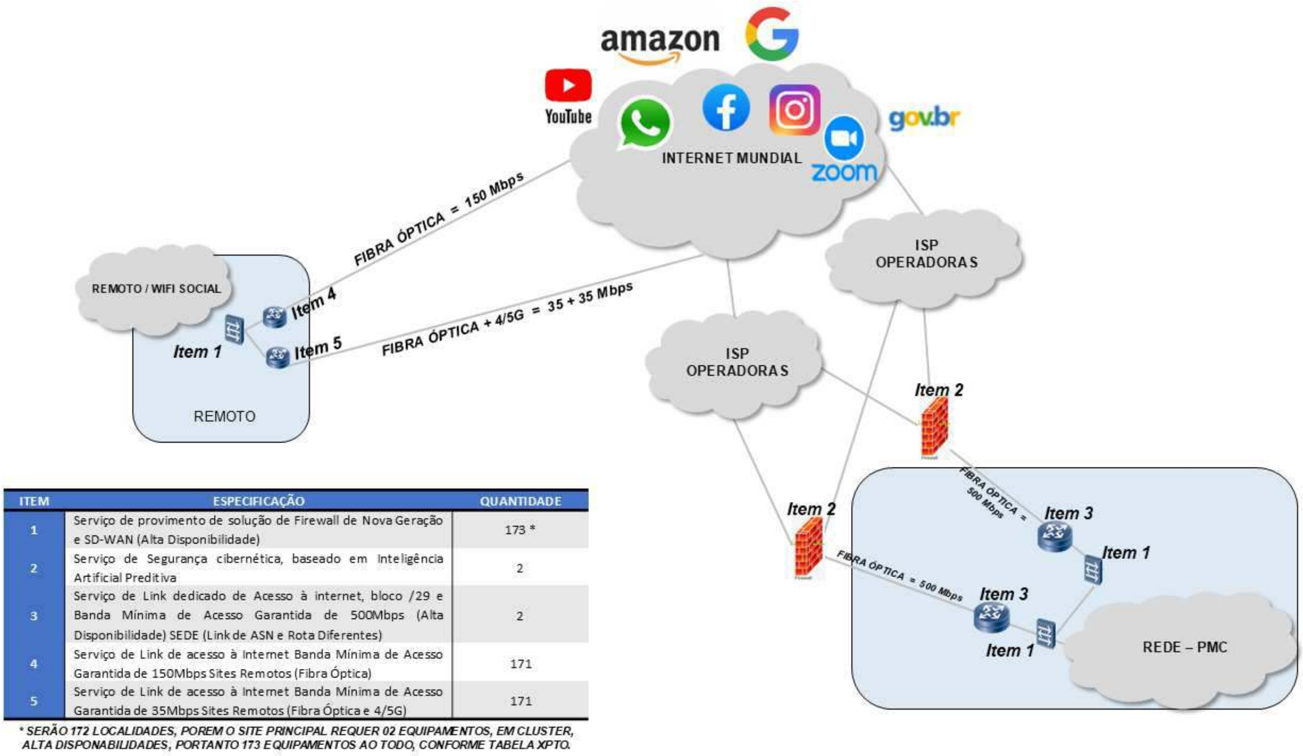
4.5.2.1.2.1.3. Dispositivos SD-WAN implementados na Sede e nos Sites Remotos, possibilitando gerenciamento eficiente do tráfego, redundância e otimização dos links de comunicação.

4.5.2.1.2.1.4. VPN IPSEC configurada em topologia hub-and-spoke, assegurando segurança na troca de informações entre os Sites Remotos e o Site Central.

4.5.2.1.2.1.5. Monitoramento centralizado, por meio de um software de gestão e segurança, permitindo a visualização em tempo real do tráfego da rede, detecção de anomalias e gerenciamento proativo de incidentes.

4.5.2.1.2.1.6. Consultoria especializada e capacitação da equipe técnica da Prefeitura, garantindo conhecimento sobre a administração da solução e autonomia na gestão da infraestrutura implantada.

4.5.2.1.2.2. Foi elaborada uma topologia lógica da solução demonstrando o produto final desta contratação:



ITEM	ESPECIFICAÇÃO	QUANTIDADE
1	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)	173 *
2	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	2
3	Serviço de Link dedicado de Acesso à internet, bloco /29 e Banda Mínima de Acesso Garantida de 500Mbps (Alta Disponibilidade) SEDE (Link de ASN e Rota Diferentes)	2
4	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 150Mbps Sites Remotos (Fibra Óptica)	171
5	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G)	171

** SERÃO 172 LOCALIDADES, POREM O SITE PRINCIPAL REQUER 02 EQUIPAMENTOS, EM CLUSTER, ALTA DISPONABILIDADES, PORTANTO 173 EQUIPAMENTOS AO TODO, CONFORME TABELA XPTO.*

4.5.3. **Equipamentos e Funcionalidades Chave**

4.5.3.1. **Os equipamentos do ITEM 1, do Lote Único, deverão ser entregues no formato e características técnicas bem como funcionalidades conforme especificações abaixo:**

4.5.3.1.1. **Appliance NGFW de 5 Gbps de Capacidade de Firewall**

4.5.3.1.1.1. **Características do Hardware**

4.5.3.1.1.1.1. O equipamento deve se instalar em mesa ocupando no máximo 1U (44,45mm) da referida mesa;

4.5.3.1.1.1.2. Dispor de fonte de alimentação com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;

4.5.3.1.1.1.3. Deverão ser fornecidos todos os cabos de energia, serial (RS-232/RJ45), para instalação e funcionamento do dispositivo;

4.5.3.1.1.1.4. Possuir led indicador on/off, disco e devices de rede;

4.5.3.1.1.1.5. Possuir throughput mínimo de 5 Gbps para tráfego UDP;

4.5.3.1.1.1.6. Suportar no mínimo 4.000.000 (quatro milhões) conexões simultâneas;

4.5.3.1.1.1.7. Suportar no mínimo 37.000 (trinta e sete mil) novas conexões por segundo;

4.5.3.1.1.1.8. Possuir throughput mínimo de 300 Mbps para tráfego IPS/IDS;

4.5.3.1.1.1.9. Possuir throughput mínimo de 280 Mbps para tráfego VPN IPSEC com criptografia (AES-256);

4.5.3.1.1.1.10. Possuir throughput mínimo de 140 Mbps para tráfego VPN SSL com criptografia (AES-256);

4.5.3.1.1.1.11. Possuir throughput mínimo de 150 Mbps para SSL Inspection;

4.5.3.1.1.1.12. Possuir throughput mínimo de 200 Mbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

4.5.3.1.1.1.13. Possuir no mínimo 4 (quatro) interfaces de rede Gigabit Ethernet 10/100/1000/2500 Mbps com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

4.5.3.1.1.1.14. Possuir dispositivo de armazenamento interno de no mínimo 64 GB padrão SSD e deve suportar expansão futura para, no mínimo, 120 GB;

4.5.3.1.1.1.15. Possuir no mínimo 1 (uma) porta console de conexão para acesso a interface de comando CLI específica para esta finalidade, utilizando cabo do tipo serial RS-232 ou RJ-45;

4.5.3.1.1.1.16. Possuir pelo menos 1 (uma) portas USB para conexão de dispositivos externos;

4.5.3.1.1.1.17. A interface USB deve suportar o uso de modem 3G/4G/LTE e/ou possuir modem interno 3G/4G/LTE para conexão de link de Internet. O módulo deverá estar incluso no valor do equipamento;

4.5.3.1.2. **Appliance NGFW de 9.7 Gbps de Capacidade de Firewall**

4.5.3.1.2.1. **Características do Hardware**

4.5.3.1.2.1.1. O equipamento deve se instalar em mesa ocupando no máximo 1U (44,45mm) da referida mesa;

4.5.3.1.2.1.2. Dispor de fonte de alimentação com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;

4.5.3.1.2.1.3. Deverão ser fornecidos todos os cabos de energia, serial (RS-232/RJ45) ou similar, para instalação e funcionamento do dispositivo;

4.5.3.1.2.1.4. Possuir led indicador on/off, disco e devices de rede;

4.5.3.1.2.1.5. Possuir throughput mínimo de 9.7 Gbps para tráfego UDP;

4.5.3.1.2.1.6. Suportar no mínimo 6.000.000 (seis milhões) conexões simultâneas;

4.5.3.1.2.1.7. Suportar no mínimo 45.000 (quarenta e cinco mil) novas conexões por segundo;

4.5.3.1.2.1.8. Possuir throughput mínimo de 1.25 Gbps para tráfego IPS/IDS;

4.5.3.1.2.1.9. Possuir throughput mínimo de 2.0 Gbps para tráfego VPN IPSEC com criptografia (AES-256);

4.5.3.1.2.1.10. Possuir throughput mínimo de 1.2 Gbps para tráfego VPN SSL com criptografia (AES-256);

4.5.3.1.2.1.11. Possuir throughput mínimo de 700 Mbps para tráfego SSL Inspection;

4.5.3.1.2.1.12. Possuir throughput mínimo de 850 Mbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

4.5.3.1.2.1.13. Possuir no mínimo 4 (quatro) interfaces de rede Gigabit Ethernet 10/100/1000/2500 Mbps com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

4.5.3.1.2.1.14. Possuir dispositivo de armazenamento interno de no mínimo 64 GB padrão SSD e deve suportar expansão futura para, no mínimo, 120 GB;

4.5.3.1.2.1.15. Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento;

4.5.3.1.2.1.16. Possuir pelo menos 1 (uma) porta USB para conexão de dispositivos externos;

4.5.3.1.2.1.17. A interface USB deve suportar o uso de modem 3G/4G/LTE e/ou possuir modem interno 3G/4G/LTE para conexão de link de Internet. O módulo deverá estar incluso no valor do equipamento;

4.5.3.1.3. **Appliance NGFW de 11.8 Gbps de Capacidade de Firewall**

4.5.3.1.3.1. **Características do Hardware**

4.5.3.1.3.1.1. O equipamento deve se instalar em mesa ocupando no máximo 1U (44,45mm) da referida mesa;

4.5.3.1.3.1.2. Dispor de fonte de alimentação com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;

4.5.3.1.3.1.3. Deverão ser fornecidos todos os cabos de energia, serial (RS-232/RJ45) ou similar, para instalação e funcionamento do dispositivo;

4.5.3.1.3.1.4. Possuir led indicador on/off, disco e devices de rede;

4.5.3.1.3.1.5. Possuir throughput mínimo de 11.8 Gbps para tráfego UDP;

4.5.3.1.3.1.6. Suportar no mínimo 7.000.000 (sete milhões) conexões simultâneas;

4.5.3.1.3.1.7. Suportar no mínimo 52.000 (cinquenta e duas mil) novas conexões por segundo;

4.5.3.1.3.1.8. Possuir throughput mínimo de 1.5 Gbps para tráfego IPS/IDS;

4.5.3.1.3.1.9. Possuir throughput mínimo de 2.5 Gbps para tráfego VPN IPSEC com criptografia (AES-256);

4.5.3.1.3.1.10. Possuir throughput mínimo de 1.5 Gbps para tráfego VPN SSL com criptografia (AES-256);

4.5.3.1.3.1.11. Possuir throughput mínimo de 900 Mbps para tráfego SSL Inspection;

4.5.3.1.3.1.12. Possuir throughput mínimo de 1.0 Gbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

4.5.3.1.3.1.13. Possuir no mínimo 6 (seis) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

4.5.3.1.3.1.14. Possuir dispositivo de armazenamento interno de no mínimo 120 GB padrão SSD;

4.5.3.1.3.1.15. Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento;

4.5.3.1.3.1.16. Possuir pelo menos 1 (uma) porta USB para conexão de dispositivos externos;

4.5.3.1.3.1.17. A interface USB deve suportar o uso de modem 3G/4G/LTE e/ou possuir modem interno 3G/4G/LTE para conexão de link de Internet. O módulo deverá estar incluso no valor do equipamento;

4.5.3.1.4. **Appliance NGFW de 19.4 Gbps de Capacidade de Firewall**

4.5.3.1.4.1. **Características do Hardware**

4.5.3.1.4.1.1. Deverá ser entregue dois equipamentos idênticos para atender a funcionalidade de cluster;

4.5.3.1.4.1.2. O equipamento deve se instalar em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo 1U (44,45mm) do referido rack;

4.5.3.1.4.1.3. Dispor de fonte de alimentação interna com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;

4.5.3.1.4.1.4. Possuir painel/led indicador on/off, disco e devices de rede;

4.5.3.1.4.1.5. Possuir throughput de no mínimo 19.4 Gbps para tráfego UDP;

4.5.3.1.4.1.6. Suportar no mínimo 8.200.000 (oito milhões e duzentas mil) conexões simultâneas;

4.5.3.1.4.1.7. Suportar no mínimo 65.000 (sessenta e cinco mil) novas conexões por segundo;

4.5.3.1.4.1.8. Possuir throughput mínimo de 3.0 Gbps para tráfego IPS/IDS;

4.5.3.1.4.1.9. Possuir throughput mínimo de 3.0 Gbps para tráfego VPN IPSEC com criptografia (AES-256);

4.5.3.1.4.1.10. Possuir throughput mínimo de 1.8 Gbps para tráfego VPN SSL com criptografia (AES-256);

4.5.3.1.4.1.11. Possuir throughput mínimo de 1.3 Gbps para tráfego SSL Inspection;

4.5.3.1.4.1.12. Possuir throughput mínimo de 2.5 Gbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);

4.5.3.1.4.1.13. Possuir pelo menos 6 (seis) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;

4.5.3.1.4.1.14. Possuir dispositivo de armazenamento interno de no mínimo 120 GB padrão SSD;

4.5.3.1.4.1.15. Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento;

4.5.3.1.4.1.16. Possuir no mínimo 1 (uma) porta USB para conexão de dispositivos externos;

4.5.3.1.4.1.17. A interface USB deve suportar o uso de modem 3G/4G/LTE e/ou possuir modem interno 3G/4G/LTE para conexão de link de Internet. O módulo deverá estar incluso no valor do equipamento;

4.5.3.2. **Especificações Gerais de Software NGFW Para Todos os Itens**

4.5.3.2.1. **Das Funcionalidades do Firewall, SD-Wan, VPN IPsec/SSL**

4.5.3.2.1.1. **Características Gerais**

4.5.3.2.1.1.1. Quaisquer licenças que forem entregues para atender aos recursos da solução especificado no termo de referência, deverão ter seu vencimento de acordo com o período de contrato.

4.5.3.2.1.1.2. O desempenho e as interfaces solicitados deverão ser comprovados através de datasheet público na internet. Caso haja divergência entre métricas do mesmo datasheet, será aceito o valor de menor capacidade.

4.5.3.2.1.1.3. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

4.5.3.2.1.1.4. Todos os recursos listados neste termo de referência deverão ser suportado e estar disponíveis na versão mais atual do software fornecido;

4.5.3.2.1.1.5. Os desempenhos dos appliances ofertados devem ser mensurados através da metodologia baseada em proxy (Proxy Based), não serão aceitos appliances mensurados somente no método baseado em fluxo (Flow Based);

4.5.3.2.1.1.6. Interface sendo em exclusivo ou em conjunto na linguagem português e/ou espanhol e/ou inglês;

4.5.3.2.1.1.7. Suportar notificação de vencimento da licença na janela de alertas com os dias restantes da data vencimento;

4.5.3.2.1.1.8. Suportar acesso à Web por HTTP e CLI por TELNET;

4.5.3.2.1.1.9. Permitir alterar a porta padrão para os acessos a interface de administração via HTTP, HTTPs e CLI;

4.5.3.2.1.1.10. Atualização de modo "offline", onde pode ser baixado na base do fabricante e posteriormente fazer o upload do arquivo na solução.

4.5.3.2.1.1.11. Restore de Snapshot sem executar o Wizard e sem licenciamento;

4.5.3.2.1.1.12. A solução deve oferecer suporte ao NAT444 (CGNAT) ou funcionalidade que implemente a persistência no NAT de saída independente da porta de destino, de forma que o endereço IP e porta traduzidos para um determinado usuário se mantenham os mesmos nas novas sessões que cheguem com o mesmo endereçamento IP e porta de origem;

4.5.3.2.1.1.13. Suportar segundo fator de autenticação (2FA/MFA) via token / OTP (One Time Password);

4.5.3.2.1.1.14. Deve suportar sistemas virtuais;

4.5.3.2.1.1.15. 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 diferentemente;

4.5.3.2.1.1.16. Qualquer interface de rede do equipamento deverá ser utilizada como gerenciamento, ou seja, não deve haver nenhuma interface exclusiva para a função de gerenciamento;

4.5.3.2.1.1.17. O sistema deve permitir o acesso à interface de gerenciamento WEB por qualquer interface de rede configurada;

4.5.3.2.1.1.18. O software deverá ser fornecido em sua versão mais atualizada, não sendo permitido qualquer tipo de comprovação futura.

4.5.3.2.1.1.19. Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução.

4.5.3.2.1.1.20. Todos os recursos detalhados no termo de referência deverão ser providos por um único software.

4.5.3.2.1.1.21. Tanto os Gateways de Segurança bem como a Gerência Centralizada deverão suportar monitoramento através de SNMP v1, v2 e v3.

4.5.3.2.1.1.22. Deverá possuir uma janela para monitoramento do tráfego de rede com informações do throughput e da quantidade de conexões simultâneas;

4.5.3.2.1.1.23. A Solução deverá prover inspeção SSL:

4.5.3.2.1.1.24. Deve suportar cluster do tipo Failover (HA) com replicação da tabela de estado;

4.5.3.2.1.1.25. Suportar a utilização de um proxy para atualização do software e licenciamento e deverá permitir as seguintes opções de configuração:

a) Endereço do servidor;
b) Porta do servidor;
c) Usuário;
d) Senha;

4.5.3.2.1.1.26. Deverá permitir o monitoramento SNMP, no mínimo, dos seguintes itens:

a) Desempenho total (throughput);
b) Conexões simultâneas;
c) Usuários autenticados;
d) Serviços habilitados ou desabilitados;
e) Quantidade de endereços distribuídos pelo DHCP.

4.5.3.2.1.1.27. Deverá implementar a funcionalidade de "zero-touch" para sua primeira implementação ou substituição. Dessa forma, deverá ser possível provisionar a configuração do equipamento via sistema de gerenciamento centralizado, transformando a atividade em uma simples conexão física de equipamento, sem a necessidade de configurações individuais nos equipamentos;

4.5.3.2.1.1.28. A Solução deve permitir ao administrador associar na solução de gerenciamento centralizado o número de série dos equipamentos ao site onde será instalado, de maneira que ao se ativar um equipamento no site remoto, esse equipamento se conecte com a Sistema Central e receba a configuração;

4.5.3.2.1.1.29. Ao instalar um equipamento no site remoto, cabeá-lo e energizá-lo, ele deverá tentar localizar Sistema Central para receber a sua configuração, sem que seja necessária qualquer configuração via console local do equipamento.

4.5.3.2.1.1.30. Deverá possuir um painel centralizado para exportação e agendamento de relatórios e deverá permitir exportá-los nos formatos: HTML, PDF, CSV;

4.5.3.2.1.1.31. Implementar protocolo de coleta de informações de fluxos que circulam pelo equipamento, como Netflow v5, v9 e v10 (IPFIX):

4.5.3.2.1.1.32. Os módulos de IPS, SD-WAN, Controle de aplicativos, Proxy WEB e Antimalware devem ser disponibilizados em perfis e estes devem ser inseridos em uma única política;

4.5.3.2.1.1.33. Deve implementar o protocolo ECMP;

4.5.3.2.1.1.34. O sistema deverá implementar otimização de fluxos TCP em conjunto com mecanismo para evitar retransmissão ou implementar métodos de correção de erros que permitam à unidade receptora recuperar pacotes que venham a ser perdidos na transmissão.

4.5.3.2.1.1.35. Deve possuir suporte ao protocolo de encapsulamento de redes MPLS;

4.5.3.2.1.1.36. Esta condição deve permitir conectar links MPLS diretamente no equipamento sem a necessidade de estar plugado a um segundo roteador/dispositivo.

4.5.3.2.1.1.37. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;

4.5.3.2.1.1.38. 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;

4.5.3.2.1.2. **Recursos Gerais de Firewall**

4.5.3.2.1.2.1. Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas;

4.5.3.2.1.2.2. Possuir um sistema de armazenamento remoto para salvar backups da solução com suporte a conexões utilizando os protocolos Network File System (NFS), SSH e que permita salvar em dispositivo USB conectado localmente;

4.5.3.2.1.2.3. Possibilitar a visualização dos países de origem e destino nos logs de eventos, de acessos e ameaças.

4.5.3.2.1.2.4. Possuir mecanismo que permita a realização de cópias de segurança (backups) do sistema e restauração remota, através da interface gráfica, a solução deve permitir o agendamento diário ou semanal;

4.5.3.2.1.2.5. O sistema deve permitir configurar o período ou número de cópias que deseja manter no repositório remoto e executar a manutenção de período automaticamente.

4.5.3.2.1.2.6. As cópias de segurança devem ser salvas compactadas e criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;

4.5.3.2.1.2.7. O sistema ainda deve contemplar um recurso de cópia de segurança do tipo snapshot, que contemple a cópia completa das configurações dos serviços e recursos do sistema;

4.5.3.2.1.2.8. Deve possibilitar a restauração do snapshot através da interface web de qualquer ponto remoto, de modo a contribuir para uma restauração imediata sem a necessidade de reinicialização do sistema;

4.5.3.2.1.2.9. Deve permitir habilitar ou desabilitar o registro de log por política de firewall.

4.5.3.2.1.2.10. Possuir controle de acesso à internet por endereço IP de origem e destino;

4.5.3.2.1.2.11. Possuir controle de acesso à internet por sub-rede;

4.5.3.2.1.2.12. Possuir suporte a tags de VLAN (802.1q);

4.5.3.2.1.2.13. Suportar agregação de links, segundo padrão IEEE 802.3ad;

4.5.3.2.1.2.14. Possuir ferramenta de diagnóstico do tipo tcpdump;

4.5.3.2.1.2.15. Possuir integração com Servidores de Autenticação RADIUS, TACACS+, LDAP e Microsoft Active Directory;

4.5.3.2.1.2.16. Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

4.5.3.2.1.2.17. Possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um, vários para vários e vários para um.

4.5.3.2.1.2.18. Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;

4.5.3.2.1.2.19. Permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br;

4.5.3.2.1.2.20. Possuir suporte a roteamento dinâmico RIP V1, V2, OSPFv2, OSPFv3, BGP e suportar duplicação de pacotes;

4.5.3.2.1.2.21. Possuir funcionalidades de DHCP Cliente, Servidor e Relay;

4.5.3.2.1.2.22. Deve ser possível configurar um servidor RADIUS para a validação de usuários;

4.5.3.2.1.2.23. A solução deve consultar o Servidor Radius integrado, caso o Servidor Radius autorize, o NGFW deve entregar o endereço IP do range; caso contrário, não fornece endereço IP e a máquina não recebe o endereço, ficando sem acesso à rede.

4.5.3.2.1.2.24. Deverá suportar aplicações multimídia como: H.323, SIP;

4.5.3.2.1.2.25. Possuir tecnologia de firewall do tipo Stateful;

4.5.3.2.1.2.26. Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo-passivo;

4.5.3.2.1.2.27. Permitir o funcionamento em modo transparente tipo "bridge";

4.5.3.2.1.2.28. Permitir a criação de mínimo 4090 VLANS no padrão IEEE 802.1q por interface de rede;

4.5.3.2.1.2.29. Possuir conexão entre estação de gerência e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando);

4.5.3.2.1.2.30. Deverá suportar forwarding de multicast;

4.5.3.2.1.2.31. Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP;

4.5.3.2.1.2.32. Permitir o agrupamento de serviços;

4.5.3.2.1.2.33. Possuir mecanismo de anti-spoofing;

4.5.3.2.1.2.34. Possuir a funcionalidade de balanceamento e contingência de links;

4.5.3.2.1.2.35. Possibilitar a configuração dos timeouts de resposta dos protocolos de conexão, devendo suportar no mínimo a definição das opções do timeout padrão do ICMP, estabelecimento do TCP, envio do SYN em sessões TCP.

4.5.3.2.1.2.36. Permitir a configuração de regras de entrada baseado em zona de rede, possibilitando habilitar recursos de autenticação e restrição por origem baseado em IP.

4.5.3.2.1.2.37. Deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas, suportando ao menos: Yahoo! Messenger, MSN Messenger, ICQ, Telegram, Whatsapp, WeChat, Snapchat BitTorrent, UTorrent, Vuze, eDonkey, GNUTella, Skype e Microsoft Teams.

4.5.3.2.1.2.38. A solução deverá suportar nativamente o recurso SIMET (nic.br) medidor de Internet.

4.5.3.2.1.3. **Política de Segurança**

4.5.3.2.1.3.1. Permitir limitar a quantidade máxima de pacotes por segundo no Firewall, evitando ataques distribuídos ou anomalias de tráfego causadas por possíveis malwares na rede;

4.5.3.2.1.3.2. A configuração de proteção DOS deve estar disponível para habilitar em modo global e por política de segurança;

4.5.3.2.1.3.3. Possuir recurso de validação das políticas de segurança para identificar regras duplicadas ou que se ofusquem;

4.5.3.2.1.3.4. Possui uma única janela de configuração de política de segurança onde seja possível inserir os perfis de Proxy WEB, IPS, APP control, SD-WAN e ATP.

4.5.3.2.1.3.5. Deverá permitir implementar filtros de IPS, WEB Filter, Threat Protection, SSL Inpection, Application Control, assim como definir roteamento de aplicativos por SD-Wan, limitação de taxa de DOS por pacotes em uma única política.

4.5.3.2.1.3.6. Exibir na própria política a visualização de quais módulos estão habilitados, sem que seja necessário a edição da regra de proteção.

4.5.3.2.1.3.7. Possibilitar a edição de objetos vinculados, sem a necessidade de recriar a política.

4.5.3.2.1.3.8. Possibilitar a duplicação de uma política, otimizando tempo de configuração;

4.5.3.2.1.4. **Identificação de Usuário**

4.5.3.2.1.4.1. Deve possuir a capacidade de criação de políticas de acesso de Firewall, VPN, IPS e Controle de aplicação integradas ao repositório de usuários sendo: Active Directory, LDAP, TACAC´S e Radius;

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

4.5.3.2.1.4.3. Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador (Captive Portal), sem a necessidade de agente;

4.5.3.2.1.4.4. Deve possuir Captive Portal com suporte a Autenticação Social (Facebook, Twitter, Google);

4.5.3.2.1.4.5. A solução deverá ser capaz de identificar nome do usuário, login, máquina/computador registrados no Microsoft Active Directory;

4.5.3.2.1.4.6. Para o sistema de controles no serviço de autenticação o produto deve possuir, no mínimo, as seguintes condições para o Controle de Autenticação:

a) Usuários e Grupos de Usuários;
b) Datas (Objetos de Datas)
c) Horários (Objetos de Horário)
d) Lista de palavras chave ou conjunto de combinações de expressões regulares, (Objetos de Dicionários)
e) Endereços Remotos (Objetos de IPv4 e IPv6)
f) Zona de Rede (Múltiplas Zonas)

4.5.3.2.1.4.7. A solução deve suportar autenticação por SSO utilizando WMI (Windows Management Instrument), ou seja, não deve ser necessário instalar nenhum agente no servidor de autenticação.

4.5.3.2.1.4.8. A solução deve suportar o sincronismo entre vários NGFW em relação a replicação das sessões autenticadas da filial (Branch) na matriz (Head Office) e vice-versa, sem a necessidade de agentes externos.

4.5.3.2.1.4.9. A solução deverá suportar múltiplos Servidores de Autenticação (MS AD e/ou Ldap) atuando no modo failover;

4.5.3.2.1.5. **Das Funcionalidades Da Vpn:**

4.5.3.2.1.5.1. VPN baseada em appliance;

4.5.3.2.1.5.2. Possuir algoritmos de criptografia para túneis VPN: AES, 3DES;

4.5.3.2.1.5.3. Suporte a certificados PKI X.509 para construção de VPNs;

4.5.3.2.1.5.4. Possuir suporte a VPNs IPSec site-to-site:

4.5.3.2.1.5.5. Criptografia, 3DES, AES128, AES256, AES-GCM-128

4.5.3.2.1.5.6. Integridade MD5, SHA-1, SHA-256, SHA384 e AES-XCBC;

4.5.3.2.1.5.7. Algoritmo Internet Key Exchange (IKE) versões I e II;

4.5.3.2.1.5.8. AES 128 e 256 (Advanced Encryption Standard);

4.5.3.2.1.5.9. Suporte a Diffie-Hellman Grupo 1, Grupo 2, Grupo 5, Grupo 14; Grupo 15, Grupo 16, Grupo 17, Grupo 18, Grupo 19, Grupo 20, Grupo 21, Grupo 22, Grupo 23, Grupo 24, Grupo 25, Grupo 26, Grupo 27, Grupo 28, Grupo 29, Grupo 30, Grupo 31, Grupo 32;

4.5.3.2.1.5.10. Possuir suporte a VPN SSL;

4.5.3.2.1.5.11. Possuir capacidade de realizar SSL VPNs utilizando certificados digitais;

4.5.3.2.1.5.12. Suportar VPN SSL Clientless, sem a necessidade de utilização de Java, no mínimo, para os serviços abaixo:

a) RDP;
b) VNC;
c) SSH;
d) WEB;
e) SMB.

4.5.3.2.1.5.13. Deve permitir a arquitetura de vpn hub and spoke;

4.5.3.2.1.5.14. Suporte a VPNs IPSec client-to-site;

4.5.3.2.1.5.15. Deverá possuir cliente próprio para Windows para o estabelecimento da VPN client-to-site.

4.5.3.2.1.5.16. Suporte à inclusão em autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol);

4.5.3.2.1.5.17. Possuir funcionalidades de Auto-Discovery VPN capaz de permitir criar tuneis de VPN dinâmicos entre múltiplos dispositivos (spokes) com um gateway centralizador (hub).;

4.5.3.2.1.5.18. A funcionalidade de AD-VPN deve suportar criar os seguintes tipos de tuneis:

a) Site-to-Site;
b) Full-Mesh;
c) Star.

4.5.3.2.1.5.19. Suportar configuração VTI (virtual interface) na configuração de túneis VPN site-to-site com BGP (Border

Gateway Protocol). Os túneis são utilizados para prover uma comunicação criptografada e encapsulada, por rotas, entre o peer (NGFW local) e o host;

4.5.3.2.1.5.20. A solução poderá atuar como cliente de tuneis VPN IPSec com suporte à autenticação XAuth/PSK e/ou XAuth/RSA.

4.5.3.2.1.5.21. A VPN client-to-site deve suportar o estabelecimento automático da VPN nos protocolos ICMP ou DNS (53/UDP), caso o cliente remoto identifique que a porta padrão está sendo bloqueada;

4.5.3.2.1.5.22. Possuir recurso para configurar vários túneis simultâneos da VPN cliente-to-site, com o objetivo de aumentar o desempenho do tráfego;

4.5.3.2.1.5.23. Suportar segundo fator de autenticação (2FA/MFA) via token / OTP (One Time Password);

4.5.3.2.1.6. **SD-WAN:**

4.5.3.2.1.6.1. Entende-se como tecnologia SD-WAN (Software-Defined WAN) a rede de área ampla definida por software que centraliza a gerência da rede WAN em uma console única, eliminando a necessidade de intervenções manuais em roteadores em localidades remotas, proporcionando visibilidade do tráfego, seleção de caminho dinâmico baseado em políticas de QoS, aplicação ou performance e utilização de túneis VPN para comunicação entre os sites remotos;

4.5.3.2.1.6.2. Possuir o balanceamento automático para conexões externas à internet através das interfaces físicas;

4.5.3.2.1.6.3. Suportar modo de duplicação de pacotes de dados pelo links WAN, para que em caso de queda do link principal, possa ser enviado ao link secundário uma cópia do pacote de dados perdido permitindo assim a maior integridade e disponibilidade do tráfego;

4.5.3.2.1.6.4. Permitir utilizar VPN IPsec para interligar unidades remotas;

4.5.3.2.1.6.5. Possuir recurso de "persistência de link" para impedir a queda de conexões em aplicações que não suportam o load balance de link;

4.5.3.2.1.6.6. O balanceamento deverá ser baseado em critérios de desempenho, devendo no mínimo, permitir verificar o monitoramento do consumo de banda, perda de pacotes, jitter e latência;

4.5.3.2.1.6.7. Deve possuir uma janela web ou dashboard capaz de fornecer informações dos eventos e com informações do monitoramento de desempenho relacionado ao recurso SD-WAN;

4.5.3.2.1.6.8. O recurso de SD-WAN deverá suportar o roteamento de tráfego por política baseado em aplicação;

4.5.3.2.1.6.9. O appliance SD-WAN deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorrerá quando o link monitorado recuperado seja avaliado. Deve suportar especificar um valor variando de 1 a 100.

4.5.3.2.1.6.10. O recurso de SD-WAN deverá permitir o monitoramento de, no mínimo 03 (três) endereços alvos para verificar a disponibilidade e desempenho do link;

4.5.3.2.1.6.11. A solução de SD-WAN NGFW deve permitir a configuração da funcionalidade de SD-WAN em qualquer interface WAN de forma agnóstica, independente se é internet, 3G/4G/LTE, entre outras;

4.5.3.2.1.6.12. A solução deverá suportar os seguintes métodos de seleção de link:

a) Failover;
b) Load Balance;
c) Spillover;
d) Dynamic Selection;

4.5.3.2.1.6.13. Deverá oferecer um monitor capaz de prover em tempo real as seguintes informações em uma única janela:

a) Consumo de banda;
b) Perda de pacotes;
c) Jitter;
d) Latência.

4.5.3.2.1.6.14. A Solução de SD-WAN deve desempenhar a função de Packet Duplication (PD) permitindo encaminhar o pacote por mais de um circuito para em casos de falhas não haver retransmissão;

4.5.3.2.1.7. **Das Funcionalidades de QoS**

4.5.3.2.1.7.1. Adotar solução de Qualidade de Serviço baseada em appliance;

4.5.3.2.1.7.2. Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;

4.5.3.2.1.7.3. Permitir modificação de valores DSCP;

4.5.3.2.1.7.4. Limitar individualmente a banda utilizada por programas de compartilhamento de arquivos do tipo peer-to-peer;

4.5.3.2.1.7.5. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

4.5.3.2.1.7.6. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;

4.5.3.2.1.7.7. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;

4.5.3.2.1.7.8. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino;

4.5.3.2.1.7.9. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

4.5.3.2.1.8. **Alta Disponibilidade**

4.5.3.2.1.8.1. Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Standby, com as implementações de Fail Over.

4.5.3.2.1.8.2. O Sincronismo dos servidores deve ser por interface exclusiva de Heartbeat;

4.5.3.2.1.8.3. No caso de falha do H.A. Ativo Primário, o H.A. Ativo secundário deve assumir de uma forma transparente sem impacto ao usuário ou perda de serviço;

4.5.3.2.1.8.4. Deverá suportar a persistências de sessão de usuarios e conexões estabelecidas, entre os membros da Alta Disponibilidade;

4.5.3.2.2. **Das Funcionalidades de Controle de Aplicação e Web Proxy**

4.5.3.2.2.1. **Controle de Aplicações**

4.5.3.2.2.1.1. As funcionalidades abaixo devem ser baseadas em appliance:

4.5.3.2.2.1.2. Deverá reconhecer no mínimo 4000 aplicações;

4.5.3.2.2.1.3. Deverá possuir, no mínimo, 19 categorias para classificação de aplicações;

4.5.3.2.2.1.4. Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações como:

a) P2P;
b) Web;
c) Transferência de arquivos;
d) Social;

4.5.3.2.2.1.5. Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;

4.5.3.2.2.1.6. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

4.5.3.2.2.1.7. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

4.5.3.2.2.1.8. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;

4.5.3.2.2.1.9. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;

4.5.3.2.2.1.10. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

4.5.3.2.2.1.11. Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino;

4.5.3.2.2.1.12. Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.

4.5.3.2.2.2. **Filtro de Conteúdo Web**

4.5.3.2.2.2.1. Possuir solução de filtro de conteúdo web integrado a solução de segurança

4.5.3.2.2.2.2. Possuir pelo menos 80 categorias para classificação de sites web

4.5.3.2.2.2.3. Possuir base mínima contendo, 48 milhões de sites internet web já registrados e classificados;

4.5.3.2.2.2.4. Possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites web como:

a) Webmail;
b) Instituições de Saúde;
c) Notícias;
d) Pornografia;
e) Restaurante;
f) Mídias Sociais;
g) Esporte;
h) Educação;
i) Games;
j) Compras;

4.5.3.2.2.2.5. Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

4.5.3.2.2.2.6. Possuir sistema de cache interno, armazenando requisições WEB em disco local e memória;

4.5.3.2.2.2.7. Deve permitir a definição do tamanho mínimo dos objetos salvos em cache no disco;

4.5.3.2.2.2.8. Deve permitir a definição do tamanho máximo dos objetos salvos em cache em memória;

4.5.3.2.2.2.9. Deve atender a estrutura de navegação através de hierarquia de proxy com e sem autenticação;

4.5.3.2.2.2.10. Possibilitar a integração com servidores de cache WEB externos;

4.5.3.2.2.2.11. Deve ser capaz de armazenar cache dinâmicos para as atualizações Microsoft Windows Update, Youtube, Sourceforge Downloads, Facebook, Google Maps;

4.5.3.2.2.2.12. Deve possuir a capacidade de excluir URL's específicas do cache web, configurável por listas de palavras chaves com suporte inclusive a expressões regulares;

4.5.3.2.2.2.13. Integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;

4.5.3.2.2.2.14. Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory, LDAP , TACACS+ e Radius;

4.5.3.2.2.2.15. Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança da contratante;

4.5.3.2.2.2.16. Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;

4.5.3.2.2.2.17. Deverá permitir o bloqueio de URLs inválidas cujo campo CN do certificado SSL não contém um domínio válido;

4.5.3.2.2.2.18. Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web;

4.5.3.2.2.2.19. Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;

4.5.3.2.2.2.20. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

4.5.3.2.2.2.21. Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem;

4.5.3.2.2.2.22. Possuir Logs e Relatórios de tempo de navegação de sites web - Domínios Web;

4.5.3.2.2.2.23. Possuir recurso capaz de controlar e restringir o acesso a sites com base em seus nomes de domínio, conhecido como DNS Content Filter;

4.5.3.2.2.3. **Recursos do Proxy**

4.5.3.2.2.3.1. Deverá funcionar em modo Proxy Explícito para HTTP, HTTPS, FTP, POP3 e SMTP e em Proxy Transparente;

4.5.3.2.2.3.2. A solução deve ser capaz de identificar o comportamento do protocolo SSH onde pode ser feito através da inspeção do protocolo;

4.5.3.2.2.3.3. Deverá permitir configurar a porta do Proxy Explícito;

4.5.3.2.2.3.4. O equipamento deverá poder suportar funcionalidades de antispam sem a necessidade de equipamento dedicado.

4.5.3.2.3. **Das Funcionalidades da Detecção de Intrusão e ATP**

4.5.3.2.3.1. **Das Funcionalidades da Detecção de Intrusão**

4.5.3.2.3.1.1. A Detecção de Intrusão deverá ser baseada em appliance:

4.5.3.2.3.1.2. Possuir no mínimo 82.000 (oitenta e duas mil) assinaturas ou regras de IPS/IDS;

4.5.3.2.3.1.3. Permitir a criação de assinaturas customizadas pelo administrador do NGFW;

4.5.3.2.3.1.4. O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;

4.5.3.2.3.1.5. Possuir tecnologia de detecção baseada em assinatura;

4.5.3.2.3.1.6. Deverá suportar a implantação em modo Gateway, inline e em modo sniffer;

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

4.5.3.2.3.1.8. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação.

4.5.3.2.3.1.9. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos.

4.5.3.2.3.1.10. Possuir opção para administrador as listas de Blacklist, Whitelist e Quarentena com suporte a endereços IPv6.

4.5.3.2.3.1.11. Possuir capacidade de remontagem de pacotes para identificação de ataques;

4.5.3.2.3.1.12. Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque; Exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de Servidores Web;

4.5.3.2.3.1.13. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;

4.5.3.2.3.1.14. Mecanismos de detecção/proteção de ataques;

4.5.3.2.3.1.15. Reconhecimento de padrões;

4.5.3.2.3.1.16. Análise de protocolos;

4.5.3.2.3.1.17. Detecção de anomalias;

4.5.3.2.3.1.18. Detecção de ataques de RPC (Remote procedure call);

4.5.3.2.3.1.19. Proteção contra-ataques de Windows ou NetBios;

4.5.3.2.3.1.20. Proteção contra-ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);

4.5.3.2.3.1.21. Proteção contra-ataques DNS (Domain Name System);

4.5.3.2.3.1.22. Proteção contra-ataques a FTP, SSH , Telnet e rlogin;

4.5.3.2.3.1.23. Proteção contra-ataques de ICMP (Internet Control Message Protocol);

4.5.3.2.3.1.24. Alarmes na console de administração;

4.5.3.2.3.1.25. Alertas via correio eletrônico;

4.5.3.2.3.1.26. Monitoração do comportamento do appliance através de SNMP, o dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;

4.5.3.2.3.1.27. Capacidade de resposta/logs ativa a ataques;

4.5.3.2.3.1.28. Terminação de sessões via TCP resets;

4.5.3.2.3.1.29. Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;

4.5.3.2.3.1.30. O Sistema de detecção de Intrusos deverá atenuar os efeitos dos ataques de negação de serviços;

4.5.3.2.3.1.31. Possuir filtros de ataques por anomalias;

4.5.3.2.3.1.32. Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;

4.5.3.2.3.1.33. Permitir filtros de anomalias de protocolos;

4.5.3.2.3.1.34. Suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;

4.5.3.2.3.1.35. Suportar verificação de ataque nas camadas de aplicação;

4.5.3.2.3.2. **Das Funcionalidades Do Threat Protection**

4.5.3.2.3.2.1. Possuir funções de Antivírus, Anti-spyware;

4.5.3.2.3.2.2. Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, SMTP, POP3, SMB/CIFS e FTP;

4.5.3.2.3.2.3. Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.)

4.5.3.2.3.2.4. Permitir o bloqueio de download de arquivos por extensão e tipo de arquivo;

4.5.3.2.4. Solução de Gerenciamento Centralizado de Firewall

4.5.3.2.4.1. Funcionalidades de Gerenciamento

4.5.3.2.4.1.1. Como boa prática de segurança e de mercado, a solução de gerência deverá ser separada do gateway de segurança, onde irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste projeto;

4.5.3.2.4.1.2. A solução de gerenciamento centralizado deve possibilitar o gerenciamento de todos os Firewall contratados.

4.5.3.2.4.1.3. A solução de gerenciamento centralizado deverá ser do mesmo fabricante da solução de segurança.

4.5.3.2.4.1.4. O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance físico deve ser compatível com rack 19 polegadas e possuir todos os acessórios necessários para sua instalação. Caso seja entregue em appliance virtual, deverá ser compatível com VMware ESXi e todo custo da infraestrutura necessária para suportar o appliance virtual é responsabilidade da CONTRATANTE;

4.5.3.2.4.1.5. Centralizar a administração de regras e políticas do(s) cluster(s), usando uma única interface de gerenciamento;

4.5.3.2.4.1.6. A solução deverá permitir seu gerenciamento por: CLI (Command Line Interface) via SSH, Web GUI utilizando protocolo HTTPS ou console gráfica;

4.5.3.2.4.1.7. Deve manter um canal de comunicação segura, com encriptação baseada em certificados, entre todos os componentes que fazem parte da solução de firewall, gerência, armazenamento de logs e emissão de relatórios;

4.5.3.2.4.1.8. A solução deve incluir a opção de segmentar a base de regra utilizando rótulos ou títulos de seção para organizar melhor a política facilitando a localização e gestão do administrador;

4.5.3.2.4.1.9. A solução de gerência deverá prover fácil administração na aplicação das políticas para os gateways, sendo capaz de realizar o processo de alteração de regras e configuração de todas as soluções de segurança, que pode ser aplicada nos gateways remotos em uma única sessão, evitando qualquer tipo de retrabalho.

4.5.3.2.4.1.10. Deve possibilitar a realização de "backup" e restauração de dados.

4.5.3.2.4.1.11. Deve possibilitar a gerência de "logs", realizando as configurações de relatórios de todos os "firewalls" integrados.

4.5.3.2.4.1.12. Deve permitir buscas e realizar análise de usuários e grupos, rastreando toda a sua atividade e uso da internet.

4.5.3.2.4.1.13. O gerenciamento deve permitir/possuir:

4.5.3.2.4.1.14. Criação e administração de políticas de Firewall, Controle de aplicação e IPS, Antivírus e Anti-Malware, Filtro de URL e prevenção contra ameaças avançadas;

4.5.3.2.4.1.15. Monitoração de logs;

4.5.3.2.4.1.16. Debugging;

4.5.3.2.4.1.17. Deve permitir usar palavras chaves para facilitar identificação de regras;

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

4.5.3.2.4.1.19. Autenticação integrada à base de dados local;

4.5.3.2.4.1.20. Deve possuir ferramenta para localização de objetos (por exemplo: endereço IP, Range de IP, subrede) na base de regras;

4.5.3.2.4.1.21. Criação de regras que fiquem ativas em horário definido;

4.5.3.2.4.1.22. Habilidade de upgrade via interface de gerenciamento;

4.5.3.2.4.1.23. Deverá ter a capacidade de gerar um relatório gráfico, que permita visualizar as mudanças na utilização de aplicações na rede, no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações, no tempo presente com relação ao passado;

4.5.3.2.4.1.24. Controle sobre todos os equipamentos da plataforma de proteção em uma única console, com administração de privilégios e funções;

4.5.3.2.4.1.25. Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de proteção;

4.5.3.2.4.1.26. Deve permitir a criação de objetos e políticas compartilhadas;

4.5.3.2.4.1.27. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

4.5.3.2.4.1.28. Solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

4.5.3.2.4.1.29. A solução deve permitir gerenciar templates de customização visual e marca do produto pelo sistema de gerenciamento centralizado e permitir aplicar nos NGFW´s gerenciados. Portanto, deve ser possível customizar a interface gráfica nos seguintes itens:

a) Título da Página;
b) Ícone (favicon);
c) Logotipo;
d) Imagem de fundo;
e) Cores do menu (primária e secundária);

4.5.3.2.4.1.30. O sistema deve ser capaz de gerenciar de modo central as políticas de backup do equipamento remotos;

4.5.3.2.4.1.31. O sistema deve permitir habilitar uma mensagem de Disclaimer na página de login da Interface de Administração. Ou seja, a página de login deverá apresentar um banner com uma mensagem customizada pelo administrador. Essa mensagem poderá ser utilizada para avisos de políticas de uso e compliance do sistema.

4.5.3.2.4.1.32. Deve suportar sistema de cluster do tipo Alta Disponibilidade para a solução ofertada;

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

4.5.3.2.4.1.34. Deve permitir inserir uma notificação do tipo "Login Disclaimer" que deve ser exibida na página de login da Interface de Administração da solução de gerenciamento centralizado.

4.5.3.2.4.1.35. Suportar API para integração com sistemas de terceiros;

4.5.3.2.4.2. **Alta Disponibilidade**

4.5.3.2.4.2.1. Deve suportar recurso de Alta-Disponibilidade (HA), sendo um primário e outros em modo secundário com sincronização e replicação das configurações;

4.5.3.2.4.2.2. O sistema de cluster deve suportar utilizar 02 (duas) interfaces como heatbeat;

4.5.3.2.4.2.3. Deve suportar definir o intervalo do sincronismo em minutos;

4.5.3.2.4.2.4. Permitir definir o número máximo de falhas dos testes do heartbeat e a solução somente irá convergir para o segundo equipamento após atingir o valor definido;

4.5.3.2.4.2.5. Suportar inserir um endereço de email para receber notificações relacionadas ao cluster.

4.5.3.2.4.3. **Armazenamento e Gerenciamento de Logs e Eventos**

4.5.3.2.4.3.1. A solução de armazenamento e gerenciamento de logs e eventos, deverá suportar, no mínimo, e estar licenciada para receber no mínimo 50GB de logs por dia;

4.5.3.2.4.3.2. A solução de armazenamento e gerenciamento de logs e eventos poderá ser entrega na mesma solução de gerenciamento centralizado, desde que atenda aos requisitos solicitados.

4.5.3.2.4.3.3. A solução de armazenamento e gerenciamento de logs e eventos deverá ser do mesmo fabricante da solução de segurança e compatível com a ferramenta de gerenciamento centralizado.

4.5.3.2.4.3.4. Deverá prover análise de tráfego de rede de modo centralizado;

4.5.3.2.4.3.5. Deve possuir análise de tráfego de rede e ameaças por geolocalização;

4.5.3.2.4.3.6. Deverá ser capaz de receber os logs e eventos com o objetivo de prover os seguintes tipos de análises:

4.5.3.2.4.3.7. Análise de ameaças e incidentes de segurança;

4.5.3.2.4.3.8. Análise de tráfego e uso de categorias Web;

4.5.3.2.4.3.9. Análise de tráfego e uso de aplicativos;

4.5.3.2.4.3.10. Análise de tráfego e ameaças por usuário;

4.5.3.2.4.3.11. Análise de desempenho de políticas de segurança;

4.5.3.2.4.3.12. A solução ofertada deve ser capaz de fazer o gerenciamento centralizado de logs, consolidação de logs, arquivamento de logs, busca avançada de logs;

4.5.3.2.4.3.13. Deverá possuir ferramenta para salvar consultas avançadas;

4.5.3.2.4.3.14. Deve possuir relatórios personalizados;

4.5.3.2.4.3.15. Deverá ser capaz de efetuar o arquivamento de relatórios;

4.5.3.2.4.3.16. Deve possuir agendamento de relatórios;

4.5.3.2.4.3.17. Os Relatórios deverão, no mínimo, serem exportados em formatos flexíveis (PDF, CSV);

4.5.3.2.4.3.18. Logs e Relatórios de tempo de navegação de sites web - Domínios Web;

4.5.3.2.4.3.19. Permitir o envio de relatórios por e-mail;

4.5.3.2.4.3.20. Relatório por Dispositivo/Consolidado;

4.5.3.2.5. **Tabela de Distribuição do Item 1, do Lote Único**

SUBITEM DO TR Nº	DESCRIÇÃO	QTDE
4.5.3.1.1	APPLIANCE NGFW DE 5 GBPS DE CAPACIDADE DE FIREWALL	157
4.5.3.1.2	APPLIANCE NGFW DE 9.7 GBPS DE CAPACIDADE DE FIREWALL	11
4.5.3.1.3	APPLIANCE NGFW DE 11.8 GBPS DE CAPACIDADE DE FIREWALL	3
4.5.3.1.4	APPLIANCE NGFW DE 19.4 GBPS DE CAPACIDADE DE FIREWALL	2
4.5.3.2.4	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE FIREWALL	1

4.5.3.3. **A solução de segurança cibernética de bloqueio de ameaças, conforme ITEM 2, do Lote Único, deve possuir as seguintes características:**

4.5.3.3.1. **Interface e Gestão:**

4.5.3.3.1.1. Deve ser instalado em equipamento com S.O. Linux, Unix ou BSD.

4.5.3.3.1.2. Deve ter uma interface amigável para configuração e gestão.

4.5.3.3.1.3. Não deve possuir endereçamento IP nas interfaces pelas quais passam o tráfego internet.

4.5.3.3.1.4. Não deve permitir a identificação da existência da solução.

4.5.3.3.1.5. Não ser suscetível à exploração externa de possíveis vulnerabilidades no software.

4.5.3.3.1.6. Deve permitir instalação de forma transparente, sem necessidade de alterações nas configurações lógicas de rede, IP ou do roteamento do ambiente atual.

4.5.3.3.1.7. Deve atuar diretamente no tráfego de entrada da internet.

4.5.3.3.1.8. Deve proporcionar proteção abrangente para toda a infraestrutura, desde o firewall podendo incluir os roteadores à internet.

4.5.3.3.1.9. O aumento de latência no tráfego de rede não deve ser superior a 5 milésimos de segundo.

4.5.3.3.1.10. Deve permitir comunicação com a internet através de proxy.

4.5.3.3.1.11. Deve possuir painel para configuração de mecanismo para detecção de acesso indesejado.

4.5.3.3.1.12. Deve possuir painel para configuração de origens confiáveis.

4.5.3.3.1.13. Deve possuir mecanismo de autoproteção.

4.5.3.3.1.14. Deve possuir log de auditoria de tudo que foi feito na solução, devendo no mínimo identificar user, data-hora e atividade realizada.

4.5.3.3.1.15. Deve armazenar no mínimo os últimos 8.000 registros de log de auditoria.

4.5.3.3.2. **Inteligência Artificial Avançada:**

4.5.3.3.2.1. Deve ser uma solução baseada em Inteligência Artificial Preditiva.

4.5.3.3.2.2. Deve ser capaz de analisar padrões de comportamento no tráfego de internet.

4.5.3.3.2.3. Deve identificar origens maliciosas e neutralizá-las imediatamente e automaticamente, sem intervenção humana.

4.5.3.3.2.4. A solução não deve depender de assinaturas para reconhecer tráfegos indesejados.

4.5.3.3.2.5. Deve criar uma blacklist local com as origens maliciosas.

4.5.3.3.2.6. Deve possuir mecanismo de gestão do tempo de guarda dos dados da blacklist.

4.5.3.3.2.7. Deve possuir capacidade de aprendizado de acessos indesejados.

4.5.3.3.3. **Taxa de Falso Positivo:**

4.5.3.3.3.1. Deve apresentar uma taxa de falso positivo inferior a 0,0001% (uma identificação errada a cada um milhão de identificações), garantindo precisão nas identificações e bloqueios.

4.5.3.3.4. **Proteção Contra Ataques de "Zero Day":**

4.5.3.3.4.1. Deve oferecer proteção eficaz contra ataques de "Zero Day", mesmo aqueles que ainda não tenham sido identificados e que ainda não possuam "assinatura de identificação" ou "patch de correção" dos fabricantes das outras soluções informáticas que o órgão disponibiliza na internet.

4.5.3.3.5. **Visibilidade:**

4.5.3.3.5.1. Deve fornecer visibilidade das origens maliciosas dos ataques.

4.5.3.3.5.2. Deve fornecer visibilidade das tentativas de acessos bloqueadas.

4.5.3.3.5.3. Deve fornecer visibilidade dos serviços de rede alvos de ataques.

4.5.3.3.5.4. Deve possuir funcionalidade que permita identificar de forma fácil e ágil o motivo do bloqueio do ataque.

4.5.3.3.5.5. Deve apresentar um dashboard para a equipe de monitoramento (SOC) com mapa dos países dos IPS atacantes.

4.5.3.3.5.6. Deve apresentar um dashboard para a equipe de monitoramento (SOC) com mapa dos países de onde foram gerados os ataques.

4.5.3.3.5.7. Deve permitir a consulta através de vários tipos de indicadores como por exemplo, IP de origem, IP de Destino, Porta de origem, Porta de destino entre outros.

4.5.3.3.5.8. Deve possuir funcionalidade de geolocalização de IP identificado como malicioso.

4.5.3.3.5.9. Deve possuir busca de CVEs na base do MITRE.

4.5.3.3.5.10. Deve possuir mecanismo de autogestão do armazenamento dos logs de ataque.

4.5.3.3.6. **Relatórios e Integrações:**

4.5.3.3.6.1. Deve permitir integração, através de API, com outros equipamentos/soluções de segurança como por exemplo firewall ou soluções de observabilidade.

4.5.3.3.6.2. Deve permitir envio dos logs de ataques para servidor externo.

4.5.3.3.6.3. Deve possuir integração com rede externa de Inteligência de Ameaças Global, com capacidade de aprendizado sobre novas ameaças identificadas exercendo atividade hacker recente pelo mundo e, de forma automática e pró-ativa, ativar proteção contra essas origens.

4.5.3.3.6.4. Deve gerar relatório gerencial mensal com pelo menos as seguintes informações: quantidade de ataques, bloqueios, origens mais frequentes, países de origem e serviços mais atacados.

4.5.3.3.6.5. Deve possuir capacidade suficiente para armazenar e disponibilizar consultas aos relatórios gerenciais mensais de pelo menos 5 anos.

4.5.3.3.6.6. Deve permitir exportar os relatórios para PDF.

4.5.3.3.7. **Especificações Técnicas do Equipamento**

4.5.3.3.7.1. **O equipamento físico deve atender aos seguintes requisitos:**

4.5.3.3.7.1.1. **Dimensões e Montagem:**

4.5.3.3.7.1.1.1. Deve ser compatível com rack de 19 polegadas, com tamanho de 1U ou 2U.

4.5.3.3.7.1.2. **Conectividade:**

4.5.3.3.7.1.2.1. Deve possuir no mínimo 8 interfaces de rede Gigabit Ethernet com conexão do tipo RJ45.

4.5.3.3.7.1.2.2. Deve ter porta console para configuração local.

4.5.3.3.7.1.2.3. Deve possuir interface de rede exclusiva para acesso e gerenciamento interno do equipamento.

4.5.3.3.7.1.3. **Alimentação elétrica:**

4.5.3.3.7.1.3.1. Deve ter fonte de alimentação elétrica VAC automática nos padrões brasileiros conforme a continuidade operacional.

4.5.3.4. **Os serviços e equipamentos do ITEM 3, do Lote Único, deverão ser entregues no formato e características técnicas bem como funcionalidades conforme especificações abaixo:**

4.5.3.4.1. O serviço de acesso à Internet compreenderá a instalação, operação, manutenção e gerenciamento da infraestrutura de acesso à Internet através de roteador PE, integrado imediatamente ao roteamento BGP da Operadora. Entende-se operadora, Provedor de Internet Autônomo, ou seja, que possua ASN (Autonomous System Number) vinculado a um CNPJ de um ISP distinto, ou seja, a CONTRATADA deverá suportar a operação através de dois link dedicado distintos, oriundo de 02(dois) ASN diferentes, através de infraestrutura de chegada ao prédio da Prefeitura percorrida por caminhos diferentes, visando a eventual queda de um dos link não haver impacto na operação como um todo.

4.5.3.4.2. Cada link deverá ser entregue com blocos IPV4 /29 e IPV6 /64, públicos, os quais serão cadastrados no portal numeração.br, compreendendo inicialmente banda de 500 Mbps mas a porta de rede não pode haver limite rate, devendo suportar os serviço em wire speed, pois eventual queda de um dos link, a operadora redundante deverá suportar o tráfego na integralidade.

4.5.3.4.3. Conforme topologia da rede, a CONTRATADA deverá entregar o link em duas portas distintas, uma porta conectada no equipamento de cibersegurança A e outra porta a ser conectada no equipamento de cibersegurança B. Tal feito se repetirá em cada ASN, conforme topologia apresentada.

4.5.3.4.4. Em caso de falha no equipamento A, o serviço deverá realizar a migração automática para o equipamento redundante em regime de failover, sem necessidade de configurações adicionais ou intervenções técnicas. O mesmo procedimento deverá ocorrer em situação inversa. Caso este Termo de Referência não detalhe alguma instrução específica, caberá à CONTRATADA assegurar a entrega da solução em pleno funcionamento, incluindo todos os custos inerentes à implantação, sem qualquer cobrança adicional.

4.5.3.4.5. A CONTRATADA deverá fornecer todos os equipamentos, acessórios e demais componentes indispensáveis à disponibilização do serviço no local designado, ainda que não estejam expressamente mencionados neste Termo de Referência, desde que sejam essenciais à operação da solução ou ao cumprimento das funcionalidades e configurações exigidas, sem gerar ônus adicionais à CONTRATANTE.

4.5.3.4.6. O acesso entre a operadora e o ambiente de TI da CONTRATANTE deverá ser feito exclusivamente por meio de fibra óptica da CONTRATADA.

4.5.3.4.7. Devem transportar pacotes IPv4 e IPv6 com no mínimo 1500 bytes sem exigir a fragmentação dos mesmos na camada 3 do modelo OSI.

4.5.3.4.8. Os links devem suportar IPv6, sendo necessário o fornecimento de endereçamento para as redes internas do CONTRATANTE.

4.5.3.4.9. Deverão ser fornecidos 1 (roteador) por link dedicado que irá compor o ambiente de alta disponibilidade.

4.5.3.4.10. Deverá suportar todos os protocolos de roteamento necessários para suportar as conexões WANs em ambiente de alta disponibilidade (OSPF, BGP, RIP etc).

4.5.3.4.11. Cada equipamento deve possuir no mínimo 2 (duas) interfaces WAN de 1 Gbps e 2 (duas) ou mais interfaces LAN de 1 Gbps.

4.5.3.4.12. Possuir LEDs de diagnóstico sobre alimentação, atividade e diagnóstico das portas.

4.5.3.4.13. Deve possuir funcionalidades necessárias para monitoramento, diagnóstico e features como QoS, permitir a atualização remota do SO e arquivos de configuração via ethernet ou serial, FTP e TFTP; Permitir a gravação de log externo via syslog; Suportar o recurso port mirroring para um endereço IP; e suportar protocolo de coleta de tráfego Netflow ou IPFIX para a realização de coleta de informações de fluxo, tráfego que circulam no equipamento.

4.5.3.5. **Os serviços e equipamentos dos ITENS 4 e 5 deverão ser entregues no formato e características técnicas bem como funcionalidades conforme especificações abaixo:**

4.5.3.5.1. As velocidades de acesso à internet contratadas serão classificadas da seguinte maneira:

4.5.3.5.1.1. Link principal (item 4, do Lote Único): 150Mbps

4.5.3.5.1.2. Link redundante (item 5, do Lote Único): 75Mbps

4.5.3.5.1.2.1. A CONTRATADA deverá comprovar que possui capacidade de operar com dois circuitos distintos, em fibra óptica.

4.5.3.5.1.2.2. A CONTRATADA deverá comprovar que possui capacidade operacional através de redes espectrais.

4.5.3.5.2. A CONTRATADA deverá garantir largura de banda simétrica (download/upload) de 100% da velocidade contratada, em link único para o link principal (Item 4, do Lote Único), não sendo aceita a agregação de múltiplos links para atingir a velocidade contratada.

4.5.3.5.3. A CONTRATADA deverá garantir largura de banda simétrica (download/upload) de pelo menos 70% da velocidade contratada, podendo ser em 02(dois) link (Item 4, do

Lote Único), um link performando em fibra óptica e outro através de chip especial para suportar esta operação estruturante, não sendo possível chip de dados convencionais, com limite de dados. Neste caso específico será aceito a agregação desses 2 link em comento, para atingir a velocidade contratada.

4.5.3.5.4. A localização e classificação de cada unidade está relacionada nos itens 7.2.1.3.1, 7.2.1.3.2 e 7.2.1.3.3.

4.5.3.5.5. O acesso de fibra óptica até o ambiente de TI da CONTRATANTE deverá ser feito exclusivamente por meio de fibra óptica da CONTRATADA, exceto chip 4/5Gbps.

4.5.3.5.6. Cada acesso de fibra óptica ao ambiente de TI deve ser percorrido por caminhos distintos; não serão aceitos acessos de redes convergindo para um mesmo ISP, sendo necessária a validação de comprovação deste quesito no momento do certame.

4.5.3.6. **Requisitos Tecnológicos Mínimos Para Suportar a Conectividade das Praças**

4.5.3.6.1. **Ponto de Acesso Outdoor Wi-Fi 6 2x2**

4.5.3.6.1.1. **Conectividade:**

4.5.3.6.1.1.1. Deve possuir, no mínimo, 1 porta uplink ethernet 100/1000/2.5G Base-T em conector RJ45 com suporte a alimentação PoE compatível com o padrão IEEE 802.3at e com reconhecimento automático de crossover MDI/MDIX;

4.5.3.6.1.1.2. Deve possuir 1 porta LAN ethernet 100/1000Base-T em conector RJ45 e com reconhecimento automático de crossover MDI/MDIX;

4.5.3.6.1.1.3. Possuir porta de console para gerenciamento e configuração via linha de comando (CLI – command line interface) com conector RJ-45 diferente da porta de rede solicitada anteriormente;

4.5.3.6.1.1.4. Deve possuir 2 rádios operando nas frequências de 2,4GHz e 5GHz simultaneamente;

4.5.3.6.1.1.5. Deve possuir rádio Bluetooth Low-Energy (BLE) integrado ao equipamento;

4.5.3.6.1.1.6. Deve possuir antenas omnidirecionais internas ao equipamento com ganho mínimo de 5 dBi na frequência de 2,4GHz, 6 dBi na frequência de 5GHz;

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

4.5.3.6.1.1.8. Deve possuir LEDs indicadores de conectividade;

4.5.3.6.1.2. **Funcionalidades WLAN Deve Atender aos Seguintes Padrões:**

4.5.3.6.1.2.1. IEEE 802.11a/b/g/n/ac/ax;

4.5.3.6.1.2.2. Dupla banda 2,4 e 5GHz simultâneas;

4.5.3.6.1.2.3. Deve operar em MIMO 2x2 com suporte a 2 spatial streams e suporte a MU-MIMO;

4.5.3.6.1.2.4. Deve suportar as seguintes taxas de dados:

- a) IEEE 802.11b: 1, 2, 5.5, 11 Mbps;
- b) IEEE 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps;
- c) IEEE 802.11n: 6.5 – 300 Mbps (20 / 40 MHz);
- d) IEEE 802.11ac: 6.5 – 866 Mbps (20 / 40 / 80 MHz);
- e) IEEE 802.11ax: 3.6 - 574 Mbps (2.4GHz, 20 / 40 MHZ)
- f) IEEE 802.11ax: 3.6 - 2400 Mbps (5GHz, 20 / 40 / 80 / 160MHz)

4.5.3.6.1.2.5. Deve oferecer potência mínima de transmissão RF de 26dBm em 2,4GHz e 25dBm em 5GHz;

4.5.3.6.1.2.6. Deve suportar no mínimo 16 SSIDs simultaneamente por rádio totalizando até 32 SSIDs no sistema;

4.5.3.6.1.2.7. Deve suportar a configuração de no mínimo 16 VLANs ativas simultaneamente por rádio totalizando até 32 VLANs ativas simultaneamente no sistema;

4.5.3.6.1.2.8. O equipamento proposto deverá poder operar nos seguintes modos:

- a) Access Point;
- b) Wireless Mesh;

4.5.3.6.1.2.9. Deverá permitir o controle de tráfego para cada SSID;

4.5.3.6.1.2.10. Deverá selecionar dinamicamente os canais de operação;

4.5.3.6.1.2.11. Deverá selecionar automaticamente a melhor opção de conexão dos clientes (Band Steering);

4.5.3.6.1.3. **Gerenciamento**

4.5.3.6.1.3.1. Deve suportar gerenciamento SNMP v2c;

4.5.3.6.1.3.2. Deve permitir configuração dos parâmetros IP através de serviço DHCP Cliente;

4.5.3.6.1.3.3. Deve permitir acesso remoto a console via HTTP e HTTPS;

4.5.3.6.1.3.4. Deve permitir a atualização de firmware via TFTP ou HTTP;

4.5.3.6.1.3.5. Deve suportar sincronização de relógio através de SNTP ou NTP;

4.5.3.6.1.3.6. Deve suportar atualização automática do firmware quando estiver operando em modo gerenciado;

4.5.3.6.1.3.7. Deve suportar plataforma em nuvem que permite o gerenciamento de pontos de acesso de diferentes fabricantes;

4.5.3.6.1.4. **Segurança**

4.5.3.6.1.4.1. Deve suportar autenticação através de servidor RADIUS;

4.5.3.6.1.4.2. Deve suportar WiFi Protected Access (WPA/WPA2);

4.5.3.6.1.4.3. Deve suportar WPA/WPA2 (PSK);

4.5.3.6.1.4.4. Deve suportar WPA3;

4.5.3.6.1.4.5. Deve permitir bloqueio da divulgação do SSID;

4.5.3.6.1.5. **Gerais**

4.5.3.6.1.5.1. Deve suportar fonte de alimentação DC externa operando em tensões de 100 a 240 V e em frequências de 50 a 60 Hz automaticamente;

4.5.3.6.1.5.2. Deve possuir a classificação IP68 de resistência a intempéries;

4.5.3.6.1.5.3. Deve permitir montagem em parede ou poste;

4.5.3.6.1.5.4. Deve suportar temperatura de operação entre - 40°C a 60°C;

4.5.3.6.1.5.5. Deve suportar sistema operacional em conformidade com o OpenWiFi da Telecom Infra Project;

4.5.3.6.1.5.6. Deverá suportar o padrão OpenRoaming para garantir a facilidade e segurança de conexão dos clientes à rede sem fio, permitindo a ampla utilização da rede pelos usuários finais;

4.5.3.6.1.5.7. A controladora deve permitir que o access point seja controlado simultaneamente com access points de diferentes fabricantes

4.5.3.6.1.5.8. A empresa fornecedora da solução deverá apresentar uma prova de conceito (PoC) comprovando o funcionamento da controladora gerenciando no mínimo 2 access points de fabricantes diferentes

4.5.3.6.1.5.9. A empresa fornecedora deverá possuir atestado de capacidade de implementação de solução equivalente com ecossistema OpenWiFi

4.5.3.6.2. **Ponto de Acesso Indoor Wi-Fi 6 2x2**

4.5.3.6.2.1. **Conectividade**

4.5.3.6.2.1.1. Deve possuir, no mínimo, 1 porta uplink ethernet 100/1000/2.5G Base-T em conector RJ45 com suporte a alimentação PoE compatível com o padrão IEEE 802.3at e com reconhecimento automático de crossover MDI/MDIX;

4.5.3.6.2.1.2. Deve possuir 1 porta LAN ethernet 100/1000Base-T em conector RJ45 e com reconhecimento automático de crossover MDI/MDIX;

4.5.3.6.2.1.3. Possuir porta de console para gerenciamento e configuração via linha de comando (CLI – command line interface) com conector RJ-45 diferente da porta de rede solicitada anteriormente;

4.5.3.6.2.1.4. Deve possuir 1 porta USB;

4.5.3.6.2.1.5. Deve possuir 2 rádios operando nas frequências de 2,4GHz e 5GHz simultáneamente;

4.5.3.6.2.1.6. Deve possuir rádio Bluetooth Low-Energy (BLE) integrado ao equipamento;

4.5.3.6.2.1.7. Deve possuir antenas omnidirecionais internas ao equipamento com ganho mínimo de 4 dBi na frequência de 2,4GHz, 6 dBi na frequência de 5GHz e 4 dBi para BLE;

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

4.5.3.6.2.1.9. Deve possuir LEDs indicadores de conectividade WLAN e Power/Diag;

4.5.3.6.2.2. **Funcionalidades WLAN Deve Atender aos Seguintes Padrões:**

4.5.3.6.2.2.1. IEEE 802.11a/b/g/n/ac/ax;

4.5.3.6.2.2.2. Dupla banda 2,4 e 5GHz simultâneas;

4.5.3.6.2.2.3. Deve operar em MIMO 2x2 com suporte a 2 spatial streams e suporte a MU-MIMO;

4.5.3.6.2.2.4. Deve suportar as seguintes taxas de dados:

a) IEEE 802.11b: 1, 2, 5.5, 11 Mbps;
b) IEEE 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps;
c) IEEE 802.11n: 6.5 – 300 Mbps (20 / 40 MHz);
d) IEEE 802.11ac: 6.5 – 866 Mbps (20 / 40 / 80 MHz);
e) IEEE 802.11ax: 3.6 - 574 Mbps (2.4GHz, 20 / 40 MHz)
f) IEEE 802.11ax: 3.6 - 1200 Mbps (5GHz, 20 / 40 / 80 MHz)

4.5.3.6.2.2.5. Deve oferecer potência mínima de transmissão RF de 23dBm em 2,4GHz e 23dBm em 5GHz;

4.5.3.6.2.2.6. Deve suportar Wi-Fi Multimedia (WMM);

4.5.3.6.2.2.7. Deve suportar no mínimo 16 SSIDs simultaneamente por rádio totalizando até 32 SSIDs no sistema;

4.5.3.6.2.2.8. Deve suportar a configuração de no mínimo 16 VLANs ativas simultaneamente por rádio totalizando até 32 VLANs ativas simultaneamente no sistema;

4.5.3.6.2.2.9. O equipamento proposto deverá poder operar nos seguintes modos:

a) Access Point;
b) Wireless Mesh;

4.5.3.6.2.2.10. Deverá permitir o controle de tráfego para cada SSID;

4.5.3.6.2.2.11. Deverá selecionar dinamicamente os canais de operação;

4.5.3.6.2.2.12. Deverá selecionar automaticamente a melhor opção de conexão dos clientes (Band Steering);

4.5.3.6.2.3. **Gerenciamento**

4.5.3.6.2.3.1. Deve suportar gerenciamento SNMP v2c;

4.5.3.6.2.3.2. Deve permitir configuração dos parâmetros IP através de serviço DHCP Cliente;

4.5.3.6.2.3.3. Deve permitir acesso remoto a console via HTTP e HTTPs;

4.5.3.6.2.3.4. Deve permitir a atualização de firmware via TFTP ou HTTP;

4.5.3.6.2.3.5. Deve suportar sincronização de relógio através de SNTP ou NTP;

4.5.3.6.2.3.6. Deve suportar atualização automática do firmware quando estiver operando em modo gerenciado;

4.5.3.6.2.3.7. Deve suportar plataforma em nuvem que permite o gerenciamento de pontos de acesso de diferentes fabricantes;

4.5.3.6.2.4. **Segurança**

4.5.3.6.2.4.1. Deve suportar autenticação através de servidor RADIUS;

4.5.3.6.2.4.2. Deve suportar WiFi Protected Access (WPA/WPA2);

4.5.3.6.2.4.3. Deve suportar WPA/WPA2 (PSK);

4.5.3.6.2.4.4. Deve suportar WPA3;

4.5.3.6.2.4.5. Deve permitir bloqueio da divulgação do SSID;

4.5.3.6.2.4.6. Desempenho

4.5.3.6.2.4.7. Deve possibilitar a conexão de até 250 clientes concorrentes por rádio totalizando 500 simultaneamente;

4.5.3.6.2.5. **Gerais**

4.5.3.6.2.5.1. Deve suportar fonte de alimentação DC externa operando em tensões de 100 a 240 V e em frequências de 50 a 60 Hz automaticamente;

4.5.3.6.2.5.2. Deve permitir montagem em parede ou teto e vir acompanhado dos devidos kits de instalação;

4.5.3.6.2.5.3. Deve permitir a instalação de trava tipo Kensington;

4.5.3.6.2.5.4. Deve suportar temperatura de operação entre 0°C a 50°C;

4.5.3.6.2.5.5. Possuir certificado válido de homologação emitido pela Anatel.

4.5.3.6.2.5.6. Deverá ser apresentado certificado válido de interoperabilidade fornecido pela Wi-Fi Alliance na categoria de Enterprise Access Point;

4.5.3.6.2.5.7. Deve suportar sistema operacional em conformidade com o OpenWiFi da Telecom Infra Project;

4.5.3.6.2.5.8. Deverá suportar o padrão OpenRoaming para garantir a facilidade e segurança de conexão dos clientes à rede sem fio, permitindo a ampla utilização da rede pelos usuários finais;

4.5.3.6.2.5.9. A controladora deve permitir que o access point seja controlado simultaneamente com access points de diferentes fabricantes

4.5.3.6.2.5.10. A empresa fornecedora da solução deverá apresentar uma prova de conceito (PoC) comprovando o funcionamento da controladora gerenciando no mínimo 2 access points de fabricantes diferentes

4.5.3.6.2.5.11. A empresa fornecedora deverá possuir atestado de capacidade de implementação de solução equivalente com ecossistema OpenWiFi

4.5.3.6.3. **Switch de Acesso POE 8 Portas 2.5base-T e 2 Portas 10G SFP+**

4.5.3.6.3.1. **Conectividade**

4.5.3.6.3.1.1. Deve possuir 8 portas padrão 2.5G/1000 Base-T em conector RJ45 compatível com o padrão IEEE 802.3az de eficiência energética;

4.5.3.6.3.1.2. Deve possuir no mínimo 2 portas 10G Base-X padrão SFP+ para a instalação de módulos padrão SFP+ ou cabos DAC;

4.5.3.6.3.1.3. As portas Base-T deverão suportar autonegociação de velocidade, modo de operação e detecção MDI-MDIX;

4.5.3.6.3.1.4. Deve possuir porta console serial padrão RS-232 em conector DB-9 ou RJ45 acompanhado do respectivo cabo para conexão ao PC;

4.5.3.6.3.2. **PoE**

4.5.3.6.3.2.1. Deve suportar alimentação PoE conforme o padrão IEEE 802.3af/802.3at nas 8 portas RJ45 dentro da disponibilidade de potência destinada a esse fim;

4.5.3.6.3.2.2. Deve suportar alimentação PoE++ conforme o padrão IEEE 802.3bt em, no mínimo, 4 portas RJ45 de forma simultânea;

4.5.3.6.3.2.3. Deve possibilitar visualização da alimentação através de LED exclusivo ou de múltipla funcionalidade;

4.5.3.6.3.2.4. Deve disponibilizar no mínimo 240W para utilização exclusiva no PoE sem utilização de fonte adicional para esse fim;

4.5.3.6.3.3. **Controle**

4.5.3.6.3.3.1. Deve suportar Jumbo Frames de 12K;

4.5.3.6.3.3.2. Deve suportar até 4K VLANs segundo o protocolo IEEE 802.1Q, por porta e por protocolo;

4.5.3.6.3.3.3. Deve suportar implementação de VLANs Privativas;

4.5.3.6.3.3.4. Deve suportar implementação de Voice VLANs;

4.5.3.6.3.3.5. Deve implementar suporte a QinQ;

4.5.3.6.3.3.6. Possuir no mínimo oito filas em hardware para priorização de tráfego por porta;

4.5.3.6.3.3.7. Implementar QoS com base no protocolo 802.1p e DSCP;

4.5.3.6.3.3.8. Deve implementar controle de fluxo com o protocolo 802.3X e Back Pressure;

4.5.3.6.3.3.9. Deve implementar IGMP Snooping v1, v2 e v3;

4.5.3.6.3.3.10. Deve implementar IGMP Filtering, Immediate Leave e Querier;

4.5.3.6.3.3.11. Deve implementar MLD Snooping;

4.5.3.6.3.3.12. Deve possibilitar a limitação de Broadcast, Multicast e Unicast;

4.5.3.6.3.3.13. Deve implementar o gerenciamento de banda com valores distintos para entrada e saída;

4.5.3.6.3.3.14. Deve implementar os mecanismos de controle de fila: SP (Strict Priority) e WRR (Weighted Round Robin);

4.5.3.6.3.4. **Disponibilidade**

4.5.3.6.3.4.1. Implementar o protocolo Spanning Tree (802.1D);

4.5.3.6.3.4.2. Implementar o protocolo Rapid Spanning Tree (802.1w);

4.5.3.6.3.4.3. Deve implementar o protocolo Multiple Spanning Tree (802.1s);

4.5.3.6.3.4.4. Deve suportar detecção de laço (loopback detection);

4.5.3.6.3.4.5. Deve implementar BPDU Guard/Filter e ROOT Guard;

4.5.3.6.3.4.6. Deve suportar até 8 grupos de agregação dinâmicos no padrão LACP ou estático de até 8 portas GbE;

4.5.3.6.3.5. **Gerenciamento**

4.5.3.6.3.5.1. Deve possuir suporte a pilha dupla de protocolo IPv4/IPv6;

4.5.3.6.3.5.2. Deve suportar gerenciamento SNMP v1, v2c e v3;

4.5.3.6.3.5.3. Deve permitir configuração dos parâmetros IP através de serviço DHCP Cliente;

4.5.3.6.3.5.4. Deve permitir acesso remoto a console via Telnet, SSHv2, HTTP e HTTPs;

4.5.3.6.3.5.5. Deve permitir configuração através de plataforma de gerenciamento em nuvem com suporte a OpenLan Switching (OLS) e OpenWiFi em conformidade com as especificações da Telecom Infra Project (TIP);

4.5.3.6.3.5.6. Deve permitir acesso local a console CLI;

4.5.3.6.3.5.7. Deve permitir atualização e provisionamento automáticos, podendo este ser executado por sistema de gestão externo, sendo, neste caso, necessário proporcionar a solução completa;

4.5.3.6.3.5.8. Deve suportar os grupos 1, 2, 3 e 9 de RMON;

4.5.3.6.3.5.9. Deve suportar o protocolo LLDP (IEEE 802.1ab);

4.5.3.6.3.5.10. Deve permitir armazenar no mínimo duas imagens de firmware em memória flash interna;

4.5.3.6.3.5.11. Deve permitir a atualização de firmware via HTTP, TFTP ou FTP em memória tipo flash;

4.5.3.6.3.5.12. Deve permitir armazenar no mínimo duas configurações distintas em memória flash interna;

4.5.3.6.3.5.13. Deve permitir salvar as configurações em um computador local (backup) via HTTP, TFTP ou FTP;

4.5.3.6.3.5.14. Deve suportar espelhamento de tráfego;

4.5.3.6.3.5.15. Deve suportar SNMP over IPv6;

4.5.3.6.3.5.16. Deve suportar HTTP over IPv6;

4.5.3.6.3.5.17. Deve suportar IPv6 remote ping;

4.5.3.6.3.5.18. Deve suportar NTP ou SNTP;

4.5.3.6.3.5.19. Deve implementar log de eventos em memória flash e permitir a gravação em servidor externo padrão Syslog;

4.5.3.6.3.6. **Segurança**

4.5.3.6.3.6.1. Deve possuir proteção a ataques Denial of Service;

4.5.3.6.3.6.2. Deve suportar autenticação local e através de servidor RADIUS e TACACS+;

4.5.3.6.3.6.3. Deve implementar segurança de acesso através do protocolo IEEE 802.1X e autenticação por MAC;

4.5.3.6.3.6.4. Deve suportar assinalamento automático de VLAN e política de QoS;

4.5.3.6.3.6.5. Deve possuir suporte à AAA (Authentication, Authorization and Account) em servidores RADIUS ou TACACS+;

4.5.3.6.3.6.6. Deve suportar implementação de VLANs para visitantes;

4.5.3.6.3.6.7. Deve permitir filtragem de pacotes identificados por cabeçalho ethernet ou IP;

4.5.3.6.3.6.8. Deve suportar DHCP snooping;

4.5.3.6.3.6.9. Deve suportar IP Source Guard;

4.5.3.6.3.6.10. Deve possuir Port Security ou funcionalidade similar;

4.5.3.6.3.6.11. Deve possuir Dynamic ARP Inspection ou funcionalidade similar;

4.5.3.6.3.6.12. Deve implementar MAC based ACL;

4.5.3.6.3.7. **Desempenho**

4.5.3.6.3.7.1. Deve possuir capacidade de vazão de ao menos 80 Gbps;

4.5.3.6.3.7.2. Deve chavear no mínimo 59 Mpps;

4.5.3.6.3.7.3. Tabela de endereços MAC com capacidade para no mínimo 16.000 endereços;

4.5.3.6.3.7.4. Funções camada 3

4.5.3.6.3.7.5. Deve implementar rotas estáticas;

4.5.3.6.3.7.6. Deve implementar o protocolo RIP;

4.5.3.6.3.8. **Padronização**

4.5.3.6.3.8.1. Deve ser compatível com os seguintes padrões:

a) IEEE 802.1D (STP)

b) IEEE 802.1p (COS)

c) IEEE 802.1Q (VLAN)

d) IEEE 802.1s (MSTP)

e) IEEE 802.1v (VLAN)
f) IEEE 802.1w (RSTP)
g) IEEE 802.1X (Security)
h) IEEE 802.3ad (Link aggregation)
i) IEEE 802.3x (Flow control)
j) IEEE 802.3z (Gigabit)
k) IEEE 802.1AB (Link Layer Discovery Protocol)
l) IEEE 802.3az (Energy Efficiency)

4.5.3.6.3.9. **Gerais**

4.5.3.6.3.9.1. Deve possuir fonte de alimentação interna operando em tensões de 100 a 240 V e em frequências de 50 a 60 Hz automaticamente;

4.5.3.6.3.9.2. Deve vir acompanhado do kit de suporte específico para montagem em Rack de 19;

4.5.3.6.3.9.3. O equipamento deverá ocupar uma unidade de rack;

4.5.3.6.3.9.4. Deve possuir temperatura de operação de 0° C a 50° C;

4.5.3.6.3.9.5. Deve possuir sistema operacional OpenLan Switching (OLS) em conformidade com as especificações da Telecom Infra Project (TIP);

4.6. O sistema de gerenciamento de acesso das praças deverá ser de responsabilidade da Contratada, seguindo todas as normas da lei 13.709/2018 (LEI GERAL DE PROTEÇÃO DE DADOS - LGPD) e Lei Federal nº 12.965/2014, Decreto Federal nº 8.771/2016 que regulamenta o Marco Civil da Internet e demais legislações Federais ou Municipais relativas à matéria.

4.7. O caráter confidencial das informações dos usuários será garantido, não podendo ser compartilhado, em nenhuma hipótese, inclusive para uso comercial, publicitário ou estatístico.

4.8. A contratada deverá fornecer acesso ao sistema de gerenciamento das Praças, quantidade de acesso, acesso para inserção de informações e ações da Prefeitura e demais secretarias, não sendo aceito propagandas da contratada.

4.9. O SSID da rede não poderá associar o nome do eventual contratante privado.

4.10. O formato do SSID será definido pela Prefeitura Municipal de Cáceres / Coordenação de Tecnologia da Informação (CTI).

4.11. A Contratada deverá fornecer o sistema de gerenciamento hotspot de fácil acesso para os visitantes, que seja feito a coleta do nome, telefone e e-mail dos visitantes.

4.12. Será obrigação contratual a armazenagem, por todo o período de vigência, do registro de conexão, de medições básicas da rede e de todas as informações de cadastro de usuários, incluindo as informações de preenchimento voluntário.

4.13. Ao pressionar o botão destinado à conexão com a internet pela primeira vez, ele será transferido para a página de cadastro definido pela Contratante;

4.14. Que os usuários não tenham acesso a equipamentos de outros usuários conectados à rede WI-FI.

4.15. A contratada deverá fornecer sistema ou API de gerenciamento de funcionamento dos Wi-Fi das praças para auxiliar a fiscalização e acompanhamento do funcionamento das conexões, além de identificar cada Wi-Fi com o nome das respectivas Praças.

4.16. A Contratada deverá apresentar junto à emissão de Nota Fiscal, os respectivos relatórios de funcionamento, login acessos dos visitantes e consumo de banda por aparelho de rádio, identificando cada praça conforme mês referência da Nota Fiscal.

4.17. A contratada, se achar necessário, poderá fazer uma visita técnica aos pontos das possíveis praças que receberão a internet, para mensurar o custo de cada praça, para a montagem da proposta do preço médio total.

4.18. A contratada deverá fornecer os aparelhos que sejam capazes de abranger geograficamente toda a área da praça ofertada, podendo ser de 1(um) ou mais aparelhos para cada praça.

4.19. Deverão ser previstos todos os equipamentos ativos e passivos de rede, infraestrutura e insumos necessários ao bom funcionamento do sistema, tais como, mas não exclusivamente: postes, fios, cabos, conectores, amplificadores, racks, pontos de conexão (access points), no- breaks, wireless controllers, watch dogs, software e suprimentos complementares de energia elétrica, conforme o caso.

4.20. Cada aparelho de acesso das Praças deverá aceitar até 500 conexões simultâneas, dividindo assim a banda de internet 100mbs igualmente para os visitantes.

4.21. Internets Wi-Fi instaladas deverão ser capazes de garantir a qualidade e estabilidade do sinal aos usuários, evitando jitters e latências, sendo compatíveis com notebooks, celulares, smartphones, netbooks, tablets e outros dispositivos comumente utilizados para acesso à internet, dentro dos padrões mínimos: 802.11b, 802.11g, 802.11n e 802.11ac.

4.22. A contratada deverá garantir o nível de sinal de pelo menos -65 dBm na área de cobertura em todas as localidades e em ambas as faixas de frequência (2,4 GHz e 5 GHz).

4.23. CONTRATADA deverá dispor de ferramentas e recursos de monitoramento e controles de hardware e/ou software que possam ser operados por seus técnicos, e que possibilitem a imediata identificação de anormalidades na operação da infraestrutura de comunicação da rede Wi-Fi

4.24. A Contratada deverá fornecer uma banda de internet de 150 Mbs dedicada para cada ponto instalado.

4.25. O funcionamento de cada praça ofertada será por 24 (vinte e quatro) horas por dia, durante 7 (sete) dias da semana.

4.26. A combinação dessas tecnologias resulta em uma infraestrutura altamente disponível, segura e escalável, proporcionando continuidade operacional, proteção avançada contra ameaças cibernéticas e eficiência na comunicação entre as unidades municipais.

4.27. A solução foi desenhada para assegurar a proteção e a disponibilidade dos serviços municipais ao longo de todo o ciclo de vida do contrato, abrangendo desde a implantação inicial até a gestão contínua da infraestrutura de segurança e conectividade. A abordagem adotada permite que o município de Cáceres modernize sua infraestrutura digital, proteja seus ativos de TI e garanta a prestação eficiente de serviços à população, sempre com segurança, confiabilidade e alta performance.

5. REQUISITOS DA CONTRATAÇÃO

5.1. Requisitos De Negócio

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

5.1.1.1. Implementação de tecnologia Next Generation Firewall (NGFW) para garantir proteção robusta contra ameaças cibernéticas e manutenção da integridade das operações de rede.

5.1.1.2. Implementação de sistema baseado em Inteligência Artificial Preditiva capaz de analisar padrões de comportamento na rede, identificar e neutralizar automaticamente ameaças sem necessidade de intervenção humana.

5.1.1.3. Disponibilização de equipamentos de hardware necessários à proteção da rede, sem a necessidade de aquisição direta, com manutenção e suporte garantidos pelo fornecedor, promovendo economicidade e flexibilidade.

5.1.1.4. Proteção eficaz contra ataques de “Zero Day”.

5.1.1.5. Atuação direta no tráfego de entrada da internet, identificando e neutralizando instantaneamente origens maliciosas.

5.1.1.6. Proteção abrangente para toda a infraestrutura, incluindo firewalls e roteadores.

5.1.1.7. Proteção abrangente para toda a infraestrutura, incluindo firewalls e roteadores.

5.1.1.8. Inclusão de software para configuração, monitoramento e gestão centralizada das políticas de segurança da rede de forma integrada e eficiente, permitindo maior controle e visibilidade.

5.1.1.9. Garantia de licenças válidas durante todo o período contratual, permitindo o pleno uso das funcionalidades da solução contratada.

5.1.1.10. Provisão de link dedicado de acesso à internet, bloco /29 e banda mínima de acesso garantida de 500Mbps para a solução NGFW SEDE (Dois Link de ASN e Rota Diferentes), essa configuração garante alta disponibilidade, resiliência a falhas e suporte eficiente às operações críticas.

5.1.1.11. Configuração e integração dos links diretamente com a solução NGFW, permitindo a gestão eficiente do tráfego e a aplicação das políticas de segurança.

5.1.1.12. Implementação de soluções SD-WAN integradas ao NGFW para conectar unidades externas vinculadas às secretarias municipais, promovendo segurança, desempenho e centralização da gestão de tráfego entre os locais.

5.1.1.13. Provisão de link primário de acesso à internet banda mínima de acesso garantida de 150Mbps Sites Remotos (Fibra Óptica), e link secundário de acesso à internet banda mínima de acesso garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G), link de ASN e rota diferentes, específicos para cada unidade externa e praças municipais, assegurando a continuidade das operações e a resiliência da rede em caso de falhas.

5.1.1.14. Realização de serviços especializados para instalação, configuração inicial e adequação às necessidades específicas do contratante e das unidades externas.

5.1.1.15. Implantação nas unidades externas de redes Wi-Fi seguras e segregadas para uso exclusivo dos servidores municipais, otimizando a conectividade e produtividade.

5.1.1.16. Garantia de autenticação por usuário e integração com políticas de segurança baseadas no NGFW.

5.1.1.17. Oferta de internet Wi-Fi gratuita nas unidades externas e nas praças municipais, com políticas de acesso baseadas no NGFW, assegurando privacidade e controle de navegação.

5.1.1.18. Implementação de mecanismos de limitação de banda e monitoramento para manter a qualidade do serviço e evitar o uso inadequado.

5.1.1.19. Atualizações regulares de firmware e assinaturas de segurança e patches, assegurando proteção contra ameaças emergentes e melhorias contínuas no desempenho da solução.

5.1.1.20. Capacitação especializada para a equipe do contratante, com emissão de certificação que ateste o domínio das funcionalidades e a capacidade de operação e manutenção da solução.

5.1.1.21. Oferta de suporte técnico com níveis de serviço bem definidos (SLA), cobrindo atendimento remoto e presencial, para resolução de incidentes e dúvidas operacionais.

5.1.1.22. Expansibilidade da solução para atender a demandas futuras de crescimento em tráfego, usuários e funcionalidades.

5.1.1.23. Ferramentas para supervisão em tempo real e geração de relatórios detalhados para análise de desempenho, auditorias e conformidade.

5.1.1.24. Garantia de aderência às regulamentações aplicáveis à proteção de dados e segurança da informação, incluindo requisitos legais e normativos vigentes.

5.1.1.25. Solução projetada para assegurar operação ininterrupta, com mecanismos de failover, redundância e backup que minimizem o impacto de falhas ou interrupções.

5.1.1.26. Redução da complexidade operacional, proporcionando maior eficiência no gerenciamento da segurança da rede e otimização de recursos técnicos e financeiros.

5.1.1.27. Configuração de políticas de tráfego e priorização de dados para garantir a performance ideal em aplicações críticas.

5.2. **Requisitos De Capacitação**

5.2.1. Deverá ser incluído na contratação capacitação técnica para a operação da solução, a serem conduzidos diretamente pelo fabricante ou por parceiro nacional devidamente capacitado, certificado e autorizado pelo fabricante para ministrar capacitações oficiais.

5.2.2. Deverá ser ministrado em Língua Portuguesa/Brasil.

5.2.3. Realização de capacitação básica com duração de 40 horas, abrangendo os conhecimentos essenciais para operar e gerenciar a solução implantada.

5.2.4. Deverá ser realizada uma reunião prévia entre o contratante e a empresa contratada para definição do calendário da capacitação básica que trata o item 5.2.3.

5.2.4.1. O cronograma deverá ser ajustado às necessidades da equipe da Coordenação de TI e compatível com a disponibilidade operacional, garantindo a participação integral dos envolvidos e a eficácia do processo de aprendizado.

5.2.5. Capacitação destinada a uma equipe de até 10 participantes da Coordenação de TI, garantindo maior interação com os instrutores e personalização do aprendizado.

5.2.6. Emissão de certificação oficial reconhecida pelo fabricante da solução ou por entidades de referência na área de segurança de rede, atestando a qualificação da equipe.

5.2.7. Capacitação presencial, realizado na sede da Prefeitura Municipal de Cáceres, para otimizar o tempo e garantir a participação efetiva da equipe.

5.2.8. Divisão do conteúdo em módulos, facilitando o aprendizado progressivo:

- Módulo 1: Introdução ao NGFW, IA Preditiva e princípios de segurança de rede.
- Módulo 2: Configuração inicial e operação básica dos equipamentos e software.
- Módulo 3: Gerenciamento de políticas de segurança e monitoramento da rede.
- Módulo 4: Configuração de links dedicados (redundância e backup).
- Módulo 5: Resolução de problemas e resposta a incidentes.

5.2.9. A divisão de conteúdo que trata o item 5.2.8 poderá ser alterado mediante reunião prévia entre o contratante e a empresa contratada.

5.2.10. Inclusão de laboratórios práticos para simulação de cenários reais, como aplicação de políticas de segurança, monitoramento de tráfego e configuração de redundância e backup.

5.2.11. Disponibilização de apostilas, guias de configuração, tutoriais e acesso a uma base de conhecimento técnico para consulta pós-capacitação.

5.2.12. Instruções específicas sobre a configuração, gerenciamento e monitoramento dos links de redundância e backup, incluindo a utilização de IPs fixos.

5.2.13. Aplicação de avaliação ao final da capacitação para validação do conhecimento adquirido, seguido da entrega de certificados aos aprovados.

5.2.14. Abordagem de procedimentos para garantir a continuidade operacional da solução, como atualizações, backup de configurações e gerenciamento de logs.

5.2.15. Disponibilização de suporte técnico após a capacitação, para auxiliar na aplicação prática dos conhecimentos adquiridos.

5.2.16. Orientação sobre as melhores práticas para gestão segura da rede, incluindo conformidade com normas e regulamentações aplicáveis, como a LGPD.

Assinado por 2 pessoas: WELYNGTON DE BARROS MACIEL JEREMIAS PEREIRA LEITE

5.2.17. Previsão de um workshop complementar, podendo este ser por vídeo conferencia, a ser realizado após a conclusão da capacitação, para reforçar conteúdos e sanar dúvidas remanescentes.

5.2.18. Elaboração de relatórios detalhados com informações sobre a participação, desempenho e certificação da equipe, para acompanhamento da gestão de competências.

5.3. **Requisitos Legais**

5.3.1. **Conformidade Legal e Normativa:**

5.3.1.1. A contratação deve obedecer à Constituição Federal, garantindo os princípios da legalidade, moralidade, publicidade, eficiência e economicidade.

5.3.1.2. Estar em conformidade com a Lei nº 14.133/2021, que regula as normas gerais de licitação e contratação pública.

5.3.1.3. Atender à Instrução Normativa SGD/ME nº 94, de 2022, que disciplina contratações de TIC no setor público.

5.3.1.4. Respeitar a Instrução Normativa SEGES/ME nº 65, de 2021, que trata da governança em aquisições de TIC.

5.3.1.5. Observar a Lei nº 13.709, de 2018 (LGPD), garantindo a proteção de dados pessoais.

5.3.1.6. Aplicar as disposições da Lei nº 10.520, de 2001, e do Decreto nº 10.024, de 2019, referentes ao pregão eletrônico.

5.3.1.7. Cumprir o Decreto Municipal nº 665, de 09 de outubro de 2024, que regulamenta contratações de TIC no âmbito municipal.

5.3.2. **Proteção de Dados e Privacidade:**

5.3.2.1. Garantir conformidade integral com a LGPD, implementando medidas para prevenir acessos não autorizados e vazamentos de dados pessoais.

5.3.2.2. O contratado deve demonstrar, quando solicitado, os mecanismos e políticas utilizados para assegurar a proteção de dados, sujeitos à auditoria da contratante.

5.3.3. **Transparência e Publicidade:**

5.3.3.1. Todos os atos do processo licitatório e de execução contratual deverão ser registrados e divulgados nos meios oficiais, conforme exigido por lei.

5.3.3.2. Relatórios e informações sobre a execução do contrato deverão ser disponibilizados periodicamente para consulta pública, garantindo transparência no uso dos recursos.

5.3.4. **Responsabilidade do Contratado:**

5.3.4.1. O contratado é responsável por cumprir integralmente as obrigações legais aplicáveis, incluindo as previstas na Lei nº 14.133/2021 e no Decreto Municipal nº 665/2024, respondendo por eventuais descumprimentos com as penalidades previstas em contrato e em lei.

5.4. **Requisitos De Manutenção**

5.4.1. **Manutenção Preventiva (Não Emergencial):**

5.4.1.1. Realização de manutenções programadas para garantir o funcionamento ideal da solução NGFW, incluindo inspeções, limpeza, análise de logs, e aplicação de atualizações de firmware.

5.4.1.2. Frequência mínima semestral ou conforme cronograma estabelecido entre as partes.

5.4.2. **Manutenção Corretiva (Emergencial):**

5.4.2.1. Atendimento imediato para corrigir falhas ou defeitos nos equipamentos ou no software, visando a restauração do funcionamento normal da solução NGFW.

5.4.2.2. Inclui diagnóstico remoto e, quando necessário, deslocamento técnico para reparos ou substituição de componentes.

5.4.3. **Manutenção Adaptativa (Não Emergencial):**

5.4.3.1. Adequação da solução NGFW às mudanças no ambiente operacional ou aos requisitos específicos do contratante, como ajustes de configuração ou implementação de novas políticas de segurança.

5.4.4. **Manutenção Evolutiva (Não Emergencial):**

5.4.4.1. Implementação de melhorias na solução, incluindo a integração de novas funcionalidades, suporte a tecnologias emergentes e expansão da capacidade para atender a demandas crescentes.

5.4.5. **Monitoramento Proativo (Não Emergencial):**

5.4.5.1. Serviço contínuo de monitoramento da solução, com análise de logs e detecção antecipada de falhas ou ameaças que exijam intervenção.

5.4.6. **Substituição de Equipamentos (Emergencial):**

5.4.6.1. Garantia de substituição rápida e sem custos adicionais de equipamentos defeituosos durante a vigência contratual, minimizando interrupções.

5.4.7. **Relatórios Periódicos (Não Emergencial):**

5.4.7.1. Emissão de relatórios detalhados sobre intervenções realizadas, estado dos equipamentos, atualizações aplicadas e resultados das manutenções.

5.4.8. **Classificação de Ocorrências:**

5.4.8.1. Critérios claros para categorizar os atendimentos em emergenciais e não emergenciais, com tratamento prioritário para problemas críticos.

5.4.9. **Tabela de atendimento:**

TIPO DE ATENDIMENTO	**DESCRIÇÃO**	**EMERGENCIAL/NÃO EMERGENCIAL**	**TEMPO DE RESPOSTA**	**TEMPO DE SOLUÇÃO**	**MEIO DE ATENDIMENTO**
Emergencial	Ocorrências críticas que impactem diretamente a operação da rede, como falhas graves nos equipamentos NGFW, links de redundância ou brechas de segurança.	Emergencial	Até 1 hora	Até 4 horas	Suporte remoto e se necessário, presencial.
Corretiva	Problemas pontuais ou defeitos que não sejam de natureza crítica, mas que exijam reparo técnico para evitar impactos futuros.	Emergencial	Até 4 horas	Até 8 horas	Suporte remoto ou presencial agendado.
Preventiva	Ações periódicas de inspeção e manutenção	Não Emergencial	Agendamento prévio	Conforme cronograma	Suporte presencial planejado.

	para prevenir falhas e garantir o desempenho ideal da solução.				
Adaptativa	Ajustes para adequação da solução a novas necessidades operacionais ou mudanças no ambiente do contratante.	Não Emergencial	Até 2 dias úteis	Até 7 dias úteis	Suporte remoto ou presencial agendado.
Evolutiva	Melhorias e implementações que ampliem as funcionalidades ou capacidades da solução NGFW.	Não Emergencial	Até 5 dias úteis	Conforme projeto	Suporte remoto ou presencial planejado.
Substituição de Equipamentos	Substituição de equipamentos defeituosos ou que apresentem falhas que afetem a continuidade do serviço.	Emergencial	Até 1 hora	Até 4 horas	Suporte remoto e, se necessário, presencial.
Monitoramento Proativo	Monitoramento contínuo da solução para antecipar problemas, como detecção de falhas ou anomalias.	Não Emergencial	Até 4 horas	Contínuo	Suporte remoto.
Relatórios Periódicos	Emissão de relatórios detalhados sobre o status da solução NGFW, ações realizadas e estado dos equipamentos.	Não Emergencial	Até 24 horas	Conforme cronograma	Suporte remoto ou presencial agendado.

5.5. **Requisitos Temporais**

5.5.1. **Prazos de Entrega dos Equipamentos e Solução:**

5.5.1.1. O fornecimento dos equipamentos necessários para a implementação da solução, incluindo hardware, licenças e software de gerenciamento, deverá ser realizado no prazo máximo de 30 dias corridos a partir da assinatura do contrato.

5.5.1.2. A instalação, configuração e ativação completa da solução, incluindo os links de internet e redundância, deverá ser concluída no prazo máximo de 45 dias corridos após a entrega dos equipamentos.

5.5.1.3. O treinamento básico com carga horária de 40 horas para a equipe técnica da Prefeitura Municipal de Cáceres deverá ser realizada uma reunião prévia entre o contratante e a empresa contratada para definição do calendário da capacitação básica.

5.5.2. **Prazos de Atendimento para Suporte Técnico:**

5.5.2.1. **Atendimento Emergencial:**

5.5.2.1.1. Chamados emergenciais, que incluem falhas críticas que afetam diretamente a operação da rede ou a disponibilidade de serviços essenciais, deverão ser atendidos no prazo máximo de 4 horas após a abertura do chamado.

5.5.2.1.2. A solução completa para o problema deverá ser implementada no prazo máximo de 8 horas, salvo situações excepcionais que exijam medidas corretivas complexas.

5.5.2.2. **Atendimento Não Emergencial:**

5.5.2.2.1. Chamados de manutenção corretiva, preventiva, adaptativa ou evolutiva que não impactem diretamente a operação da rede deverão ser atendidos no prazo máximo de 24 horas úteis após a abertura do chamado.

5.5.2.2.2. A resolução deverá ocorrer no prazo de até 5 dias úteis, salvo a necessidade de ajustes ou implementações que exijam maior prazo, o qual será acordado previamente.

5.5.3. **Forma de Atendimento do Suporte Técnico:**

5.5.3.1. **Atendimento Remoto:**

5.5.3.1.1. O suporte técnico deverá ser disponibilizado remotamente como primeira opção para resolução de problemas, utilizando ferramentas seguras para acesso remoto e diagnóstico.

5.5.3.1.2. O suporte remoto deverá estar disponível 24x7 (24 horas por dia, 7 dias por semana) para incidentes emergenciais.

5.5.3.2. **Atendimento Presencial:**

5.5.3.2.1. Quando a resolução do problema não for possível de forma remota, será realizado atendimento presencial por técnicos especializados.

5.5.3.2.2. O prazo para deslocamento e início do atendimento no local para casos emergenciais será de até 4 horas úteis a partir da solicitação.

5.5.3.2.3. Para casos não emergenciais, o atendimento presencial será agendado com a equipe de TI da Prefeitura, respeitando o prazo máximo de 2 dias úteis.

5.5.4. **Monitoramento e Relatórios de SLA:**

5.5.4.1. A empresa contratada deverá monitorar e registrar os tempos de atendimento e resolução de chamados, emitindo relatórios mensais que comprovem o cumprimento dos SLAs estabelecidos.

5.5.4.2. O descumprimento dos prazos estabelecidos implicará penalidades contratuais conforme especificado nos termos do contrato.

5.5.5. **Atendimento de Manutenção Preventiva e Evolutiva:**

5.5.5.1. Manutenções preventivas deverão ser realizadas trimestralmente, com agendamento prévio com a equipe de TI da Prefeitura Municipal de Cáceres.

5.5.5.2. Manutenções evolutivas, que envolvam atualizações ou melhorias significativas na solução, deverão ser realizadas mediante planejamento e acordo prévio, com prazo máximo de implementação em 30 dias úteis após a aprovação.

5.6. **Requisitos de Segurança e Privacidade**

5.6.1. **Políticas de Segurança Baseadas no NGFW**

5.6.1.1. Permitir a configuração de políticas robustas de segurança para controle e monitoramento do tráfego de rede, assegurando proteção contra ataques cibernéticos, intrusões, malwares e acessos não autorizados.

5.6.1.2. Definir regras personalizadas para bloquear tráfego malicioso e permitir apenas conexões seguras e autorizadas.

5.6.1.3. Configuração de proteção contra ataques de negação de serviço (DoS), com a opção de habilitação global ou por política específica.

5.6.1.4. Disponibilizar uma interface única para configuração de políticas, integrando perfis de segurança como Proxy Web, IPS, Controle de Aplicações, SD-WAN e Proteção contra Ameaças Avançadas (ATP).

5.6.1.5. Implementar validação automatizada das políticas de segurança para identificar e resolver regras duplicadas ou conflitantes.

5.6.2. **Segmentação e Isolamento de Redes**

5.6.2.1. Segmentação lógica da rede principal e das redes das unidades externas, garantindo o isolamento entre setores e usuários, reduzindo os riscos de propagação de ataques.

5.6.2.2. Configuração de SD-WAN para roteamento dinâmico de tráfego entre diferentes unidades e praças municipais, assegurando desempenho e segurança.

5.6.3. **Proteção Avançada Contra Ameaças**

5.6.3.1. Ativação de funcionalidades como inspeção profunda de pacotes (DPI), prevenção contra intrusões (IPS) e detecção de anomalias baseadas em inteligência artificial.

5.6.3.2. Integração com serviços de inteligência de ameaças para identificação e mitigação de ataques emergentes.

5.6.4. **Criptografia de Dados e Segurança em Trânsito**

5.6.4.1. Garantir que todas as comunicações de dados entre firewall principal, unidades externas e dispositivos sejam protegidas por protocolos de criptografia avançados, como TLS/SSL.

5.6.4.2. Implementação de inspeção de tráfego criptografado (SSL Inspection) para detecção de ameaças em comunicações seguras.

5.6.5. **Controle de Acessos e Gerenciamento Centralizado**

5.6.5.1. Adotar autenticação multifator (MFA) para acesso ao sistema de gerenciamento do NGFW e a serviços críticos.

5.6.5.2. Realizar o gerenciamento centralizado de permissões, com auditoria detalhada de acessos e atividades realizadas na rede.

5.6.6. **Monitoramento, Logs e Alertas de Segurança**

5.6.6.1. Configuração de logs detalhados de eventos e atividades, com centralização das informações em uma solução de SIEM (Gestão de Informações e Eventos de Segurança).

5.6.6.2. Geração de alertas em tempo real para eventos críticos, como tentativas de intrusão ou anomalias de tráfego.

5.6.6.3. Emissão de relatórios periódicos sobre segurança da rede, destacando vulnerabilidades detectadas e ações tomadas.

5.6.7. **Conformidade com Normas de Segurança e Privacidade**

5.6.7.1. Garantir que a solução NGFW esteja em conformidade com a LGPD e outras legislações aplicáveis, assegurando a proteção e privacidade dos dados pessoais.

5.6.7.2. Disponibilizar recursos para anonimização ou pseudonimização de dados, conforme exigido pelas normas.

5.6.8. **Testes e Avaliações Periódicas de Segurança**

5.6.8.1. Realização de testes de penetração (pentests) regulares para avaliar a eficácia das medidas de segurança.

5.6.8.2. Simulações de incidentes de segurança para treinar equipes e validar os planos de resposta a incidentes.

5.6.9. **Backup e Recuperação Segura**

5.6.9.1. Implementar backups automáticos e criptografados das configurações do NGFW e de dados críticos, com armazenamento em locais seguros.

5.6.9.2. Garantir processos rápidos de recuperação em caso de falha ou desastre, assegurando a continuidade operacional.

5.6.10. **Conscientização e Educação de Usuários**

5.6.10.1. Desenvolver programas regulares de conscientização sobre segurança da informação para servidores municipais, abordando práticas seguras de uso da internet.

5.6.10.2. Orientar os cidadãos sobre o uso responsável das redes Wi-Fi públicas disponibilizadas nas praças e unidades municipais.

5.7. **Requisitos de Metodologia de Trabalho**

5.7.1. Emissão de Ordem de Serviço (OS):

5.7.1.1. A execução de qualquer serviço contratado está condicionada ao recebimento pelo contratado de uma Ordem de Serviço (OS) emitida pela contratante.

5.7.1.2. A Ordem de Serviço deverá especificar, de forma clara:

- O serviço a ser executado.
- A quantidade de serviços.
- A localidade onde o serviço deverá ser prestado.

5.7.2. **Meios de Contato e Registro de Ocorrências:**

5.7.2.1. O contratado deve fornecer canais de comunicação para contato e registro de ocorrências, conforme as seguintes especificações:

- Atendimento eletrônico (e-mail, sistema de chamados ou aplicativo): 24 horas por dia, 7 dias por semana.

- Atendimento telefônico: 12 horas por dia, 5 dias por semana, garantindo resposta ágil a chamados emergenciais.

5.7.3. **Acompanhamento e Comunicação Durante a Execução:**

5.7.3.1. A execução de todos os serviços deverá ser acompanhada diretamente pelo contratado, assegurando o cumprimento das especificações definidas na Ordem de Serviço.

5.7.3.2. Eventuais ocorrências ou desvios identificados durante a execução deverão ser imediatamente comunicados à contratante, com descrição detalhada da situação e das medidas corretivas adotadas.

5.7.4. **Prazos de Atendimento e Execução:**

5.7.4.1. O prazo para início da execução dos serviços será contado a partir do recebimento da Ordem de Serviço, respeitando os prazos definidos nos Requisitos Temporais.

5.7.4.2. Os serviços deverão ser finalizados dentro dos prazos estabelecidos, salvo justificativas formalmente apresentadas e aceitas pela contratante.

5.7.5. **Registro e Relatório de Serviços Executados:**

5.7.5.1. Ao término de cada serviço, o contratado deverá entregar à contratante um relatório detalhado contendo:

- Descrição do serviço realizado.
- Data e horário de início e conclusão do serviço.
- Identificação dos profissionais envolvidos.
- Observações sobre eventuais dificuldades ou necessidades futuras.

5.7.5.2. O relatório deverá ser aprovado pela contratante para formalizar a conclusão do serviço.

5.7.6. **Garantia de Qualidade e Conformidade:**

5.7.6.1. O contratado deverá assegurar que todos os serviços sejam executados em conformidade com as especificações técnicas, normativas e de segurança previamente acordadas.

5.7.6.2. Qualquer serviço executado em desacordo com o estabelecido será considerado não conforme, cabendo ao contratado refazê-lo sem custos adicionais para a contratante.

5.7.7. **Reuniões de Alinhamento e Planejamento:**

5.7.7.1. O contratado deverá participar de reuniões periódicas com a contratante para alinhar prioridades, revisar o cronograma e discutir ajustes necessários nos serviços prestados.

5.7.7.2. Essas reuniões ocorrerão em frequência mínima trimestral ou conforme solicitado pela contratante.

5.7.8. **Garantia de Resposta a Ocorrências:**

5.7.8.1. O contratado deverá manter equipe disponível para atender a chamados dentro dos prazos especificados nos Requisitos de Manutenção, priorizando serviços emergenciais.

5.7.8.2. As ocorrências serão classificadas conforme sua criticidade, e o atendimento será realizado de acordo com a priorização estabelecida na Ordem de Serviço.

5.8. **Requisitos de Experiência Profissional**

5.8.1. **Experiência Comprovada no Fornecimento de Soluções NGFW:**

5.8.1.1. O contratado deverá comprovar experiência na implementação e gerenciamento de soluções de Next Generation Firewall (NGFW) em instituições públicas ou privadas de grande porte, preferencialmente na administração municipal.

5.8.1.2. Será exigida a comprovação da capacidade técnico-operacional da licitante, mediante a apresentação de atestados emitidos por pessoa jurídica de direito público ou privado, que comprovem a execução de serviços compatíveis em características, quantidades e prazos com o objeto deste contrato, incluindo o fornecimento e a instalação de equipamentos correlatos aos ofertados, bem como a prestação de serviços de instalação, configuração e suporte técnico. A licitante deverá comprovar, no mínimo, experiência prévia correspondente a **30% (trinta por cento)** do quantitativo estimado do **item 1 – Solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)**, considerado de maior relevância técnica para a consecução do objeto. Tal exigência encontra amparo no inciso III do art. 67 da Lei nº 14.133/2021, sendo justificada pela complexidade e especificidade do objeto, que demanda experiência comprovada na execução de soluções integradas de segurança cibernética, com destaque para componentes baseados em Inteligência Artificial Preditiva, visando garantir a eficiência, a continuidade dos serviços e a mitigação de riscos operacionais, em observância aos princípios da legalidade, razoabilidade, eficiência e interesse público. O detalhamento das condições para aceitação dos atestados encontra-se disciplinado no item **10.2.1.5.1** e respectivos subitens.

5.8.2. **Qualificação da Equipe Técnica:**

5.8.2.1. A equipe técnica alocada deve possuir profissionais certificados pelo fabricante da solução NGFW a ser implementada, garantindo competência técnica para execução dos serviços contratados.

5.8.2.2. Os profissionais responsáveis pela execução dos serviços devem ter experiência mínima de 2 (dois) anos em funções relacionadas à implantação, manutenção e suporte de soluções de segurança da informação.

5.8.3. **Experiência em Projetos de TIC para o Setor Público:**

5.8.3.1. O contratado deverá demonstrar experiência específica em projetos de Tecnologia da Informação e Comunicação (TIC) realizados para órgãos da administração pública, especialmente em contextos municipais.

5.8.3.2. A comprovação poderá incluir contratos anteriores, declarações ou relatórios técnicos que atestem a capacidade do contratado em atender às exigências específicas de órgãos públicos.

5.8.4. **Atendimento a Requisitos de Escalabilidade e Complexidade:**

5.8.4.1. A empresa deverá comprovar ter executado projetos que envolvam ambientes complexos, com integração de múltiplas unidades ou localidades, utilizando tecnologias como SD-WAN e links redundantes.

5.8.4.2. Será considerado diferencial a experiência em projetos que incluíram a disponibilização de internet Wi-Fi para servidores e cidadãos.

5.8.5. **Experiência em Treinamento e Capacitação:**

5.8.5.1. A empresa deve demonstrar ter conduzido treinamentos técnicos relacionados à operação de soluções NGFW, com fornecimento de certificações reconhecidas.

5.8.5.2. O contratado deverá apresentar registro de treinamentos realizados, com informações sobre a carga horária, conteúdo programático e feedback dos participantes.

5.8.6. **Critérios de Avaliação da Experiência:**

5.8.6.1. A experiência profissional será avaliada com base nos documentos apresentados, como contratos, atestados, certificados de conclusão de projetos e outros registros comprobatórios.

5.8.6.2. A ausência de comprovação adequada poderá resultar na desclassificação da proposta, conforme previsto na legislação vigente.

5.9. **Requisitos de Segurança da Informação e Privacidade**

5.9.1. **Conformidade com Normas e Padrões de Segurança:**

5.9.1.1. O contratado deve aderir às diretrizes da ISO/IEC 27001, garantindo a gestão eficiente da segurança da informação durante toda a execução do contrato.

5.9.1.2. Implementar controles técnicos e organizacionais para mitigar riscos de acessos não autorizados, vazamentos de dados e interrupções nos serviços.

5.9.2. **Proteção de Dados Sensíveis:**

5.9.2.1. A CONTRATADA deverá assegurar a proteção de todos os dados sensíveis e confidenciais trafegados, processados ou armazenados nos equipamentos fornecidos, utilizando criptografia adequada e outros mecanismos de segurança, em estrita conformidade com a Lei Geral de Proteção de Dados (LGPD).

5.9.2.2. É vedado à CONTRATADA compartilhar, divulgar ou permitir o acesso de terceiros a quaisquer dados sensíveis ou confidenciais, salvo mediante autorização expressa e formal da CONTRATANTE, observadas as disposições legais aplicáveis.

5.9.3. **Gestão de Políticas de Segurança:**

5.9.3.1. A solução fornecida deverá possibilitar a criação, gerenciamento e auditoria de políticas de segurança de forma centralizada, assegurando a rastreabilidade de todas as alterações e acessos.

5.9.3.2. As políticas deverão integrar funcionalidades de IPS (Prevenção contra Intrusões), SD-WAN, controle de aplicações, filtros de conteúdo web e inspeção de tráfego criptografado (SSL/TLS).

5.9.4. **Monitoramento e Resposta a Incidentes:**

5.9.4.1. O sistema deve realizar monitoramento contínuo para identificar e mitigar incidentes de segurança em tempo real.

5.9.4.2. Eventos críticos deverão gerar alertas automáticos e relatórios detalhados, a serem compartilhados com a CONTRATANTE conforme prazos previamente estabelecidos.

5.9.5. **Controle de Acesso:**

5.9.5.1. O acesso ao sistema de gerenciamento do NGFW e demais serviços críticos deverá ser protegido por mecanismos robustos de autenticação, incluindo autenticação multifator (MFA).

5.9.5.2. Os acessos deverão ser controlados por perfis de usuário, com registros completos (logs) de todas as atividades realizadas.

5.9.6. **Tratamento de Dados de Redes Wi-Fi:**

5.9.6.1. A solução deverá garantir a segregação lógica entre os dados trafegados por servidores municipais e cidadãos nas redes Wi-Fi disponibilizadas.

5.9.6.2. É vedada a utilização dos dados coletados ou trafegados na rede Wi-Fi para qualquer finalidade sem autorização formal da CONTRATANTE e em conformidade com a LGPD.

5.9.7. **Backup e Recuperação de Dados:**

5.9.7.1. O sistema deverá realizar backups automáticos e criptografados de todas as configurações, incluindo logs de segurança e políticas implementadas.

5.9.7.2. Deve-se garantir a recuperação rápida e segura dos dados em caso de falhas ou incidentes.

5.9.8. **Educação e Conscientização de Segurança:**

5.9.8.1. A CONTRATADA deverá fornecer materiais educativos ou treinamentos para conscientização dos servidores municipais sobre práticas seguras de navegação, uso de redes Wi-Fi e proteção contra ameaças cibernéticas.

5.9.9. **Auditorias e Testes de Segurança:**

5.9.9.1. Realizar auditorias periódicas no ambiente de segurança implementado, identificando vulnerabilidades e propondo medidas corretivas.

5.9.9.2. Realizar testes de vulnerabilidade e simulações de incidentes para avaliar a eficácia das medidas de proteção e identificar oportunidades de aprimoramento.

5.10. **Requisitos de Sustentabilidade**

5.10.1. **Uso Eficiente de Recursos Energéticos:**

5.10.1.1. Os equipamentos fornecidos, incluindo os dispositivos NGFW, deverão possuir características de eficiência energética, certificadas por padrões internacionais reconhecidos, como Energy Star ou equivalentes.

5.10.1.2. A empresa contratada deverá garantir que os equipamentos operem com consumo energético reduzido, promovendo a sustentabilidade ambiental e diminuindo os custos operacionais.

5.10.2. **Descarte Adequado de Equipamentos Obsoletos:**

5.10.2.1. Todos os equipamentos substituídos durante a vigência do contrato deverão ser descartados de forma responsável e conforme as normas ambientais vigentes, incluindo a Política Nacional de Resíduos Sólidos (PNRS).

5.10.2.2. A contratada deverá apresentar comprovantes de descarte adequado ou reciclagem dos componentes eletrônicos substituídos.

5.10.3. **Redução de Impacto Ambiental no Transporte:**

5.10.3.1. Sempre que possível, as atividades de instalação, manutenção e suporte deverão ser realizadas de forma remota, minimizando deslocamentos físicos e reduzindo a emissão de gases de efeito estufa.

5.10.3.2. Quando o atendimento presencial for indispensável, a empresa contratada deverá priorizar o uso de veículos elétricos ou de baixo consumo energético.

5.10.4. **Promoção de Práticas Digitais Sustentáveis:**

5.10.4.1. O contratado deverá implementar soluções digitais que reduzam o uso de papel, como relatórios, registros de manutenção e documentação de configuração disponibilizados exclusivamente em formato eletrônico.

5.10.4.2. Os sistemas e ferramentas utilizados deverão ser otimizados para minimizar o consumo de banda de rede, evitando desperdícios e sobrecargas desnecessárias.

5.10.5. **Gestão Responsável dos Links de Internet:**

5.10.5.1. A configuração dos links de internet deverá priorizar o uso eficiente dos recursos disponíveis, evitando sobrecargas e consumo desnecessário.

5.10.5.2. O contratado deverá implementar práticas de monitoramento contínuo para garantir que os links estejam sendo utilizados de forma sustentável e equilibrada.

5.10.6. **Capacitação com Enfoque Sustentável:**

5.10.6.1. Os treinamentos oferecidos para a equipe da Prefeitura deverão incluir orientações sobre práticas sustentáveis no uso e gerenciamento dos sistemas e dispositivos de rede.

5.10.6.2. A capacitação deverá enfatizar a importância da economia de recursos, como energia e banda, no contexto de TI sustentável.

5.10.7. **Relatórios de Sustentabilidade:**

5.10.7.1. A contratada deverá apresentar relatórios periódicos sobre ações e práticas sustentáveis implementadas, incluindo:

- Consumo energético dos equipamentos fornecidos.
- Impacto ambiental reduzido pelas operações remotas.
- Quantidade de materiais reciclados ou descartados adequadamente.

5.10.7.2. Esses relatórios deverão ser analisados em conjunto com a contratante para identificar oportunidades adicionais de sustentabilidade.

5.11. **Da Exigência de Carta de Solidariedade**

5.11.1. Será exigida a apresentação de Carta de Solidariedade, emitida pelo fabricante, como garantia da execução contratual.

5.11.2. A referida carta deverá ser apresentada juntamente com a qualificação técnica da licitante e abranger os seguintes itens da solução ofertada:

- Item 1, do Lote Único;
- Item 2, do Lote Único;
- Item 3, do Lote Único;

- Item 4, do Lote Único.

5.11.3. A exigência visa assegurar que as licitantes contratadas possuam plenas condições de fornecimento e manutenção dos equipamentos mencionados, garantindo seu pleno funcionamento durante a vigência do contrato.

5.11.4. A exigência busca resguardar a Administração contra eventuais prejuízos decorrentes da indisponibilidade de peças de reposição ou da ausência de suporte técnico necessário para ajustes e aprimoramentos dos equipamentos fornecidos.

5.12. Subcontratação

5.12.1. **Critérios para Subcontratação:**

5.12.1.1. A subcontratação de serviços pela empresa contratada será permitida apenas mediante autorização prévia e formal da Prefeitura Municipal de Cáceres.

5.12.1.2. A empresa contratada deverá garantir que a subcontratada possua capacidade técnica comprovada, com experiência e certificações relevantes ao escopo dos serviços a serem executados.

5.12.2. **Responsabilidades da Contratada em Caso de Subcontratação:**

5.12.2.1. A empresa contratada será responsável integralmente pelos serviços executados pela subcontratada, respondendo pelos mesmos padrões de qualidade, prazos e resultados exigidos no contrato.

5.12.2.2. A contratada deverá assegurar que os serviços realizados pela subcontratada estejam em conformidade com todos os requisitos técnicos, normativos e de segurança estabelecidos no contrato.

5.12.2.3. Qualquer prejuízo ou falha decorrente de serviços executados pela subcontratada será de total responsabilidade da empresa contratada, que deverá arcar com os custos e medidas corretivas necessárias.

5.12.3. **Obrigações Adicionais da Subcontratada:**

5.12.3.1. A subcontratada deverá seguir rigorosamente as normas de segurança e privacidade, especialmente aquelas relacionadas à Lei Geral de Proteção de Dados (LGPD).

5.12.3.2. A subcontratada deverá assinar um Termo de Confidencialidade, comprometendo-se a proteger todas as informações relacionadas ao projeto e à infraestrutura da Prefeitura Municipal de Cáceres.

5.12.4. **Limitações e Proibições:**

5.12.4.1. Não será permitido subcontratar o fornecimento de equipamentos essenciais, como os dispositivos NGFW, IA preditiva e softwares de gerenciamento, que deverão ser fornecidos diretamente pela contratada ou pelo fabricante autorizado.

5.12.4.2. Não será permitido subcontratar serviços que envolvam suporte emergencial ou atividades críticas que demandem resposta imediata.

5.12.4.3. A subcontratação de serviços especializados (ex.: treinamento oficial, suporte técnico avançado) somente será permitida se o subcontratado for certificado pelo fabricante da solução NGFW, IA preditiva e softwares de gerenciamento.

5.12.5. **Comunicação e Relatórios:**

5.12.5.1. A empresa contratada deverá notificar previamente a Prefeitura Municipal de Cáceres sobre qualquer intenção de subcontratar serviços, fornecendo informações detalhadas sobre a empresa subcontratada e os serviços a serem realizados.

5.12.5.2. Relatórios detalhados sobre a execução de serviços pela subcontratada deverão ser incluídos nos relatórios periódicos enviados pela empresa contratada.

5.12.6. **Penalidades em Caso de Irregularidades na Subcontratação:**

5.12.6.1. O não cumprimento das condições estabelecidas para subcontratação poderá implicar penalidades contratuais, incluindo advertências, multas ou até rescisão contratual.

5.12.6.2. A Prefeitura Municipal de Cáceres poderá solicitar a substituição imediata da subcontratada caso se identifiquem falhas graves ou descumprimento dos requisitos contratuais.

5.13. **Garantia Da Contratação**

5.13.1. Não se aplica ao objeto deste Termo de Referência.

5.14. **Da Alteração Subjetiva**

5.14.1. Não se aplica no presente processo licitatório.

6. PAPÉIS E RESPONSABILIDADES

6.1. Durante o período de vigência do contrato sem prejuízo para as obrigações mencionadas em outros dispositivos deste instrumento ou de qualquer outra obrigação imposta por lei, **serão obrigações da CONTRATANTE**:

6.1.1. Proporcionar à CONTRATADA todas as condições necessárias para a execução dos serviços e entrega dos produtos, incluindo infraestrutura, suporte técnico e informações adicionais de responsabilidade da CONTRATANTE.

6.1.2. Prestar à CONTRATADA todas as informações, esclarecimentos, elementos e dados técnicos necessários ao cumprimento do contrato.

6.1.3. Encaminhar à CONTRATADA todas as solicitações relativas à execução dos serviços e ao fornecimento de produtos, detalhando requisitos, prazos e especificações.

6.1.4. Permitir o acesso de empregados, prepostos ou representantes da CONTRATADA às dependências da Prefeitura Municipal de Cáceres, desde que previamente autorizado e em conformidade com as normas de segurança do local.

6.1.5. Acompanhar e fiscalizar a execução do contrato, designando servidor ou comissão responsável para monitoramento das atividades da CONTRATADA, conforme previsto na Lei nº 14.133/2021.

6.1.6. Garantir que os fiscais designados documentem ocorrências, elaborem relatórios e comuniquem irregularidades à CONTRATADA de forma tempestiva.

6.1.7. Verificar, no prazo fixado, a conformidade dos serviços prestados e produtos entregues, garantindo sua adequação às especificações contratuais.

6.1.8. Rejeitar, total ou parcialmente, serviços ou produtos que não atendam aos requisitos contratuais, comunicando a necessidade de correção ou substituição.

6.1.9. Aplicar as penalidades cabíveis, garantindo a prévia e ampla defesa da CONTRATADA.

6.1.10. Informar imediatamente à CONTRATADA qualquer problema ou irregularidade detectada nos serviços ou produtos fornecidos.

6.1.11. Solicitar, por escrito, a substituição dos serviços que apresentarem desconformidade com o contrato.

6.1.12. Emitir o Termo de Aceite Definitivo após a devida implantação dos serviços contratados.

6.1.13. Atestar as faturas de serviço apresentadas mensalmente pela CONTRATADA.

6.1.14. Manifestar-se, no prazo de 3 dias úteis, sobre as informações contidas na planilha de memória de cálculo fornecida pela CONTRATADA.

6.1.15. Efetuar o pagamento à CONTRATADA no prazo estipulado, desde que todas as obrigações contratuais tenham sido devidamente cumpridas e homologadas.

6.1.16. Promover reuniões periódicas com a CONTRATADA para avaliação do andamento dos serviços, apresentação de relatórios técnicos e resolução de eventuais problemas.

6.1.17. Registrar todas as interações e ocorrências relacionadas ao contrato, garantindo rastreabilidade e acompanhamento das obrigações de ambas as partes.

6.2. Durante o período de vigência do contrato, sem prejuízo para as obrigações mencionadas em outros dispositivos deste instrumento ou de qualquer outra obrigação imposta por lei, **serão obrigações da CONTRATADA**:

6.2.1. Cumprir todas as obrigações previstas no Edital, seus anexos e na proposta apresentada, assumindo integralmente os riscos e as despesas decorrentes da execução do contrato.

6.2.2. Executar o objeto do contrato em sua totalidade, em conformidade com as especificações estabelecidas no Termo de Referência e no contrato firmado.

6.2.3. Efetuar a entrega dos serviços e produtos dentro dos prazos estabelecidos, garantindo que estejam em perfeitas condições e em conformidade com as especificações contratuais.

6.2.4. Acompanhar a entrega dos produtos com a devida nota fiscal, contendo marca, fabricante, modelo, procedência, prazo de garantia ou validade e demais informações exigidas.

6.2.5. Garantir que os serviços e produtos fornecidos sejam de boa qualidade, atendendo integralmente as condições, quantidades e padrões estipulados no contrato.

6.2.6. Resolver prontamente quaisquer falhas ou não conformidades apontadas pela CONTRATANTE, incluindo a substituição ou correção dos serviços e produtos rejeitados.

6.2.7. Manter, durante toda a execução do contrato, as condições de habilitação exigidas, incluindo requisitos técnicos, fiscais, trabalhistas e sociais.

6.2.8. Assumir integralmente as despesas relacionadas à execução do contrato, incluindo tributos, encargos trabalhistas e previdenciários de seus empregados.

6.2.9. Disponibilizar equipe técnica qualificada e apta a atender às demandas durante toda a vigência do contrato.

6.2.10. Implementar práticas de sustentabilidade ambiental, social e econômica na execução dos serviços, conforme princípios legais e normativos aplicáveis.

6.2.11. Permitir à CONTRATANTE a fiscalização da execução dos serviços e fornecimento dos produtos, prestando todos os esclarecimentos solicitados.

6.2.12. Registrar todas as interações e ocorrências relacionadas ao contrato, garantindo rastreabilidade e acompanhamento das obrigações contratuais.

6.2.13. Fornecer canais de atendimento eficientes para comunicação com a CONTRATANTE, garantindo solução ágil para eventuais problemas.

6.2.14. Tomar todas as providências necessárias para implantar e manter os serviços contratados em níveis satisfatórios, de acordo com o IMR e demais disposições contratuais.

6.2.15. Fornecer, sem custo adicional, todos os equipamentos e acessórios necessários à prestação dos serviços nas condições estabelecidas no contrato.

6.2.16. Diagnosticar falhas nos serviços relatadas pela CONTRATANTE e eliminar defeitos nos componentes sob sua responsabilidade.

6.2.17. Sanar quaisquer falhas, degradações ou indisponibilidades do serviço, independentemente de notificação da CONTRATANTE ou detecção via monitoramento proativo.

6.2.18. Executar serviços que acarretem riscos aos sistemas em produção ou requeiram parada de servidores, equipamentos ou rede elétrica somente fora do expediente, incluindo finais de semana e feriados, mediante prévia autorização do Setor de Tecnologia da Informação e Comunicação.

6.2.19. Comunicar à CONTRATANTE, via e-mail e com antecedência mínima de três horas, a presença de seus colaboradores no ambiente da CONTRATANTE, informando nome completo e CPF do técnico para prestação de serviços de instalação ou manutenção.

6.2.20. Fornecer crachá de identificação a seus prepostos durante a realização das atividades no ambiente da CONTRATANTE.

6.2.21. Apresentar mensalmente relatório contendo a planilha de memória de cálculo do faturamento, detalhando:

I) Período de faturamento;
II) Discriminação dos serviços prestados e seus valores;
III) Relação dos eventos, incluindo numeração de chamado, horários de início e término;
IV) Eventos que ensejam descontos contratuais e seus respectivos valores;
V) Totais e subtotais.

6.2.22. Informar, nos relatórios fornecidos, detalhes sobre indisponibilidades ocorridas, incluindo data, período, causas, total de minutos e percentual de disponibilidade do período faturado.

6.2.23. Aplicar os devidos descontos em fatura por descumprimento do IMR, conforme previsto no contrato.

6.2.24. Apresentar mensalmente as faturas dos serviços prestados, acompanhadas da planilha de memória de cálculo definitiva validada pela CONTRATANTE.

6.2.25. Atender a reclamações ou pedidos de esclarecimento relacionados ao faturamento dos serviços contratados.

7. MODELO DE EXECUÇÃO DO OBJETO

7.1. A execução do objeto será conduzida de forma estratégica, visando garantir a plena implementação da solução contratada, conforme os requisitos previamente estabelecidos. A prestação dos serviços envolverá a implantação de um ambiente de segurança cibernética robusto, integrando tecnologias de Firewall de Nova Geração (NGFW), SD-WAN e IA Preditiva, conectividade segura e suporte técnico especializado, de modo a proporcionar alta disponibilidade, eficiência operacional e proteção integral dos ativos digitais da Prefeitura Municipal de Cáceres.

7.2. A prestação do serviço se dará em duas fases, garantindo uma implementação estruturada e um suporte contínuo para a operação da solução contratada, respeitando os prazos estipulados:

7.2.1. **Fase de Implantação** (até 60 dias após a assinatura do contrato):

7.2.1.1. Essa etapa compreende todas as atividades relacionadas à implementação física e lógica da solução. Inclui a instalação e configuração dos equipamentos, ativação dos links dedicados de internet, integração das unidades externas e praças municipais à infraestrutura de comunicação, além da capacitação técnica da equipe da Prefeitura. A fase será concluída com a entrega da documentação técnica detalhada (As Built) e a validação operacional dos serviços prestados.

7.2.1.2. A solução será implantada na sede da Prefeitura e em todas as unidades externas e praças municipais, garantindo conectividade segura e redundante para os serviços essenciais. Para viabilizar a execução adequada, serão instalados e configurados equipamentos de última geração, com capacidade para gerenciar múltiplas conexões simultâneas e otimizar o fluxo de dados.

7.2.1.3. A distribuição dos serviços seguirá a estrutura administrativa do município, contemplando unidades estratégicas vinculadas a diversas secretarias. O quantitativo necessário foi dimensionado considerando a demanda operacional de cada local, garantindo que todos os pontos críticos estejam devidamente atendidos. Entre as unidades contempladas, incluem-se:

7.2.1.3.1. **Unidades Centralizadas**

SECRETARIA	UNIDADE	LOCALIZAÇÃO	QUANTIDADE
SMEAE	SMEAE - PREFEITURA SEDE (COC)	https://maps.app.goo.gl/qTzbhDM8NCAEBxBf7	2
	UNIDADE CENTRALIZADA 1		1
	UNIDADE CENTRALIZADA 2		1
SMA	SMA - ALMOXARIFADO	https://maps.app.goo.gl/NiAhRcuDi3oF6Qvn9	1
	SMA - GUARDA MUNICIPAL	https://maps.app.goo.gl/hoMkt4EuyDL3BrFKA	1
SMAGRI	SMAGRI	https://maps.app.goo.gl/J1rDH3pp4oPSEfsj7	1
SMASC	SMASC - CCI	https://maps.app.goo.gl/j8UjTvfKLx4ypbPs5	1
SME	SME - CMEC	https://maps.app.goo.gl/ZUD6oU9HeMvLqXe89	1
SMIL	SMIL - GUARITA OBRAS	https://maps.app.goo.gl/PTWC8Lr3aGwXPxnP9	1
	SMIL - GUARITA PORTICO	https://maps.app.goo.gl/u39WX2UzVeVQQWS28	1

	SMIL - OFICINA	https://maps.app.goo.gl/wQmT4CxnPbdKZUYC9	1
TOTAL			**12**

7.2.1.3.2. **Unidades Descentralizadas**

SECRETARIA	UNIDADE	LOCALIZAÇÃO	QUANTIDADE
SMEAE	SMEAE - DEFESA CIVIL	https://maps.app.goo.gl/zYaMoX5jtfJ1VQ2h8	1
	UNIDADE DESCENTRALIZADA 1	-	1
SMA	SMA - ARQUIVO	https://maps.app.goo.gl/n6Jj6YzpqNfS8cHF7	1
	UNIDADE DESCENTRALIZADA 2	-	1
SMASC	SMASC - ALMOXARIFADO	https://maps.app.goo.gl/CZV2nUAkbYMhY6uq9	1
	SMASC - CASA BELBELITA	https://maps.app.goo.gl/DxddTbATc7X73Bns5	1
	SMASC - CASA DE PASSAGEM	https://maps.app.goo.gl/WrVThbciHZooSfgX6	1
	SMASC - CENTRO DE MULTIPLO USO	https://maps.app.goo.gl/Lz5UoPyGg42jrnUn8	1
	SMASC - CONSELHO TUTELAR	https://maps.app.goo.gl/tyQnNc8nTmMfQ3MW7	1
	SMASC - CRAS I	https://maps.app.goo.gl/xPiY5KnmduNnBgK49	1
	SMASC - CRAS II	https://maps.app.goo.gl/HPNPDMJ2U98R5tRm8	1
	SMASC - CREAS	https://maps.app.goo.gl/xoJqeaMyfF9Ds6g19	1
	SMASC - SAICA	https://maps.app.goo.gl/CCwLfifR6sWyhhdm7	1
	SMASC - GANHA TEMPO	https://maps.app.goo.gl/5AXCG6MYtbiF1gwV7	1
	UNIDADE DESCENTRALIZADA 3	-	1
SME	SME - SECRETARIA DE EDUCAÇÃO	https://maps.app.goo.gl/WbNKuCbpt1rDS5TE7	1
	SME - MERENDA	https://maps.app.goo.gl/byhFeQxucnAjkWfH8	1
	SME - CENTRO MUNICIPAL DE EDUCAÇÃO INFANTIL	https://maps.app.goo.gl/r9P3FHMDnqK3KTGUA	1
	SME - EM 16 DE MARÇO	https://goo.gl/maps/irEBgMynkLFUVdqDA	1
	SME - EM BRINCANDO E APRENDENDO	https://goo.gl/maps/qUYuASgJv5KN9z9v6	1
	SME - EM BURITI	https://goo.gl/maps/oJLMV4MMGaWkxdi7A	1
	SME - EM BUSCANDO O SABER	https://maps.app.goo.gl/52UwvjnQcLHDWQ7k6	1
	SME - EM CENTRO EDUCACIONAL DOM MÁXIMO BIENNÉS	https://goo.gl/maps/BDNwB6uZWrEapfWx5	1
	SME - EM DES. GABRIEL PINTO DE ARRUDA	https://goo.gl/maps/BDCMfHEfwrEELscN9	1
	SME - EM DR. JOSÉ RODRIGUES FONTES	https://maps.app.goo.gl/gN8iVN15FtGRnxbB9	1
	SME - EM DUQUE DE CAXIAS	https://goo.gl/maps/s5PAoUDUNHedzdks6	1
	SME - EM FAZENDO ARTE	https://maps.app.goo.gl/kTP6RNoQeYxuAfPNA	1
	SME - EM GARCÊS	https://goo.gl/maps/3J1HfZuFZ9v5WEcj9	1
	SME - EM GOTINHAS DO SABER	https://goo.gl/maps/mYM52pa2QkFA2j2C9	1
	SME - EM JARDIM GUANABARA	https://goo.gl/maps/Rfg8wh2T7iw4NrbP6	1

	SME - EM JARDIM PARAÍSO	https://goo.gl/maps/kkyMp6LAXieSyvPW9	1
	SME - EM NOVO ORIENTE	https://maps.app.goo.gl/4gacByZXhJ48UMvt5	1
	SME - EM PEQUENO SÁBIO	https://goo.gl/maps/EMEBFPffRm6Tb62a8	1
	SME - EM PROF. EDUARDO BENEVIDES LINDOTE	https://goo.gl/maps/Y43ifBkKTAwNN1U86	1
	SME - EM PROFª ISABEL CAMPOS	https://goo.gl/maps/1MgqjESG46yCxwe88	1
	SME - EM PROFA. ERENICE SIMÃO ALVARENGA	https://goo.gl/maps/yo4E1htCJ5EJYWE48	1
	SME - EM RAQUEL RAMÃO DA SILVA	https://goo.gl/maps/ke1dUMYCGWqwve6P8	1
	SME - EM SANTOS DUMONT	https://goo.gl/maps/uyBXsZNDDszodCxk6	1
	SME - EM TANCREDO NEVES	https://goo.gl/maps/fKVomd6j3LZtfjkS8	1
	SME - EM VILA IRENE	https://goo.gl/maps/aGdb2PV6NF3Yoxhe7	1
	SME - EM VILA REAL	https://goo.gl/maps/dfKNaDkEfK2V8YiJ8	1
	SME - EM VITÓRIA RÉGIA	https://goo.gl/maps/vP5EUrdTiHhhw13y6	1
	SME - EMEI FREI GRIGNION	https://goo.gl/maps/LmB1VSuePV8FtSXHA	1
	SME - EMEI IRENE COELHO CRUZ	https://goo.gl/maps/BiLhvdeg1tRmiuR37	1
	SME - EMEI MADRE MARIA ESTEVÃO	https://goo.gl/maps/kRXo9FN7eFvufAaV8	1
	SME - EMEI PROFESSORA DULSÂNGELA DE ALMEIDA SOUZA	https://maps.app.goo.gl/QZKQCN7SU9D2qwgd8	1
	SME- LIMOEIRO	https://goo.gl/maps/nrqaUDmiZV3xDpUN9	1
	SME - NOSSA SENHORA APARECIDA	https://goo.gl/maps/uYpxYHJzCmm6Qo1w8	1
	SME - PAULO FREIRE	https://maps.app.goo.gl/DE7sbzdMQVbaQXS77	1
	SME - PROFª LÉA MARIA LARA SILVA	https://maps.app.goo.gl/pjrMdwiU6wSSn3Uf7	1
	SME - PROVÍNCIA DE AREZZO	https://goo.gl/maps/NSNEbdrq1cjknywX8	1
	SME - ROÇA VELHA	https://goo.gl/maps/fGfEoY7trAGZhmS9A	1
	SME - SANTA CATARINA	https://goo.gl/maps/VzU6r8C8TVQJc3RM7	1
	SME - SANTO ANTÔNIO DO CARAMUJO	https://goo.gl/maps/ducAKNjzSQXECMHj9	1
	SME - SOTECO	https://maps.app.goo.gl/P32RY2iPJR7VLC9p7	1
	SME - TRANSPORTE EDUCAÇÃO	https://maps.app.goo.gl/cQumZ9jvaygvLQ159	1
	SME - EM UNIÃO	https://goo.gl/maps/zxtNZfD4YSyKrDVk8	1
	SME - CLARINÓPOLIS	https://goo.gl/maps/ducAKNjzSQXECMHj9	1
	SME - INFRAESTRUTURA EDUCAÇÃO	https://maps.app.goo.gl/b3bCUzB8qwz7vRd77	1
	SME - LARANJEIRA I	https://goo.gl/maps/jB1SZ3za3cdYev4a6	1
	SME - SÃO FRANCISCO	https://maps.app.goo.gl/sxzj1LsfxkFEX7Zy6	1
	UNIDADE DESCENTRALIZADA 4	-	1
	UNIDADE DESCENTRALIZADA 5	-	1

	UNIDADE DESCENTRALIZADA 6	-	1
	UNIDADE DESCENTRALIZADA 7	-	1
SMMADE	SMMADE	https://maps.app.goo.gl/zYaMoX5jtfJ1VQ2h8	1
	UNIDADE DESCENTRALIZADA 8	-	1
SMEL	SMEL - CIE	https://maps.app.goo.gl/Kkk4g4zUipLG7RDw6	1
	SMEL - DIDI PROFETA	https://maps.app.goo.gl/wUmbU83AgrRCFAjy6	1
	UNIDADE DESCENTRALIZADA 9	-	1
SMIL	SMIL - AEROPORTO	https://maps.app.goo.gl/N6nKAp5k4TpbGE1n6	1
	UNIDADE DESCENTRALIZADA 10	-	1
SMS	SMS - SECRETARIA DE SAUDE	https://maps.app.goo.gl/VWf4EYS5mnNdMk85A	1
	SMS - CAPS, AMBULATÓRIO DERMATOLÓGICO, LABORATORIO MUNICIPAL, ALMOXARIFADO, CMS	https://maps.app.goo.gl/3YsQdJ4PJUVqd6nG7	1
	SMS - CAPSI INFANTO JUVENIL	https://maps.app.goo.gl/NRE6n76fGEMAzeyy9	1
	SMS - CENTRO DE ESPECIALIDADES MEDICAS CEM	https://maps.app.goo.gl/zkjGjchEE1wsL14r8	1
	SMS - CENTRO DE SAUDE REFERENCIAL	https://maps.app.goo.gl/Z5MEaMJi68dU5hrG6	1
	SMS - CENTRO REAB DOM AQUINO CORREA CACERES CER II	https://maps.app.goo.gl/VhCQc4YayPyXp7sj8	1
	SMS - CEO	https://maps.app.goo.gl/wZMwZd1mfqVrkuRW6	1
	SMS - CTA CENTRO DE TESTAGEM E ACONSELHAMENTO SAE CACERES	https://maps.app.goo.gl/QPC3oTbJjodwapDV7	1
	SMS - FARMACIA BASICA DA SMS	https://maps.app.goo.gl/YwUSzHzPiKE5h3Vy8	1
	SMS - FROTAS	https://maps.app.goo.gl/UQZEQZxDpudbq1wH7	1
	SMS - POSTO DE SAUDE DA PAIOL	https://maps.app.goo.gl/PHsDSTgdLW1CdkacA	1
	SMS - POSTO DE SAUDE DE VILA APARECIDA	https://maps.app.goo.gl/uGRnxEjReD6jHpJ9A	1
	SMS - POSTO DE SAUDE DO LIMAO	https://maps.app.goo.gl/CfPip6ysDGqhiWmT6	1
	SMS - POSTO DE SAUDE HORIZONTE DOESTE	https://maps.app.goo.gl/6bkzEYMH7wQsigL49	1
	SMS - POSTO DE SAUDE LARANJEIRAS	https://maps.app.goo.gl/XpkQdasWsWE86U9q6?g_st=aw	1
	SMS - POSTO DE SAUDE PROF VERA LYGIA BALDO FACAO	https://maps.app.goo.gl/f6PfkXjMQjTudKqZ8	1
	SMS - POSTO DE SAUDE SADIA	https://maps.app.goo.gl/H29oLsoimParvAwv8	1
	SMS - UNID DE SAUDE DA FAMILIA VISTA ALEGRE	https://maps.app.goo.gl/FirXbqEx2srZf787A	1

	SMS - UNID SAUDE DA FAMILIA VITORIA REGIA	https://maps.app.goo.gl/mZmvrRyEijHAnTFY7	1
	SMS - UNIDADE BASICA DE SAUDE DR ADEMAR ROCHA DE OLIVEIRA CAVALHADA	https://maps.app.goo.gl/8gjpYWP87HBqcoZ46	1
	SMS - UNIDADE BASICA DE SAUDE JARDIM DAS OLIVEIRAS	https://maps.app.goo.gl/tT5o6Y7N38AVLUkZ9	1
	SMS - UNIDADE BASICA DE SAUDE SANTA ISABEL	https://maps.app.goo.gl/kUwep6ZQ8h7MucdX7	1
	SMS - UNIDADE DE SAUDE DA FAMILIA COHAB NOVA	https://maps.app.goo.gl/2dwof9LpsMAPALtM7	1
	SMS - UNIDADE DE SAUDE DA FAMILIA DO CAIC	https://maps.app.goo.gl/oJAf3xrRqWLe5Jev8	1
	SMS - UNIDADE DE SAUDE DA FAMILIA DO RODEIO	https://maps.app.goo.gl/2jADTBF6EXEvx9Ew6	1
	SMS - UNIDADE DE SAUDE DA FAMILIA JD PARAISO	https://maps.app.goo.gl/TdhriFPJ8nPUpFVx6	1
	SMS - UNIDADE DE SAUDE DA FAMILIA VILA REAL	https://maps.app.goo.gl/E1nPn9mTybVmcB267	1
	SMS - UNIDADE DE SAUDE SANTOS DUMONT	https://maps.app.goo.gl/oZuia8p4RaSbPKzP7	1
	SMS - UNIDADE DE SAUDE UNIVERSITÁRIO	https://maps.app.goo.gl/vYJEuN1ufGKzoEeK7	1
	SMS - UNIDADE SAUDE FAMILIA DO CARAMUJO	https://maps.app.goo.gl/zhXa1oX3UQzTwcHj9	1
	SMS - UNIDADE SAUDE FAMILIA JARDIM GUANABARA	https://maps.app.goo.gl/bRE93W32464phEPJ7	1
	SMS - UPA PRONTO ATENDIMENTO JOSE SOUTO FARIAS	https://maps.app.goo.gl/mgaRTmkRznLoMFrY7	1
	SMS - VIGILANCIA EM SAÚDE	https://maps.app.goo.gl/YJFGaUT4mc3VeFoV6	1
	UNIDADE DESCENTRALIZADA 11	-	1
	UNIDADE DESCENTRALIZADA 12	-	1
	UNIDADE DESCENTRALIZADA 13	-	1
	UNIDADE DESCENTRALIZADA 14	-	1
SMTC	SMTC	https://maps.app.goo.gl/sMPDMtU3poAP51LF7	1
	SMTC - CASA DAVERON	https://maps.app.goo.gl/fHqLcuW2X5nJCHBv6	1
	SMTC - BIBLIOTECA	https://maps.app.goo.gl/6cGeYMDAR1YMQXTX6	1
	SMTC - CLUBINHO 2000	https://maps.app.goo.gl/vaUxdTdcihpHVacH9	1
	SMTC - MUSEU	https://maps.app.goo.gl/kKvwGsx58CZmAqDfA	1
	UNIDADE DESCENTRALIZADA 15	-	1
TOTAL			**115**

7.2.1.3.3. **Praças Públicas**

SECRETARIA	PRAÇA	LOCALIZAÇÃO	QUANTIDADE
SMEAE	SMEAE - AROLDO FANAIA	https://maps.app.goo.gl/8J86ycmMgagCRjCb6	1
	SMEAE - COHAB VELHA	https://maps.app.goo.gl/ExPmvCxJtbZ6Tsxk6	1
	SMEAE - PRAÇA BENJAMIN CONSTANT	https://goo.gl/maps/Bp9fHEKnFKQ4shkB7	1
	SMEAE - PRAÇA CARAMUJO	https://maps.app.goo.gl/7h6GapqJ9cnAkc8T7	1
	SMEAE - PRAÇA CIDADE ALTA	https://goo.gl/maps/MxXmDgoFqVtZdNex8	1
	SMEAE - PRAÇA CIDADE NOVA	https://maps.app.goo.gl/W8wgiTyN45SChQ9d8	1
	SMEAE - PRAÇA COHAB NOVA	https://goo.gl/maps/7xNnbDpDas9VePnN9	1
	SMEAE - PRAÇA DA FEIRA - CENTRO	https://goo.gl/maps/sjqGYtg7KatQcwcZ8	1
	SMEAE - PRAÇA DNER - BOMBEIROS	https://goo.gl/maps/3tgxS4Uz2pnsdPxH9	1
	SMEAE - PRAÇA DO GERALDÃO	https://goo.gl/maps/iGDeEFGjFZqQ3ct79	1
	SMEAE - PRAÇA DO MONTE VERDE	https://goo.gl/maps/VDYK2HWXctL7tgmV6	1
	SMEAE - PRAÇA DOM MÁXIMO	https://goo.gl/maps/om21uh8nLLWQdJs1A	1
	SMEAE - PRAÇA DUQUE DE CAXIAS - CENTRO	https://goo.gl/maps/sjqGYtg7KatQcwcZ8	1
	SMEAE - PRAÇA HORIZONTE D'OESTE	https://maps.app.goo.gl/yNFf1xADWNWK6NkZ6	1
	SMEAE - PRAÇA JARDIM AEROPORTO	https://goo.gl/maps/W6oEg6qd6pwi7MwF9	1
	SMEAE - PRAÇA JARDIM DA OLIVEIRA (EMPA)	https://maps.app.goo.gl/Z1yuZWjrLsYP5jwP7	1
	SMEAE - PRAÇA JARDIM PARAISO	https://maps.app.goo.gl/pYiSUbjpqciUhE3N9	1
	SMEAE - PRAÇA JARDIM SÃO LUIZ	https://maps.app.goo.gl/nBF5xryfXZoMWjUQ9	1
	SMEAE - PRAÇA JARDIM UNIVERSITÁRIO III	https://goo.gl/maps/ofActSaScSGdXz4R6	1
	SMEAE - PRAÇA JOSÉ DE ANCHIETA	https://goo.gl/maps/A8WHwD7BX6NUWhJT6	1
	SMEAE - PRAÇA JUNCO	https://maps.app.goo.gl/qXAReBWJ7BQRPpkM9	1
	SMEAE - PRAÇA MAJOR JOÃO CARLOS	https://goo.gl/maps/Qcwdn4CXJdT5VCWQ6	1
	SMEAE - PRAÇA MEDEIROS	https://goo.gl/maps/HUThKqHzuPa6ABpEA	1
	SMEAE - PRAÇA NOVA ERA (CAMPO)	https://maps.app.goo.gl/YQKX7SBhzB9dcjcj9	1
	SMEAE - PRAÇA PANTANAL	https://goo.gl/maps/AUKWENW5iR2gENDT7	1
	SMEAE - PRAÇA RESIDENCIAL ANA PAULA	https://goo.gl/maps/pA2tyTfhq8jqo5Fk7	1
	SMEAE - PRAÇA SANTA CRUZ	https://maps.app.goo.gl/KFsn7XrjbpDGFV1X9	1
	SMEAE - PRAÇA SANTA ISABEL	https://maps.app.goo.gl/TBJYXELoqvGd7Lkm9	1

	SMEAE - PRAÇA SANTO ANTONIO	https://maps.app.goo.gl/Tu2hhrXUFw4rSABn6	1
	SMEAE - PRAÇA SÃO JORGE	https://goo.gl/maps/MxXmDgoFqVtZdNex8	1
	SMEAE - PRAÇA SÃO LOURENÇO (CAMPO)	https://maps.app.goo.gl/bouowePQbhfCzuRm7	1
	SMEAE - PRAÇA SÃO MIGUEL	https://goo.gl/maps/TeYnV6RyQdD3d4Zo8	1
	SMEAE - PRAÇA VALTER FIDELIS - VILA REAL	https://maps.app.goo.gl/PyeiqkA6niDZH3hE9	1
	SMEAE - PRAÇA VILA APARECIDA	https://maps.app.goo.gl/Cjpoxp8VnhRTkBMa9	1
	SMEAE - PRAÇA VILA REAL	https://maps.app.goo.gl/Yp8X21VytfkPPvgw6	1
	SMEAE - PRAÇA VITÓRIA RÉGIA	https://goo.gl/maps/mJXKjDVQASbukgY37	1
	SMEAE - RODOVIÁRIA	https://maps.app.goo.gl/8LyQniCzZ74f3oCC7	1
	SMEAE - SADIA	https://maps.app.goo.gl/tc1GB5cCztjYFNtm9	1
	PRAÇA MUNICIPAL 1		1
	PRAÇA MUNICIPAL 2		1
	PRAÇA MUNICIPAL 3		1
	PRAÇA MUNICIPAL 4		1
SMTC	SMTC - PALCO DE EVENTOS SEMATUR	https://maps.app.goo.gl/WsUtv8cTtAgazbeP9	1
	SMTC - PRAÇA BARÃO	https://maps.app.goo.gl/vP3qT3xGyzzbTkVf8	1
	PRAÇA MUNICIPAL 5		1
	PRAÇA MUNICIPAL 6		1
TOTAL			**46**

7.2.2. **Fase de Prestação de Serviço Mensal** (até 180 meses após a assinatura do contrato):

7.2.2.1. Após a implantação, será iniciada a fase de operação contínua da solução, garantindo a manutenção preventiva e corretiva dos equipamentos, suporte técnico especializado, monitoramento em tempo real da infraestrutura de segurança cibernética e otimização do tráfego de rede com a tecnologia SD-WAN. Essa fase inclui a prestação de serviços de segurança cibernética baseada em Inteligência Artificial Preditiva, bem como a consultoria contínua para aprimoramento da política de segurança da informação do município.

7.3. Além da estruturação física, a execução do contrato incluirá a implantação de links dedicados de internet para garantir alta disponibilidade, com redundância de ASN e rotas distintas, estabilidade para os serviços administrativos e operacionais e alternativa de contingência para evitar interrupções nos serviços

7.4. O serviço de Link de Internet para as localidades que serão contempladas com WI-FI Social deverá ser implantado impreterivelmente em até 30 (trinta) dias a partir da ordem de serviço emitida pelo Gestor do Contrato.

7.5. Para o **Lote único** a CONTRATADA deverá cumprir os eventos descritos na tabela a seguir, respeitando os prazos máximos estabelecidos

MARCOS DIA	PRAZOS MÁXIMOS (EM DIAS)	EVENTO	RESPONSÁVEL

Assinado por 2 pessoas: WELLYNGTON DE BARROS INÁCIO e JEREMIAS PEREIRA LEITE

D0		Assinatura do contrato entre o CONTRATANTE e a empresa licitante vencedora.	CONTRATANTE e a CONTRATADA
D1		Emissão da Ordem de Serviço pelo CONTRATANTE	CONTRATANTE
D2	D1+2	Entrega do projeto executivo	CONTRATADA
D3	D2+2	Aprovação do projeto executivo	CONTRATANTE
D4	D1+15	Entrega dos link de Internet e WI-FI nas praças, contemplando toda a solução de segurança de SDWAN e NGFW	CONTRATADA
D5	D4+3	Emissão do Termo de Recebimento provisório, para início da conferência do serviço entregue dos Links de Internet das praças	CONTRATANTE
D6	D5+5	Emissão do Termo de Recebimento Definitivo, autorização para emissão de faturamento e início do período de execução dos serviços dos Links de Internet das praças	CONTRATANTE
D7	D1+60	Conclusão da entrega, instalação e configuração dos equipamentos, capacitação e operacionalização de todos os links de comunicação, Firewall, IA Preditiva, sensores de cibersegurança, SDWAN, NGFW	CONTRATADA
D8	D7+3	Emissão do Termo de Recebimento provisório, para início da conferência do serviço entregue.	CONTRATANTE
D9	D8+5	Emissão do Termo de Recebimento Definitivo, autorização para emissão de faturamento e início do período de execução dos serviços de links de comunicação, Firewall, Sensores de Cibersegurança, SDWAN, NGFW	CONTRATANTE

7.6. A instalação da solução será realizada por uma empresa homologada e credenciada, com compromisso solidário ao fabricante, garantindo a fluidez da implantação dentro do prazo estipulado no edital. Para assegurar a operacionalidade da solução, serão promovidas capacitações técnicas para a equipe da Prefeitura, visando aprimorar a gestão e monitoramento dos sistemas implementados.

7.7. O modelo de execução do objeto visa garantir não apenas a segurança cibernética e a conectividade da administração pública municipal, mas também a eficiência na prestação de serviços essenciais à população, promovendo inovação, resiliência e modernização tecnológica.

8. MODELO DE GESTÃO DO CONTRATO

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

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

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

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

8.5. Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

8.6. **Fiscalização**

8.6.1. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput), nos termos do Decreto nº 665 de 09 de outubro de 2024.

8.6.2. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

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

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

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

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

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

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

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

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

8.6.5. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

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

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

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

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

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

9. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

9.1. Forma de Acompanhamento da Garantia e Níveis de Serviço

9.1.1. Para cumprir com os níveis de disponibilidade a prestadora de serviços deve trabalhar com duas variáveis principais: o MTBF (Tempo médio entre falhas) da solução, e o MTTR (Tempo médio de reparação de falhas). Para aumentar a disponibilidade deve-se aumentar o MTBF e diminuir o MTTR, de forma que o sistema apresente falhas com menor frequência e que estas sejam recuperadas mais rapidamente.

Abaixo estão listados os valores de disponibilidade mensal para cada Item deste Termo:

LOTE	ITEM	SERVIÇO	DISPONIBILIDADE
1 (ÚNICO)	1	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)	99,8%
	2	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	99,8%
	3	Serviço de Link dedicado de Acesso à internet, bloco /29 e Banda Mínima de Acesso Garantida de 500Mbps (Alta Disponibilidade) SEDE (Dois Link de ASN e Rota Diferentes)	99,8%
	4 5	Serviço de Link de acesso à Internet Sites Remotos, aplica-se ao WIFI Social	99,2%

9.2. Nas planilhas abaixo estão detalhados todos os indicadores destinados à aferição dos níveis mínimos de serviço da contratação pretendida. Na apuração dos indicadores poderão ser confrontados os dados da solução de gerenciamento da CONTRATADA e do sistema de monitoramento da CONTRATANTE.

MÉTRICA 1 - DISPONIBILIDADE (IMR-01)	
Indicador de Qualidade	Índice de Disponibilidade.
Métrica	Indicador é calculado com a seguinte forma: **IDM=[(To - Ti)/To]*100** Onde: IDM = índice de disponibilidade mensal do LINK em % To = período de operação (um mês) em minutos. Ti = somatório dos tempos de inoperância durante o período de operação (1 mês) em minutos. No caso de inoperância reincidente num período inferior a 3 horas, contado a partir do restabelecimento do link da última inoperância, considerar-se-á como tempo de indisponibilidade do enlace o início da primeira inoperância até o final da última inoperância, quando o link estiver totalmente operacional. Os tempos de inoperância serão os tempos em que os links apresentarem problemas que serão obtidos dos chamados abertos no sistema de abertura de chamados técnicos (Trouble Ticket) e os tempos de indisponibilidade computados pela violação do indicador de Retardo. Somente serão desconsiderados os tempos de inoperância causados por manutenções programadas com o CONTRATANTE, ressalvados, contudo, os casos fortuitos e de força maior.
Periodicidade de Aferição	Mensal
Limiar de Qualidade	Vide Item 9.1 - Forma de Acompanhamento da Garantia e Níveis de Serviço
Pontos de Controle	A CONTRATADA realizará, por meio da sua solução de gerenciamento, a coleta e o armazenamento de informações a respeito de todos os serviços pelo tempo de duração do contrato.
Relatórios de Níveis de Serviço	A CONTRATADA deverá disponibilizar mensalmente à CONTRATANTE, relatórios com os índices apurados, totalizados e apresentados mensalmente por serviço. Nos relatórios citados deverão ser apresentados: o número do ticket, tempo de indisponibilidade (horas e minutos), o tempo de interrupções programadas, o tempo de interrupções de responsabilidade da CONTRATANTE. A CONTRATADA deverá disponibilizar, quando demandada pelo CONTRATANTE, relatório detalhando os tempos de falhas (com hora de início e fim da inoperância), minutos excedentes ao prazo máximo para reparo e disponibilidade no período (mês) e motivo(s) da(s) indisponibilidade(s) apurada(s). Após análise do fiscal técnico, poderá ser desconsiderado do período de inoperância, o tempo decorrente da impossibilidade da CONTRATADA acessar os equipamentos nas instalações da CONTRATANTE, comprovando a CONTRATADA que o problema estava nas dependências da CONTRATANTE.

MÉTRICA 2 - TAXA DE ERRO (IMR-02)	
Indicador de Qualidade	Percentual de erros nos enlaces.
Métrica	Indicador é calculado com a seguinte fórmula: **TER = (QEQ / TTQ)* 100** Sendo: TER = Indicador de taxa de erro; TTQ = Quantidade total de quadros enviados ou recebidos em um determinado período; QEQ = Quantidade de erros identificados em um determinado período. Para efeito de mensuração desta métrica utiliza-se as seguintes considerações: • Quadro é a unidade de transferência de dados na camada de enlace do modelo OSI, ou

	seja, o frame Ethernet; • Os erros devem ser reportados pelo roteador da CONTRATADA utilizado na conexão com a rede da CONTRATANTE; • Serão considerados os erros em ambas as interfaces de ingresso e egresso no roteador da CONTRATADA.
Periodicidade de Aferição	Esta métrica deverá ser aferida, ininterruptamente, em intervalos de 5 minutos.
Limiar de Qualidade	0,5%
Pontos de Controle	O período utilizado no cálculo da métrica e, quando for o caso, o período considerado como indisponível será o do intervalo entre as aferições

MÉTRICA 3 - LATÊNCIA (IMR-03)	
Indicador de Qualidade	Tempo de latência de ida e volta do pacote através do link contratado
Métrica	A latência deve mensurar o tempo do trajeto de ida-e-volta (RTT - round trip time) de um pacote do tipo ICMP com tamanho de 1000 bytes. Para efeito de mensuração desta métrica utiliza-se as seguintes considerações: • Para os links Internet, as medições de latência devem ser feitas entre o Roteador Internet ou Appliance SD-WAN e o primeiro roteador da CONTATADA na Internet. • Pacote é a unidade de transferência de dados na camada de redes do modelo OSI, ou seja os datagramas TCP, UDP, ICMP e ARP; • O envio de pacotes para obtenção dos quantitativos utilizados no cálculo desta métrica deve ocorrer entre dois pontos distintos e remotos, um localizado no segmento de rede da CONTRATANTE onde estiver conectado o roteador da CONTRATADA, e outro localizado em segmento de rede de terceiros que estejam ligados a Internet por meio da rede da mesma CONTRATADA, ou em segmento de rede utilizado para troca de tráfego entre de operadoras de acesso à Internet (Pontos de Troca de Tráfego), podendo inclusive, tratar-se dos roteadores de borda da CONTRATADA conectados aos segmentos aqui mencionados. Serão desconsiderados os períodos em que os valores mensurados ultrapassem o limite aceitável desta métrica, caso a volume médio de utilização do link no mesmo período seja superior a 80% da velocidade do respectivo enlace.
Mínimo aceitável	Links de Internet: 65 ms
Periodicidade Aferição	Esta métrica deverá ser aferida, ininterruptamente, em intervalos de 5 minutos. O período utilizado no cálculo da métrica será o período do intervalo entre as aferições

MÉTRICA 4 – PERDA DE PACOTES (IMR-04)	
Indicador de Qualidade	Percentual de perda de pacotes IP ao longo da rede da CONTRATADA em um determinado período.
Métrica	Indicador é calculado com a seguinte forma: **TPP = (QPP / QTP)* 100** Sendo: TPP = Indicador de perda de pacotes QTP = Quantidade total de pacotes enviados ou recebidos em um determinado período QPP = Quantidade de pacotes perdidos em um determinado período Para efeito de mensuração desta métrica utiliza-se as seguintes considerações: • Pacote é a unidade de transferência de dados na camada de redes do modelo OSI, ou seja os datagramas TCP, UDP, ICMP e ARP; • O envio de pacotes para obtenção dos quantitativos utilizados no cálculo desta métrica deve

	ocorrer entre dois pontos distintos e remotos, um localizado no segmento de rede da CONTRATANTE onde estiver conectado o roteador da CONTRATADA, e outro localizado em segmento de rede de terceiros que estejam ligados a Internet por meio da rede da mesma CONTRATADA, ou em segmento de rede utilizado para troca de tráfego entre de operadoras de acesso à Internet (Pontos de Troca de Tráfego), podendo inclusive, tratar-se dos roteadores de borda da CONTRATADA conectados aos segmentos aqui mencionados. Serão desconsiderados os períodos em que os valores mensurados ultrapassem o limite aceitável desta métrica, caso a volume médio de utilização do link no mesmo período seja superior a 80% da velocidade do respectivo enlace.
Máximo aceitável	3% de perda
Periodicidade Aferição	Esta métrica deverá ser aferida, ininterruptamente, em intervalos de 5 minutos. O período utilizado no cálculo da métrica será o período do intervalo entre as aferições.

MÉTRICA 5 – PRAZO PARA ALTERAÇÃO DE CONFIGURAÇÃO DOS EQUIPAMENTOS SOLICITADOS PELO CONTRATANTE	
Indicador de Qualidade	Prazo, em horas, para a contratada alterar a configuração dos equipamentos solicitada pelo CONTRATANTE.
Métrica	Apuração mensal do tempo que a contratada executa e apresente uma alteração na configuração de equipamentos, a partir do momento do registro da solicitação de alteração da configuração na base de dados relativa à solução de gerenciamento do Provedor e de comparação com o valor do Limiar de Qualidade desta tabela. **PA = Taa – Tsa** onde: PA = Prazo de alteração da configuração de equipamentos Taa = Instante da aceitação pela da alteração Tsa = Instante da solicitação da alteração
Periodicidade de Aferição	Mensal
Limiar de Qualidade	Prazo máximo: 48 horas após a solicitação de alteração da configuração pela CONTRATANTE. Em caso de agendamento pelo CONTRATANTE este prazo ficará suspenso.
Pontos de Controle	De acordo com os registros na Central de Atendimento.
Relatórios de Níveis de Serviço	A CONTRATADA deverá disponibilizar mensalmente à CONTRATANTE, relatórios com os índices apurados, totalizados e apresentados mensalmente por serviço. Nos relatórios citados deverão ser apresentados: o número do ticket, tempo de indisponibilidade (horas e minutos), o tempo de interrupções programadas, o tempo de interrupções de responsabilidade do CONTRATANTE.
Descontos	Para cada 1 (uma) hora acima do Prazo para Alteração de Configuração de Equipamentos (PAC), será implicado à contratada desconto correspondente a 2,0% (dois por cento), calculado sobre o valor mensal do circuito afetado. O referido desconto deverá ser retratado nos relatórios de prestação dos serviços, junto ao faturamento apresentados mensalmente por enlace.

9.3. **Recebimento do Objeto**

9.3.1. A emissão do Termo de Recebimento Definitivo é o marco inicial da efetiva prestação do serviço contratado, nas condições em que foram definidas pela CONTRATANTE neste instrumento.

9.3.2. Os serviços serão recebidos provisoriamente, no prazo de até 3 (três) dias, pelos fiscais técnico e administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. (Art. 140, I, a , da Lei nº 14.133 e Arts. 22, X e 23, X do Decreto nº 11.246, de 2022);

9.3.2.1. O prazo da disposição acima será contado do recebimento de comunicação de cobrança oriunda do contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga;

9.3.2.2. O fiscal técnico do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico. (Art. 22, X, Decreto nº 11.246, de 2022);

9.3.2.3. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo. (Art. 23, X, Decreto nº 11.246, de 2022)

9.3.2.4. O fiscal setorial do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo.

9.3.3. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato:

9.3.3.1. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

9.3.3.2. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório. (Art. 119 c/c art. 140 da Lei nº 14133, de 2021)

9.3.3.3. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

9.3.3.4. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

9.3.4. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

9.3.5. Os serviços serão recebidos definitivamente no prazo de 7(sete) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

9.3.5.1. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento (art. 21, VIII, Decreto nº 11.246, de 2022).

9.3.5.2. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções;

9.3.5.3. Emitir Termo Circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e

9.3.5.4. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

9.3.5.5. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão

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

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

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

9.3.9. Será permitido a emissão do Termo de Recebimento Definitivo, de forma individual, para serviço de Link de Internet WI-FI nas praças.

9.4. **Sanções Administrativas e Procedimentos Para Retenção ou Glosa no Pagamento**

9.4.1. **Descontos Aplicáveis em Caso de Descumprimento do IMR**

9.4.1.1. Durante a vigência do contrato poderão ser aplicados descontos na fatura, em caso de eventual descumprimento do Instrumento de Medição de Resultado (IMR), a título de glosa, limitando-se cada um ao limite do valor mensal do contrato.

9.4.1.2. Para fins de cálculo do valor do desconto de glosa contratual serão observados os critérios do **Item 9.1. Forma de Acompanhamento da Garantia e Níveis de Serviço**, nos termos do Instrumento de Medição de Resultado - IMR, aplicando os descontos correspondentes à disponibilidade mensal aferida, conforme a tabela abaixo:

LOTE	ITEM	SERVIÇO	FAIXA ATÉ 24H	FAIXA 24H ATÉ 48H	FAIXA ACIMA 48 H

1 (ÚNICO)	1	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN Sede (Alta Disponibilidade)	0,01% /min	0,02% /min	0,02% /min + multa moratória prevista no subitem 9.4.3.1
	2	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	0,01% /min	0,02% /min	0,02% /min + multa moratória prevista no subitem 9.4.3.1
	3	Serviço de Link dedicado de Acesso à internet, bloco /29 e Banda Mínima de Acesso Garantida de 500Mbps (Alta Disponibilidade) SEDE (Dois Link de ASN e Rota Diferentes)	0,01% /min	0,02% /min	0,02% /min + multa moratória prevista no subitem 9.4.3.1
	4 5	Serviço de Link de acesso à Internet Sites Remotos, aplica-se ao WIFI Social	0,009% /min	0,025% /min	0,025% /min

9.4.1.3. Em caso do não cumprimento da Métrica 5 do IMR o desconto será aplicado conforme abaixo:

MÉTRICA	FAIXA ATÉ 48H	FAIXA 48H ATÉ 72H	FAIXA ACIMA 72H
MÉTRICA 5 - Solicitação de alteração de configuração dos equipamentos - Prazo 48 horas	2,0% /hora	2,5% /hora	2,5% /hora + multa moratória prevista no subitem 9.4.3.1

9.4.1.4. Nos cálculos de desconto, em que a faixa for ultrapassada, todo o cálculo deverá ser feito na faixa posterior.

9.4.1.5. O valor do desconto será aplicado no mês imediatamente subsequente ao mês em que ocorreram os fatos causadores dos descontos, tendo como base o valor vigente do acesso do mês da ocorrência da interrupção.

9.4.1.6. Os descontos não poderão ultrapassar o valor do item do serviço prestado.

9.4.2. **Sanções Aplicáveis Fase de Instalação**

9.4.2.1. O atraso injustificado no cumprimento do objeto sujeitará a CONTRATADA às seguintes penalidades:

- Advertência;
- Multa moratória no valor de 1% do valor anual do contrato para o enlace, por dia de atraso, limitado a 10 dias, pelo atraso injustificado na entrega do projeto executivo, podendo ser adotadas medidas administrativas para rescisão contratual por inexecução total da obrigação. Entende-se por enlace/circuito como qualquer link Internet nos Sites Remotos e na Sede do CONTRATANTE;
- Multa moratória no valor de 1% do valor anual do contrato para o enlace, por dia de atraso, limitado a 30 dias, pelo atraso injustificado na instalação e configuração dos enlaces contratados, podendo ser adotadas medidas administrativas para rescisão contratual por inexecução total da obrigação. Entende-se por enlace/circuito como qualquer link Internet nos Sites Remotos e na Sede do CONTRATANTE.

9.4.3. **Sanções Aplicáveis Fase de Operação**

9.4.3.1. Caso a CONTRATADA ultrapasse a última faixa dos descontos aplicáveis, além da aplicação dos descontos, será imposta multa moratória de 1% do valor mensal do serviço não atendido no IMR, limitada a 10 dias.

9.4.3.2. A não manutenção das condições de habilitação da empresa ao longo da execução do contrato poderá ensejar sua rescisão unilateral pelo CONTRATANTE, após devido processo administrativo, assegurados o contraditório e a ampla defesa, além da aplicação de multa de 30% sobre o valor da parcela inadimplida.

9.4.3.3. A multa poderá ser aplicada cumulativamente com outras penalidades previstas no contrato ou na legislação vigente.

9.4.3.4. A inexecução total ou parcial do contrato poderá resultar em rescisão, nos termos deste instrumento e dos arts. 155 e 156 da Lei nº 14.133/21, incluindo indenização por eventuais prejuízos causados ao CONTRATANTE.

9.4.3.5. A aplicação das sanções será realizada mediante processo administrativo específico, assegurados o contraditório e a ampla defesa, com comunicação formal da penalidade à CONTRATADA.

9.4.3.5.1. A critério da autoridade competente, com base nos princípios da proporcionalidade e razoabilidade, as penalidades poderão ser atenuadas ou relevadas mediante comprovação fundamentada, desde que requeridas por escrito no prazo de 5 dias úteis a contar da notificação.

9.4.3.6. O atraso no pagamento de multas será corrigido pelo IPCA, divulgado pelo IBGE.

9.4.3.7. O CONTRATANTE registrará no SICAF todas as penalidades aplicadas à CONTRATADA.

9.4.4. **Sanções Administrativas**

9.4.4.1. Comete infração administrativa, nos termos da Lei nº 14.133/2021, a CONTRATADA que:

9.4.4.1.1. Der causa à inexecução parcial ou total do contrato, especialmente quando causar grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

9.4.4.1.2. Deixar de entregar documentação exigida no certame ou para a contratação;

9.4.4.1.3. Não manter a proposta, salvo por fato superveniente devidamente justificado;

9.4.4.1.4. Ensejar o retardamento injustificado da execução do objeto;

9.4.4.1.5. Apresentar declaração ou documentação falsa durante a licitação ou execução do contrato;

9.4.4.1.6. Fraudar a licitação ou praticar atos fraudulentos na execução do contrato;

9.4.4.1.7. Adotar comportamento inidôneo, praticar fraudes ou atos ilícitos visando frustrar os objetivos da licitação;

9.4.4.1.8. Praticar ato lesivo conforme o art. 5º da Lei nº 12.846/2013.

9.4.4.2. Pela inexecução total ou parcial do contrato, poderão ser aplicadas as seguintes sanções:

9.4.4.2.1. Advertência, quando não se justificar penalidade mais grave;

9.4.4.2.2. Multa, variando entre 0,5% e 30% do valor do contrato, conforme art. 155 da Lei nº 14.133/2021;

9.4.4.2.3. Impedimento de licitar e contratar, pelo prazo máximo de 3 anos, nos casos de infrações previstas nos incisos II a VII do art. 155 da Lei nº 14.133/2021, quando não for cabível penalidade mais severa;

9.4.4.2.4. Declaração de inidoneidade para licitar e contratar, pelo prazo de 3 a 6 anos, nos casos das infrações previstas nos incisos VIII a XII do art. 155 da Lei nº 14.133/2021, bem como naquelas previstas nos incisos II a VII que justifiquem penalidade mais grave.

9.4.4.3. Na aplicação das sanções, serão considerados:

9.4.4.3.1. A natureza e a gravidade da infração;

9.4.4.3.2. As peculiaridades do caso concreto;

9.4.4.3.3. Circunstâncias agravantes ou atenuantes;

9.4.4.3.4. Os danos causados à Administração Pública;

9.4.4.3.5. A existência de programa de integridade na empresa.

9.4.4.4. A sanção prevista no item 9.4.4.2.4. será precedida de análise jurídica observando as seguintes regras:

9.4.4.4.1. Quando aplicada por órgão do Poder Executivo, será de competência exclusiva de Ministro de Estado, Secretário Estadual ou Municipal, ou da autoridade máxima da autarquia ou fundação responsável;

9.4.4.4.2. Quando aplicada por órgãos dos Poderes Legislativo e Judiciário, Ministério Público ou Defensoria Pública, será de competência exclusiva de autoridade equivalente às referidas no item 9.4.4.4.1, conforme regulamento.

9.4.4.5. As sanções previstas nos itens 9.4.4.2.1., 9.4.4.2.3. e 9.4.4.2.4. poderão ser aplicadas cumulativamente com a prevista no item 9.4.4.2.2.

9.4.4.6. Se o valor das multas e indenizações exceder eventuais créditos da CONTRATADA junto à Administração, a diferença será descontada da garantia prestada ou cobrada judicialmente.

9.4.4.7. A aplicação das sanções previstas nos itens 9.4.4.2.1., 9.4.4.2.2., 9.4.4.2.3. e 9.4.4.2.4. não exclui a obrigação de reparação integral dos danos causados à Administração.

9.4.4.8. A defesa quanto à aplicação das sanções previstas no item 9.4.4.2.2., poderá ser apresentada no prazo de 15 dias úteis a contar da intimação.

9.4.4.9. Para a aplicação das sanções previstas nos itens 9.4.4.2.3. e 9.4.4.2.4. será instaurado processo de responsabilização conduzido por comissão composta por, no mínimo, dois servidores estáveis, garantindo-se o direito à defesa no prazo de 15 dias úteis, nos termos do art. 158 da Lei nº 14.133/2021.

9.5. **Liquidação**

9.5.1. O faturamento mensal terá início somente após a emissão do Termo de Recebimento Definitivo, não sendo contada a fase de implantação do Item.

9.5.2. Para o serviço de Link de Internet nas localidades praças será permitido o faturamento após o Termo de Recebimento Definitivo de cada uma das unidades.

9.5.3. Durante a fase de prestação mensal a CONTRATANTE deverá validar minuciosamente as planilhas de memória de cálculo fornecidas pela CONTRATADA a fim de apurar os valores a serem faturados e os descontos aplicados, às planilhas de memória de cálculo deverão ser enviadas até o quinto dia após o fechamento do período de apuração.

9.5.4. CONTRATADA poderá optar por emitir a nota fiscal/fatura após a validação da memória de cálculo pela CONTRATANTE que terá prazo de 5 dias úteis para validação.

9.5.5. A CONTRATADA poderá emitir a nota fiscal/fatura com descontos apurados pela CONTRATADA e em caso de discordância dos descontos apurados por parte da CONTRATANTE, os descontos poderão ser aplicados na fatura do mês posterior.

9.5.6. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de 5 dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 6º, §1º do Decreto nº089/2024 .

9.5.6.1. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

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

a) o prazo de validade;
b) a data da emissão;
c) os dados do contrato e do órgão contratante;
d) o período respectivo de execução do contrato;
e) os descontos com mês referência;
f) o valor a pagar;
g) dados bancários para o recebimento do montante; e
h) eventual destaque do valor de retenções tributárias cabíveis.

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

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

9.5.10. A Administração deverá realizar consulta ao SICAF para:

a) verificar a manutenção das condições de habilitação exigidas no edital;
b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

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

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

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

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

9.6. **Prazo de pagamento**

9.6.1. O pagamento será efetuado no prazo de até 15 (quinze) dias úteis contados da finalização da liquidação da despesa, nos termos do art. 6º, §1º do Decreto nº089/2024.

9.7. **Forma de pagamento**

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

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

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

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

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

9.8. **Reajuste**

9.8.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do Orçamento.

9.8.2. Após o interregno de um ano do orçamento estimado, mediante pedido expresso do contratado, os preços iniciais serão reajustados pelo contratante, mediante a aplicação do índice IPCA ou outro que reflita a inflação e seja mais vantajoso à Administração Pública Municipal, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

10. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

10.1. **Forma de seleção e critério de julgamento da proposta**

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

10.1.2. A presente aquisição adotará como regime de execução por preço unitário, a ser contratado mediante licitação, na modalidade Pregão Eletrônico, com lances abertos com intervalos mínimos entre lances de R$ 0,01 (um centavo) com valor de referência sigilos, levando em conta o objetivo da promoção de uma maior disputa entre os licitantes, com resultados satisfatórios para as empresas e o órgão público, considerando que o valor ultimado pelo mercado é variável, já que o referido objeto depende de tecnologias cada vez mais avançadas.

10.1.3. A presente licitação será julgada pelo critério de menor valor global, tendo em vista que o objeto consiste na contratação de empresa especializada para prestação de serviços de segurança cibernética com Inteligência Artificial Preditiva, garantindo alta disponibilidade, segurança, eficiência e sustentabilidade no atendimento às demandas do Município de Cáceres. Considerando a natureza integrada dos serviços, que envolvem soluções tecnológicas interdependentes, como conectividade segura, monitoramento preditivo, suporte técnico especializado e infraestrutura crítica de proteção de dados, a execução por um único fornecedor assegura a compatibilidade entre os componentes, a uniformidade dos padrões técnicos, a continuidade do serviço e a racionalização dos custos operacionais. Assim, a adoção do julgamento por valor global mostra-se técnica e economicamente mais vantajosa para a Administração Pública, promovendo a otimização dos recursos públicos e garantindo a eficiência na implementação da solução proposta.

10.1.4. É lícito o agrupamento em lotes de itens a serem contratados por meio de pregão, desde que possuam mesma natureza e que guardem relação entre si (Acórdão TCU nº 5.260/2011 – 1ª Câmara);

10.2. Exigências de habilitação

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

10.2.1.1. **Habilitação jurídica**

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

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

10.2.1.1.3. **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;

10.2.1.1.4. **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;

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

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

10.2.1.1.7. **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

10.2.1.1.8. **Sociedade cooperativa:** ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

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

10.2.1.2. **Habilitação fiscal, social e trabalhista**

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

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

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

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

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

10.2.1.2.6. Prova de regularidade com a Fazenda [Estadual/Distrital] e [Municipal/Distrital] do domicílio e sede do fornecedor, relativa à atividade em cujo exercício contrata e concorre;

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

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

10.2.1.3. **Qualificação Econômico-Financeira**

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

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

10.2.1.3.3. Índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), comprovados mediante a apresentação pelo licitante de balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais e obtidos pela aplicação das seguintes fórmulas:

I) Liquidez Geral (LG) = (Ativo Circulante + Realizável a Longo Prazo) / (Passivo Circulante + Passivo Não Circulante);

II) Solvência Geral (SG)= (Ativo Total) / (Passivo Circulante +Passivo não Circulante); e

III) Liquidez Corrente (LC) = (Ativo Circulante) / (Passivo Circulante).

10.2.1.3.4. 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] OU [patrimônio líquido mínimo] de 5% do valor total estimado do item.

10.2.1.4. **Qualificação Econômico-Financeira. (Justificativa)**

10.2.1.4.1. Ressalta-se que as exigências de habilitação relativas à qualificação econômico-financeira acima previstas e de acordo com o artigo 69 da Lei nº 14.133/21, têm a finalidade de viabilizar a aferição da situação financeira dos licitantes pela Administração. Dessa forma, será possível verificar se o interessado reúne condições indispensáveis para suportar as despesas relativas à satisfatória execução do objeto contratual, como dado objetivo de comprovação da qualificação econômico-financeira dos licitantes e para efeito de garantia ao adimplemento do contrato a ser ulteriormente celebrado, visando assegurar que a empresa contratada possa cumprir suas obrigações de curto e longo prazo, cumprindo as obrigações previstas no Edital e contrato, por se tratar de registro de preço o índice de 5% do valor de cada item, a Administração escolheu este valor por entender ser o mínimo a exigir de uma empresa para se manter um contrato, dentro de um nível de segurança e equilíbrio. Ademais, com o objetivo de não restringir o universo de concorrentes, resolveu não exigir valor acima da unidade. Ante o exposto, a exigência do Edital nada mais fez que traduzir em critérios objetivos o disposto no art. 37, XXI, da Constituição Federal, ademais, os índices escolhidos foram democráticos, na medida em que estabelecem um “mínimo” de segurança na contratação. Desta forma, atende plenamente a Lei Federal nº 14.133/21 limitando-se a exigir índices que demonstrem a capacidade financeira dos licitantes com vistas ao compromisso a ser assumido para plena execução do contrato.

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

10.2.1.4.3. O balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos. (Lei nº 14.133, de 2021, art. 69, §6º)

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

10.2.1.5. **Qualificação Técnica**

10.2.1.5.1. Será exigida a comprovação da capacidade técnico-operacional da licitante, mediante a apresentação de atestados emitidos por pessoa jurídica de direito público ou privado, que comprovem a execução de serviços compatíveis em características, quantidades e prazos com o objeto deste contrato, incluindo o fornecimento e a instalação de equipamentos correlatos aos ofertados, bem como a prestação de serviços de instalação, configuração e suporte técnico. A licitante deverá comprovar, no mínimo, experiência prévia correspondente a **30% (trinta por cento)** do quantitativo estimado do **item 1 – Solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)**, considerado de maior relevância técnica para a consecução do objeto. Tal exigência encontra amparo no inciso III do art. 67 da Lei nº 14.133/2021, sendo justificada pela complexidade e especificidade do objeto, que demanda experiência comprovada na execução de soluções integradas de segurança cibernética, com destaque para componentes baseados em Inteligência Artificial Preditiva, visando garantir a eficiência, a continuidade dos serviços e a mitigação de riscos operacionais, em observância aos princípios da legalidade, razoabilidade, eficiência e interesse público.

10.2.1.5.1.1. A comprovação poderá ser feita por meio de um ou mais atestados que, **conjuntamente**, demonstrem a experiência da licitante de forma compatível com o objeto contratado, especialmente no que se refere ao atendimento do percentual mínimo de 30% do item de maior relevância técnica, vedada a exigência de comprovação integral do quantitativo estimado.

10.2.1.5.1.2. Os atestados deverão conter, no mínimo:

10.2.1.5.1.2.1. Identificação completa do emitente, com razão social, CNPJ, endereço e dados de contato;

10.2.1.5.1.2.2. Descrição detalhada dos serviços executados, permitindo aferir a compatibilidade em características com o objeto, incluindo fornecimento e instalação de equipamentos, implantação de soluções de segurança cibernética, configuração e suporte técnico;

10.2.1.5.1.2.3. Indicação de que os serviços foram executados em quantidades compatíveis, com destaque para a experiência mínima equivalente a 30% do quantitativo estimado do item de maior relevância técnica, conforme avaliação da Administração, vedada a exigência de quantidades idênticas ou desproporcionais, nos termos do art. 67, §§ 1º, 2º e 5º, da Lei nº 14.133/2021;

10.2.1.5.1.2.4. Período de execução dos serviços, com datas de início e de conclusão ou, se for o caso, vigência atual, para fins de comprovação da compatibilidade em prazos;

10.2.1.5.1.2.5. Declaração de que os serviços foram prestados de forma satisfatória, assinada por representante legal da entidade emitente;

10.2.1.5.1.2.6. Assinatura e identificação do responsável pela emissão, com nome legível, cargo e meios de contato.

10.2.1.5.2. A licitante deve comprovar que dispõe de, no mínimo, dois (02) técnicos certificados pelo fabricante da solução proposta, os quais participarão diretamente da execução dos serviços previstos.

10.2.1.5.3. As certificações devem ser reconhecidas pelo fabricante e estar atualizadas, garantindo conhecimento técnico adequado às demandas do projeto.

10.2.1.5.4. O fornecedor deve fornecer todas as informações e documentos necessários para validar a legitimidade dos atestados apresentados, incluindo:

- Cópia do contrato que deu origem à prestação dos serviços mencionados nos atestados;
- Endereço atual da contratante que emitiu o atestado;
- Local onde os serviços foram executados;
- Outros documentos complementares, se solicitados pela Administração.

10.2.1.5.5. A licitante deve comprovar experiência em projetos de complexidade e escopo semelhantes, preferencialmente na área pública ou em ambientes corporativos de grande porte, apresentando histórico de projetos realizados com soluções NGFW, SD-WAN e links de redundância.

10.2.1.5.6. A licitante deverá demonstrar a capacidade técnica necessária para atender aos requisitos específicos do projeto, incluindo:

- Disponibilidade de suporte técnico especializado durante todo o período contratual;
- Experiência em integrar soluções de segurança em redes heterogêneas e complexas;
- Conhecimento comprovado em tecnologias de alta disponibilidade, criptografia e gestão de redes com políticas de segurança.

10.2.1.5.7. Sempre que solicitado pela Administração, a licitante deverá apresentar documentação adicional que comprove a qualificação técnica e a capacidade operacional para executar o objeto contratado, garantindo transparência e segurança no processo de contratação.

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

11.1. O custo estimado da contratação possui caráter sigiloso e será tornado público apenas e imediatamente após o julgamento das propostas nos termos do Art. 9º do Decreto municipal 240/23.

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

12. DA PARTICIPAÇÃO DE CONSORCIO

12.1. Trata-se da vedação da participação de consórcios quanto ao registro de preços para CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA PRESTAÇÃO DE SERVIÇOS DE SEGURANÇA CIBERNÉTICA COM INTELIGÊNCIA ARTIFICIAL PREDITIVA, GARANTINDO ALTA DISPONIBILIDADE, SEGURANÇA, EFICIÊNCIA E SUSTENTABILIDADE NO ATENDIMENTO ÀS DEMANDAS DO MUNICÍPIO DE CÁCERES.

12.2. Art. 14 da Lei 14.133/21, conferiu a discricionaridade à Administração para permitir ou vetar a formação de consórcio em certame licitatório. É sabido que, em regra, a formação de consórcio é admitida quando o objeto a ser licitado envolve questões de alta complexidade técnica ou de relevante vulto, em que, isoladamente, as empresas não teriam condições de suprir os requisitos de habilitação do edital.

12.3. Tratando-se do objeto em questão, a ausência de consórcio não trará prejuízos à competitividade do certame por se tratar de um registro de preços, de serviços comuns, a ser executado ao longo de 12 (doze) meses em sua totalidade ou não, que não demandam especialidades diferentes entre as empresas, as quais poderiam impedir à execução dos serviços por uma única empresa. É nítido, neste caso também que, a reunião de empesas em consórcio, ao invés de estabelecer uma disputa entre as empresas, as mesmas formalizariam acordo para eliminar a competição caso estivessem reunidas em consórcio.

12.4. Diante de todo o exposto e, considerando que existem diversas empresas com capacidade para fornecer os serviços a serem contratados facilmente comprovados através do número de cotações inseridas no processo, fica vedada à participação de consórcios na licitação.

13. ADESÃO A ATA DE REGISTRO DE PREÇO

13.1. Em conformidade com a Lei nº 14.133/2021, a Lei nº 14.770/2023 e demais regulamentos aplicáveis, a adesão à Ata de Registro de Preços (ARP) configura-se como mecanismo de cooperação interfederativa, baseado na manifestação de interesse mútuo entre os entes públicos. Tal procedimento visa proporcionar maior eficiência administrativa e econômica, especialmente diante das dificuldades enfrentadas por órgãos e entidades para realizar processos licitatórios frequentes, seja por limitações de pessoal, infraestrutura ou outras razões justificáveis.

13.2. A adesão à ARP pelos demais entes federados será viabilizada desde que respeitados os limites quantitativos previstos no instrumento convocatório e nas legislações mencionadas, bem como observadas as condições estabelecidas neste Termo de Referência. A formalização da adesão deverá ocorrer mediante solicitação formal do ente interessado, acompanhada da anuência do órgão gerenciador e da CONTRATADA, conforme exigido pela legislação vigente.

13.3. A adesão não poderá resultar em prejuízo ao fornecimento ou à prestação dos serviços destinados ao órgão gerenciador e demais participantes da ARP. Caso o volume decorrente das adesões comprometa o atendimento das quantidades inicialmente previstas, a CONTRATADA deverá priorizar o fornecimento ao órgão gerenciador e aos participantes originais, conforme os prazos e condições estabelecidos neste instrumento.

13.4. Os entes federados que aderirem à ARP assumem integral responsabilidade pela gestão e fiscalização dos contratos celebrados diretamente com a CONTRATADA, sem qualquer interferência ou solidariedade do órgão gerenciador. Caberá ao ente aderente zelar pelo cumprimento das obrigações pactuadas, inclusive no que se refere às condições de pagamento, prazos de entrega e demais cláusulas contratuais.

13.5. O órgão gerenciador poderá, a qualquer tempo, solicitar relatórios à CONTRATADA para acompanhar as adesões realizadas, garantindo o cumprimento dos limites quantitativos e demais disposições legais aplicáveis. Eventuais irregularidades deverão ser comunicadas ao órgão gerenciador, que adotará as providências cabíveis em conformidade com a legislação vigente.

14. ADEQUAÇÃO ORÇAMENTÁRIA

14.1. As despesas oriundas da presente aquisição correrão por conta de todas as dotações vigentes, conforme especificado pelas Secretarias no momento do empenho.

ÓRGÃO/ UNIDADE	FUNCIONAL-PROGRAMÁTICA	NATUREZA DA DESPESA	FONTE DE RECURSOS	SECRETARIA
021301	04.129.1002.2109	3.3.90.	1.1.500	SMFAZ
021201	27.122.1009.2107	3.3.90.	1.1.500	SMFAZ
020501	10.122.1003.2021	33.90.	1.1.500	SMS
020502	10.304.1003.2030	33.90.	1.600	SMS
020901	04.121.1002.2071	3.3.90.	1.1.500	SMPLAN
020901	04.127.1002.2071	3.3.90.	1.1.500	SMPLAN
021101	08.122.1008.2074	3.3.90.	1.1.500	SMASC
021102	08.244.1008.2082	3.3.90.	4.1.660	SMASC
021102	08.244.1008.2083	3.3.90.	1.1.500	SMASC
021102	08.244.1008.2083	3.3.90.	4.1.660	SMASC
021102	08.244.1008.2086	3.3.90.	4.1.660	SMASC
021102	08.244.1008.2091	3.3.90.	1.1.500	SMASC
020601	12.122.1004.2046	3.3.90.	2.1.500	SME
020401	04.123.1002.2019	3.3.90.	1.1.500	SMFIN
020701	15.122.1005.2061	3.3.90.	1.1.500	SMIL
021401	18.122.1010.2111	3.3.90.	1.1.500	SMMADE
021001	20.122.1007.2072	3.3.90.	1.1.500	SMAGRI
020101	04.122.1002.2004	3.3.90.	1.1.500	GABINETE
020201	04.122.1002.2012	3.3.90.	1.1.500	SMEAE
020801	04.122.1006.2066	3.3.90.	1.1.500	SMTC
021201	27.122.1009.2.107	3.3.90.	1.1.500	SMEL
020201	04 126 1002 2014 0000	3.3.90	1.1.500	SMEAE
020201	04 122 1002 2012 0000	3.3.90	1.1.500	SMEAE
020301	04 122 1002 2018 0000	3.3.90	1.1.500	SMA

Cáceres-MT, 13 de junho 2025.

WELLYNGTON DE BARROS MACIEL
Coordenador de Informações Sistêmicas e Tecnologia de Informação em Substituição
Decreto nº. 392 de 11 de junho de 2025

JEREMIAS PEREIRA LEITE
Secretário Municipal Especial de Assuntos Estratégicos

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: 7BE7-17D2-35C8-081E

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

✓ WELLYNGTON DE BARROS MACIEL (CPF 004.XXX.XXX-60) em 13/06/2025 10:01:32 GMT-04:00
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

✓ JEREMIAS PEREIRA LEITE (CPF 045.XXX.XXX-72) em 13/06/2025 10:02:03 GMT-04:00
Papel: Parte
Emitido por: AC SOLUTI Multipla v5 << AC SOLUTI v5 << Autoridade Certificadora Raiz Brasileira v5 (Assinatura ICP-Brasil)

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

https://caceres.1doc.com.br/verificacao/7BE7-17D2-35C8-081E

De: Igor O. - SMA-CPL

Para: SMA-CPL - Comissão Permanente de Licitação

Data: 13/06/2025 às 14:57:24

Senhor Secretário,

Segue em anexo edital retificado de abertura referente ao pregão eletrônico 15/2025 formatado, com o número 90015/2025 no compras.gov.br, abertura prevista para o dia 03/07/2025.

Atenciosamente;

_

Igor de Souza Oliveira
Pregoeiro Oficial

Anexos:

EDITAL_RETIFICADO_PE_15_2025_FIREWALL.pdf

Assinado digitalmente (anexos) por:

Assinante	Data	Assinatura	
Jeremias Pereira Leite	13/06/2025 15:24:20	ICP-Brasil	JEREMIAS PEREIRA LEITE CPF 045.XXX.XXX-72

Para verificar as assinaturas, acesse **https://caceres.1doc.com.br/verificacao/** e informe o código: **2E87-4C08-ED11-C406**