

Protocolo 1.943/2025

De: Gabinete do Prefeito- PREFEITURA MUNICIPAL DE CÁCERES

Para: DCAT - DEPARTAMENTO DE COMUNICAÇÃO ADMINISTRATIVA E TELEFONIA

Data: 05/12/2025 às 10:50:41

Setores (CC):

DCAT

Setores envolvidos:

GAB-VER, DAL, DCAT

1.07-Resposta a Requerimento

Entrada*:

Site

Senhor Presidente:

Acusamos o recebimento do Ofício n.º 1287/2025 – SL/CMC, por meio do qual essa Colenda Câmara encaminha-nos o Requerimento n.º 0278/2025, de autoria do ilustre vereador, Cézare Pastorello (PT), em resposta, vimos encaminhar o Ofício n.º 2.290/2025-GP/PMC e documentos anexos.

Respeitosamente,

Ivanilde Melo.

Anexos:

1_APOSTILAMENTO_DO_CONT_104_2025_outubro_2025_.pdf

CONTEUDO_DESPACHO_4_SMEAE_CTI.pdf

CT_ADM_104_02025_PGM.pdf

em_34C7D88059D2E321B6628991_proc_administrativo_processo_licitatorio_029_2025_parte_1.pdf

em_34C7D88059D2E321B6628991_proc_administrativo_processo_licitatorio_029_2025_parte_10.pdf

em_34C7D88059D2E321B6628991_proc_administrativo_processo_licitatorio_029_2025_parte_11.pdf

em_34C7D88059D2E321B6628991_proc_administrativo_processo_licitatorio_029_2025_parte_12.pdf

em_34C7D88059D2E321B6628991_proc_administrativo_processo_licitatorio_029_2025_parte_13.pdf

em_34C7D88059D2E321B6628991_proc_administrativo_processo_licitatorio_029_2025_parte_14.pdf

em_34C7D88059D2E321B6628991_proc_administrativo_processo_licitatorio_029_2025_parte_15.pdf

em_34C7D88059D2E321B6628991_proc_administrativo_processo_licitatorio_029_2025_parte_16.pdf

em_34C7D88059D2E321B6628991_proc_administrativo_processo_licitatorio_029_2025_parte_17.pdf

em_34C7D88059D2E321B6628991_proc_administrativo_processo_licitatorio_029_2025_parte_18.pdf

em_34C7D88059D2E321B6628991_proc_administrativo_processo_licitatorio_029_2025_parte_19.pdf

em_34C7D88059D2E321B6628991_proc_administrativo_processo_licitatorio_029_2025_parte_2.pdf

em_34C7D88059D2E321B6628991_proc_administrativo_processo_licitatorio_029_2025_parte_20.pdf
em_34C7D88059D2E321B6628991_proc_administrativo_processo_licitatorio_029_2025_parte_21.pdf
em_34C7D88059D2E321B6628991_proc_administrativo_processo_licitatorio_029_2025_parte_22.pdf
em_34C7D88059D2E321B6628991_proc_administrativo_processo_licitatorio_029_2025_parte_3.pdf
em_34C7D88059D2E321B6628991_proc_administrativo_processo_licitatorio_029_2025_parte_4.pdf
em_34C7D88059D2E321B6628991_proc_administrativo_processo_licitatorio_029_2025_parte_5.pdf
em_34C7D88059D2E321B6628991_proc_administrativo_processo_licitatorio_029_2025_parte_6.pdf
em_34C7D88059D2E321B6628991_proc_administrativo_processo_licitatorio_029_2025_parte_7.pdf
em_34C7D88059D2E321B6628991_proc_administrativo_processo_licitatorio_029_2025_parte_8.pdf
em_34C7D88059D2E321B6628991_proc_administrativo_processo_licitatorio_029_2025_parte_9.pdf
EQUIPAMENTOS_SD_WAN.jpeg
FIREWALL_1.jpeg
FIREWALL_2.jpeg
FIREWALL_3_INTERFACE.jpeg
IMAGEM_LINK_DE_INTERNET_1.jpeg
IMAGEM_LINK_DE_INTERNET_2.jpeg
Impressao_RELATORIO.pdf
Oficio_n_2_290_2025_GP.pdf
PORTARIA_N_587_25_Fiscal_do_Contrato_de_n_104_2025_SMEAE.pdf
PROTECAO_INTELIGENCIA_CIBERNETICA.pdf
RELATORIO_EXS_PAG_2024.pdf
RELATORIO_PAG_EXS_2025.pdf
RELATORIO_PEDROSA.pdf
RELATORIO_PEDROSA_2022.pdf
RELATORIO_PEDROSA_2023.pdf
RELATORIO_REDE_2023.pdf
RELATORIO_REDE_EXS_PAG_2023.pdf



ESTADO DE MATO GROSSO
PREFEITURA MUNICIPAL DE CÁCERES
PROCURADORIA GERAL DO MUNICÍPIO

PRIMEIRO TERMO DE APOSTILAMENTO DO CONTRATO ADMINISTRATIVO N°. 104/2025-PGM

CONTRATANTE: Prefeitura Municipal de Cáceres/MT, através da **SECRETARIA MUNICIPAL ESPECIAL DE ASSUNTOS ESTRATÉGICOS**.

CONTRATADA: SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA

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.

Em conformidade com o Memorando 29.499/2025, inserido na plataforma 1DOC, fica necessário o Apostilamento do Contrato epigrafado, **RETIFICANDO A CLÁUSULA QUARTA - DA VIGÊNCIA CONTRATUAL** do contrato administrativo n°. 104/2025-PGM, em plena conformidade com o artigo 136 da Lei n° 14.133/2021, uma vez que o ato não caracteriza alteração do contrato podendo então, ser realizados por simples Apostilamento, dispensada a celebração de termo aditivo.

ONDE SE LÊ:

4. CLÁUSULA QUARTA - DA VIGÊNCIA CONTRATUAL

4.1. A vigência do presente instrumento vigorará pelo período de 12 (doze) meses, com início na data de 05/09/2025 e encerramento em 04/09/2026, prorrogável na forma dos artigos 106 e 107 da Lei n° 14.133 de 2021.

4.2. 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.

4.3. O contratado não tem direito subjetivo à prorrogação contratual.

4.4. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

4.5. 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.

4.6. 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.



ESTADO DE MATO GROSSO
PREFEITURA MUNICIPAL DE CÁCERES
PROCURADORIA GERAL DO MUNICÍPIO

LEIA-SE:

4. CLÁUSULA QUARTA - DA VIGÊNCIA CONTRATUAL

4.1. A vigência do presente instrumento vigorará pelo período de 12 (doze) meses, com início na data de 05/09/2025 e encerramento em 04/09/2026, prorrogável na forma do artigo 114 da Lei nº 14.133/2021.

4.2. 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.

4.3. O contratado não tem direito subjetivo à prorrogação contratual.

4.4. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

4.5. 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.

4.6. 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.

Art. 2º Permanecem íntegras e ratificadas as demais cláusulas anteriormente pactuadas no Contrato Administrativo nº 104/2025-PGM, naquilo que não contrariem o presente termo.

Cáceres/MT, 13 de outubro de 2025.

RUBENS MACEDO
SECRETÁRIO MUNICIPAL ESPECIAL DE ASSUNTOS ESTRATÉGICOS
CONTRATANTE





Protocolo 27.112/2025

Código: 612.717.647.669.080.538

De: **Wellyngton de Barros Maciel** Setor: **SMEAE - CTI - Coordenação de Tecnologia da Informação**

Despacho: **4- 27.112/2025**

Para: **GAB- ED - Edson Flávio AC: Edson Flávio Santos**

Assunto: **Requerimento Câmara**

Cáceres/MT, 04 de Dezembro de 2025

Para:

[Gleison da Silva Souza](#)

mensageiro.gleison@caceres.mt.leg.br

CPF 004.XXX.XXX-02

Cáceres/MT, . . /

Prezado,

Em atendimento ao Requerimento apresentado pelo vereador Cézare Pastorello, seguem as informações solicitadas:

- **ITEM 1 – SUBITENS “a” a “d”**

Documentos anexados no Despacho nº 2.

- **ITEM 2 – SUBITEM “a”**

Foram anexadas fotografias da instalação realizada na sede da Prefeitura. Esclarece-se que houve atraso no processo inicial, razão pela qual foi solicitada **Notificação Oficial**, devidamente anexada.

Registra-se, ainda, que:

Neste primeiro momento, está sendo executada **a migração do firewall e a implementação das políticas de segurança**, a fim de garantir pleno funcionamento da solução. Após a conclusão dessa etapa, será iniciado o atendimento às **unidades externas urbanas e do campo**, mediante instalação dos **dois links de internet** e dos **equipamentos SD-WAN**. Na sequência, serão contempladas as **praças municipais**, conforme previsto nos documentos técnicos.

Todos os elementos estão devidamente especificados no **ETP** e no **TR**.

- **ITEM 2 – SUBITEM “b”**

Portaria anexada.

- **ITEM 2 – SUBITEM “c”**

Esclarece-se que **nenhuma Nota Fiscal foi emitida até o presente momento**, uma vez que **a implantação total ainda não foi concluída**. Conforme disposto no **item 7.5 do Termo de Referência**, a emissão da Nota Fiscal somente ocorrerá após o **Termo de Recebimento Definitivo**.

- **ITEM 3 – SUBITEM “a” e “b”**

Foi anexado o **Relatório Anual das empresas prestadoras de serviço**.

- **ITEM 3 – SUBITEM “c” — JUSTIFICATIVA TÉCNICA DETALHADA**

- 1. Considerações Iniciais**

Registra-se, previamente, a manifestação do vereador Cézare Pastorello, que pontuou:

“A transparência na aplicação destes recursos é essencial para garantir que o dinheiro público, que poderia estar sendo investido em saúde, educação ou infraestrutura nos bairros periféricos, não esteja sendo escoado através de contratos de tecnologia superdimensionados.”

A Administração reconhece a pertinência da preocupação, especialmente diante dos princípios da **transparência, economicidade, eficiência e supremacia do interesse público**. Todavia, com fundamento técnico, jurídico e documental, esclarece-se que **a contratação não é superdimensionada e não se afasta das prioridades públicas**, sendo direcionada majoritariamente às áreas essenciais de:

- ? saúde,
- ? educação,
- ? unidades descentralizadas urbanas e do campo,
- ? atendimento direto ao cidadão.

- 2. Situação Fática que Originou a Demanda**

O Estudo Técnico Preliminar constatou que a infraestrutura preexistente encontrava-se **em estado crítico**, apresentando riscos significativos à segurança, continuidade e confiabilidade dos serviços públicos.

Entre os principais fatores que motivaram a contratação, destacam-se:

- ? **Equipamento obsoleto**: o firewall Sophos, adquirido em 2018, encontrava-se com hardware defasado e **licença expirada em 2025**, não sendo mais possível renová-la por tratar-se de produto **descontinuado pelo fabricante**.
- ? **Falta de capacitação**: a equipe técnica municipal **não possuía treinamento** para configurar e operar recursos avançados do equipamento anterior.
- ? **Conectividade precária**: inúmeras unidades — especialmente **saúde e educação** — utilizavam **conexões via satélite ou antena por rádio**, com alta instabilidade, perda de dados e morosidade nos atendimentos.
- ? **Ausência de integração segura**: não havia políticas robustas de proteção de dados, segregação de redes ou arquitetura de segurança compatível com a estrutura municipal.
- ? **Indisponibilidade recorrente**: as falhas afetavam diretamente o atendimento à população urbana e rural, prejudicando serviços essenciais como prontuário eletrônico, matrícula, sistemas contábeis, assistenciais e educacionais.

Por esta razão, a modernização não apenas se tornou necessária, como absolutamente indispensável para garantir continuidade, integridade e segurança das informações públicas.

3. Comunicado Oficial – Circular nº 38.967/2025

Em **19/11/2025**, foi expedida a **Circular nº 38.967/2025**, encaminhada a **todos os setores da Prefeitura**, incluindo:

- ? todas as escolas urbanas e do campo;
- ? unidades de saúde urbanas e rurais;
- ? secretarias municipais.

O documento informou oficialmente o **início da implantação e migração da nova solução de segurança e conectividade**, alertando quanto à possibilidade de **oscilações temporárias e/ou inconsistências momentâneas** no acesso aos sistemas corporativos, em razão dos ajustes inerentes à fase de transição tecnológica.

Tal medida evidencia boa-fé administrativa, transparência e planejamento prévio, assegurando que todos os setores fossem cientificados sobre impactos temporários decorrentes da migração.

4. Fundamentação Técnica do Investimento

A contratação contempla solução completa composta por **NGFW de última geração**, infraestrutura SD-WAN, redundância de links e recursos avançados de segurança, cobrindo **172 unidades**.

Principais componentes:

- ? inspeção profunda de tráfego (DPI);
- ? inteligência artificial preditiva;
- ? proteção contra ataques **Zero Day**;
- ? VPN segura entre todas as unidades;
- ? segmentação de rede conforme diretrizes da **LGPD**;
- ? Wi-Fi Social controlado em escolas, unidades e praças;
- ? links de fibra com contingência de **fibra ou 4G/5G**.

Trecho de alta relevância:

“A PMC enfrenta desafios cada vez mais complexos no âmbito da segurança cibernética, sendo indispensável a ampliação da infraestrutura vigente, proporcionando maior capacidade de processamento, resiliência e escalabilidade.” (ETP)

5. Justificativa Econômica e Proporcionalidade do Custo

O valor contratado decorre da necessidade de atender uma rede municipal ampla e distribuída, incluindo:

- ? **344 links** (primários e secundários);
- ? **172 equipamentos SD-WAN** em comodato;

- ? **2 firewalls corporativos** em cluster;
- ? suporte especializado 24/7;
- ? atualizações de segurança;
- ? substituição integral em caso de falhas;
- ? políticas, consultorias técnicas e licenças completas.

Trecho de alta relevância:

“Não haverá aquisição de equipamentos; todos os ativos serão fornecidos em comodato, com manutenção e substituição garantidas.”
(TR)

6. Atendimento às Áreas Mencionadas pelo Vereador

Com base nos documentos técnicos, constata-se que o projeto:

- ? **não concorre com saúde e educação – viabiliza saúde e educação;**
- ? atende diretamente escolas, unidades de saúde urbanas e do campo;
- ? amplia conectividade nos bairros por meio do **Wi-Fi Social;**
- ? reduz indisponibilidades e falhas em sistemas essenciais;
- ? fortalece a proteção de dados sensíveis (LGPD);
- ? melhora o atendimento à população urbana e rural.

Trecho de máxima relevância:

“A expansão e modernização da solução configura-se como investimento estratégico, plenamente alinhado às necessidades institucionais da Prefeitura de Cáceres, reforçando a proteção dos interesses públicos, a integridade das informações e a continuidade das atividades administrativas.” (ETP)

7. Conclusão

Diante de todo o exposto, resta demonstrado que:

- ? o investimento é **necessário, proporcional e tecnicamente fundamentado;**
- ? observa rigorosamente os princípios da **legalidade, eficiência, economicidade e interesse público;**
- ? é direcionado prioritariamente às áreas essenciais de **saúde, educação e cidadania;**
- ? foi previamente comunicado por meio da **Circular nº 38.967/2025;**
- ? não se trata de solução superdimensionada, mas sim de **adequação tecnológica imprescindível ao funcionamento da estrutura pública municipal.**

Permanecemos à disposição para quaisquer esclarecimentos adicionais.

Atenciosamente,

Wellyngton de Barros Maciel

Gerente de Hardware

Decreto nº 117 de 25 de fevereiro de 2022

Coordenação de Tecnologia da Informação

Secretaria Municipal Especial de Assuntos Estratégicos Município de Cáceres – MT

Prefeitura de Cáceres - Av. Brasil, nº119, Jardim Celeste, CEP 78210-906 Protocolo Geral - Expediente 07h30 às 11h30 e das 13h30 às 17h30 Responsáveis pelo Protocolo Geral Marileide Lopes Paraba Campos Simone Cardoso de Mello • 1Doc • www.1doc.com.br

Impresso em 05/12/2025 10:37:58 por Ivanilde Barbosa de Melo - Recepcionista (matrícula 2332-1)

1Doc



ESTADO DE MATO GROSSO
PREFEITURA MUNICIPAL DE CÁCERES
PROCURADORIA GERAL DO MUNICÍPIO

CONTRATO ADMINISTRATIVO Nº. 104/2025-PGM

Contrato que entre si celebram o **MUNICÍPIO DE CÁCERES-MT**, através da **SECRETARIA MUNICIPAL ESPECIAL DE ASSUNTOS ESTRATÉGICOS** e a empresa **SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA**, para o fim que especifica.

O **MUNICÍPIO DE CÁCERES - MT**, pessoa jurídica de direito público, inscrito no CNPJ sob nº 03.214.145/0001-83 com sede no COC – Centro Operacional de Cáceres, que compreende complexo administrativo da Prefeitura Municipal, sito a Avenida Brasil, Nº. 119, neste ato representado pelo secretário municipal especial de assuntos estratégicos, Sr. **JEREMIAS PEREIRA LEITE**, doravante denominado **CONTRATANTE**, e de outro lado, a empresa **SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA**, inscrita no CNPJ nº 44.122.701/0001-79, neste ato representada pela, Sra. **ROSELANE GONZALEZ DO NASCIMENTO ALMEIDA**, doravante denominada simplesmente **CONTRATADA**, tem certo, justo e acordado o seguinte, considerando a autorização para contratação dos serviços de que trata o **Processo Administrativo Licitatório nº 029/2025**, mediante **PREGÃO ELETRÔNICO Nº 015/2025**, originando a **Ata de Registro de Preço nº 155/2025**, número da licitação no compras.gov.br 90015/2025, considerando, também, o Termo de Referência nº **001/2025**, e, por fim, a solicitação contida no **Memorando nº 29.499/2025**, resolvem celebrar o presente Contrato, em observância às disposições da Lei nº 14.133, de 1º de abril de 2021 e demais legislação aplicável, amparado nos princípios da finalidade pública e princípio da continuidade do serviço público e, supletivamente, pelos princípios da teoria geral dos contratos e pelas disposições de direito privado e, ainda, pelas cláusulas e condições a seguir delineadas:

1. CLÁUSULA PRIMEIRA - 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.

1.2. DESCRIÇÃO DO OBJETO:

ITEM	DESCRIÇÃO	UNID.	QUANT.	VALOR UNITÁRIO (R\$)	VALOR TOTAL (R\$)
01	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)	Serviço	2076	564,99	1.172.919,24
02	Serviço de Segurança	Serviço	24	8.999,99	215.999,76



ESTADO DE MATO GROSSO
PREFEITURA MUNICIPAL DE CÁCERES
PROCURADORIA GERAL DO MUNICÍPIO

	cibernética, baseado em Inteligência Artificial Preditiva				
03	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	24	3.399,99	81.599,76
04	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 150Mbps Sites Remotos (Fibra Óptica)	Serviço	2052	214,99	441.159,48
05	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G)	Serviço	2052	164,66	337.882,32
06	Implantação da Solução	Serviço	1	269.999,99	269.999,99
07	Capacitação especializada da equipe com emissão de certificação	Treinamento	1	8.416,67	8.416,67
08	Consultoria Política de Segurança	Serviço	1	35.666,67	35.666,67
TOTAL: R\$ 2.563.643,89					

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.



ESTADO DE MATO GROSSO
PREFEITURA MUNICIPAL DE CÁCERES
PROCURADORIA GERAL DO MUNICÍPIO

2. CLÁUSULA SEGUNDA - DO VALOR

2.1. A contratante pagará à contratada pelo fornecimento do objeto ora contratado o **VALOR TOTAL DE R\$ 2.563.643,89 (Dois Milhões e Quinhentos e Sessenta e Três Mil e Seiscentos e Quarenta e Três Reais e Oitenta e Nove Centavos)**, a ser empenhado gradativamente conforme necessidade e disponibilidade financeira e orçamentária da Secretaria Contratante.

2.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, bem como taxas de licenciamento, administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

3. CLÁUSULA TERCEIRA - DOS RECURSOS ORÇAMENTÁRIOS

3.1. As despesas decorrentes da execução do presente Contrato correrão à conta de recursos próprios do orçamento vigente, alocado sob a classificação funcional:

ÓRGÃO/ UNIDADE	FUNCIONAL- PROGRAMÁTICA	NATUREZA DA DESPESA	FONTE DE RECURSOS	SECRETARIA
020501	10.122.1003.2021	33.90.	1.1.500	SMS
020502	10.304.1003.2030	33.90.	1.600	SMS
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
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

4. CLÁUSULA QUARTA - DA VIGÊNCIA CONTRATUAL

4.1. A vigência do presente instrumento vigorará pelo período de 12 (doze) meses, com início na data de 05/09/2025 e encerramento em 04/09/2026, prorrogável na forma dos artigos 106 e 107 da Lei nº 14.133 de 2021.

4.2. 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;

ESTADO DE MATO GROSSO
PREFEITURA MUNICIPAL DE CÁCERES
PROCURADORIA GERAL DO MUNICÍPIO

ESTADO DE MATO GROSSO
PREFEITURA MUNICIPAL DE CÁCERES
PROCURADORIA GERAL DO MUNICÍPIO

- 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 (três) 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.

7. CLÁUSULA SÉTIMA - OBRIGAÇÕES DA CONTRATADA

7.1. São obrigações da CONTRATADA:

- 7.1.1.** 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.
- 7.1.2.** Executar o objeto do contrato em sua totalidade, em conformidade com as especificações estabelecidas no Termo de Referência e no contrato firmado.
- 7.1.3.** Efetuar a entrega dos serviços e produtos dentro dos prazos estabelecidos, garantindo que estejam em perfeitas condições e em conformidade com as especificações contratuais.
- 7.1.4.** Acompanhar a entrega dos produtos com a devida nota fiscal, contendo marca, fabricante, modelo, procedência, prazo de garantia ou validade e demais informações exigidas.
- 7.1.5.** Garantir que os serviços e produtos fornecidos sejam de boa qualidade, atendendo integralmente às condições, quantidades e padrões estipulados no contrato.
- 7.1.6.** Resolver prontamente quaisquer falhas ou não conformidades apontadas pela CONTRATANTE, incluindo a substituição ou correção dos serviços e produtos rejeitados.
- 7.1.7.** Manter, durante toda a execução do contrato, as condições de habilitação exigidas, incluindo requisitos técnicos, fiscais, trabalhistas e sociais.
- 7.1.8.** Assumir integralmente as despesas relacionadas à execução do contrato, incluindo tributos, encargos trabalhistas e previdenciários de seus empregados.
- 7.1.9.** Disponibilizar equipe técnica qualificada e apta a atender às demandas durante toda a vigência do contrato.
- 7.1.10.** Implementar práticas de sustentabilidade ambiental, social e econômica na execução dos serviços, conforme princípios legais e normativos aplicáveis.
- 7.1.11.** Permitir à CONTRATANTE a fiscalização da execução dos serviços e fornecimento dos produtos, prestando todos os esclarecimentos solicitados.
- 7.1.12.** Registrar todas as interações e ocorrências relacionadas ao contrato, garantindo rastreabilidade e acompanhamento das obrigações contratuais.



**ESTADO DE MATO GROSSO
PREFEITURA MUNICIPAL DE CÁCERES
PROCURADORIA GERAL DO MUNICÍPIO**

14.9. O termo de extinção, sempre que possível, será precedido:

14.9.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

14.9.2. Relação dos pagamentos já efetuados e ainda devidos;

14.9.3. Indenizações e multas.,

14.10. 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).

14.11. 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.

14.12. 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.

14.13. 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.

14.14. Até que o contratado comprove o disposto no item anterior, o contratante reterá:

14.14.1. 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

14.14.2. Os valores das Notas fiscais ou Faturas correspondentes em valor proporcional ao inadimplemento, até que a situação seja regularizada.

14.15. 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 n.º 14.133/2021).

14.16. O contratante poderá ainda:

14.16.1. 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

14.16.2. 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.

14.17. 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).

15. CLÁUSULA DÉCIMA QUINTA - DO COMBATE À CORRUPÇÃO

15.1. Para a execução deste Contrato, nenhuma das partes poderá oferecer dar ou se comprometer a dar a quem quer que seja, ou aceitar ou se comprometer a aceitar de quem quer que seja, tanto por



ESTADO DE MATO GROSSO
PREFEITURA MUNICIPAL DE CÁCERES
PROCURADORIA GERAL DO MUNICÍPIO

conta própria quanto por intermédio de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou benefícios de qualquer espécie, seja de forma direta ou indireta quanto ao objeto deste Contrato, ou de outra forma a ele não relacionada, o que deve ser observado, ainda, pelos prepostos e colaboradores.

16. CLÁUSULA DÉCIMA SEXTA - LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

16.1. As Partes se comprometem integralmente com as disposições da Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e demais normas legais ou regulamentares aplicáveis à matéria, em relação aos dados pessoais tratados no âmbito deste contrato, devendo garantir medidas técnicas e organizacionais razoáveis para a segurança dos dados pessoais e respeito aos direitos dos titulares.

17. CLÁUSULA DÉCIMA SÉTIMA - DA PUBLICIDADE

17.1. A Contratante providenciará a divulgação do contrato no Portal Nacional de Contratações Públicas (PNCP) como condição indispensável para a sua eficácia, nos termos do art. 94, da Lei 14.133/2021. Ademais, o contrato e o extrato dele decorrente, deverão ser divulgados e mantidos à disposição do público em sítio eletrônico oficial, a teor parágrafo único do art. 72 e do art. 91, ambos da Lei 14.133/2021.

18. CLÁUSULA DÉCIMA OITAVA - DO FORO

18.1. As partes elegem o Foro da Comarca de Cáceres-MT, excluído qualquer outro, por mais privilegiado que seja ou que se torne para a solução de qualquer dúvida, litígio ou incidentes oriundos da execução do presente contrato, ou que com ele se relacionar.

Prefeitura Municipal de Cáceres-MT, 05 de setembro de 2025.

JEREMIAS PEREIRA LEITE
SECRETARIA MUNICIPAL ESPECIAL DE ASSUNTOS ESTRATÉGICOS
CONTRATANTE

ROSELANE GONZALEZ DO NASCIMENTO
ALMEIDA:07894477702
ROSELANE GONZALEZ DO NASCIMENTO ALMEIDA
SH7 PROTECAO E INTELIGENCIA CIBERNETICA LTDA
CONTRATADA

Assinado de forma digital por
ROSELANE GONZALEZ DO
NASCIMENTO ALMEIDA:07894477702
Dados: 2025.09.09 09:30:56 -03'00'

Proc. Administrativo Processo Licitatório - 029/2025

De: Andressa C. - SMEAE - Compras

Para: SMEAE - Secretaria Municipal Especial de Assuntos Estratégicos

Data: 20/03/2025 às 08:58:10

Setores (CC):

SMEAE, SMEAE - Compras

Setores envolvidos:

SMEAE-CIS, SMEAE, SMEAE - Compras

Registro de Preço para futura e eventual aquisição de serviço de locação de firewall e segurança cibernética para atender à demanda do Município de Cáceres

Senhor Secretário,

Cumprimentando cordialmente Vossa Senhoria, considerando a regularização do Processo Administrativo Eletrônico – PAE, no âmbito da Administração Direta e Indireta do Poder Executivo Municipal de Cáceres-MT, destinado à tramitação, em formato digital, de documentos e processos administrativos entre seus órgãos e entidades, segue, em anexo, formalização da demanda, Termo de Referência para abertura de PAE - Processo Administrativo Eletrônico de licitação, em conformidade com o estabelecido no Decreto 024/2020 - que dispõe a instituição do processo administrativo eletrônico.

Segue em anexo estudo técnico, mapa de risco e termo de referência.

Memorando 6.530/2025 - SOLICITAÇÃO DE PROCESSO LICITATÓRIO PARA CONTRATAÇÃO DE SERVIÇOS DE LOCAÇÃO DE FIREWALL E SEGURANÇA CIBERNÉTICA

Atenciosamente,

Andressa Nair

Gerência de Compras

Anexos:

ETP_FIREWALL_2025_FINAL2.docx

ETP_FIREWALL_2025_FINAL2.pdf

MR_FIREWALL_2025_FINAL.docx

MR_FIREWALL_2025_FINAL.pdf

TR_FIREWALL_2025_FINAL.docx

TR_FIREWALL_2025_FINAL.pdf

Assinado por 2 pessoas: GIRLANE VIEIRA PEREIRA e JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321>

ESTUDO TÉCNICO PRELIMINAR – 01/2025

1. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

1.1. Necessidade a Ser Atendida

1.1.1. A Prefeitura Municipal de Cáceres (PMC) desempenha um papel central na representação democrática da comunidade, sendo essencial para a governança e a tomada de decisões estratégicas voltadas ao desenvolvimento do município. Com o avanço contínuo da tecnologia e a crescente digitalização dos processos administrativos, a PMC enfrenta desafios cada vez mais complexos no âmbito da segurança cibernética. A proteção de dados sensíveis, a garantia da integridade dos sistemas e a continuidade operacional constituem pilares fundamentais para a eficiência e transparência das atividades municipais. A ampliação do uso de serviços de tecnologia da informação pela PMC demanda soluções robustas que assegurem tanto a proteção das informações que trafegam pela rede corporativa quanto o acesso seguro dos usuários. Nesse contexto, revela-se imprescindível a expansão e a modernização da solução de segurança baseada em Next Generation Firewall (NGFW), conjugada a um sistema avançado de bloqueio de acessos não autorizados, com utilização de inteligência artificial preditiva, bem como a um sistema de armazenamento de registros de eventos (logs) com capacidade para geração de relatórios analíticos. Atualmente, a PMC dispõe de um dispositivo Sophos Firewall em operação no Datacenter, responsável pela proteção do perímetro da rede. No entanto, considerando a evolução das ameaças cibernéticas e o aumento da complexidade dos ataques, torna-se indispensável a ampliação da infraestrutura vigente, proporcionando maior capacidade de processamento, resiliência e escalabilidade para atender às demandas presentes e futuras. A segurança da informação é uma prioridade estratégica de âmbito global e, no contexto da PMC, não se configura de forma distinta. Medidas preventivas são imprescindíveis para mitigar riscos relacionados a acessos indevidos, vazamento de dados e sequestro de informações mediante ataques sofisticados. Diante desse cenário, a contratação de uma solução de segurança abrangente, contemplando hardware, licenciamento de software, garantia, suporte técnico especializado, serviços de instalação, configuração e gestão contínua (24x7), bem como capacitação técnica, revela-se estratégica para a proteção do perímetro da rede. A solução, baseada em tecnologia NGFW, deverá contemplar funcionalidades essenciais, tais como: administração de banda (QoS), SD-WAN, VPN IPSec e SSL, IPS, proteção contra códigos maliciosos, filtragem de URLs, controle de aplicações e um sistema avançado de bloqueio de acessos não autorizados com inteligência artificial preditiva, garantindo a capacidade de detecção em tempo real de incidentes e a adoção de medidas imediatas para a mitigação de ameaças cibernéticas.

1.2. Necessidade de Expansão do Investimento

1.2.1. A expansão desse investimento é justificada pelos seguintes fatores:

- **Aumento do Fluxo de Informações:** O crescimento no número de estações de trabalho, a expansão das redes das Secretarias Municipais e a adição de novos recursos computacionais exigem a ampliação da infraestrutura de segurança.



- ### 1.2.2. Justificativa do Ponto de Vista do Interesse Público

- Em síntese, a expansão e a modernização da solução de segurança baseada em Next Generation Firewall (NGFW), associada à implementação de um sistema avançado de bloqueio de acessos não autorizados, com o uso de inteligência artificial preditiva, configuram-se como um investimento estratégico, plenamente alinhado às necessidades institucionais da Prefeitura Municipal de Cáceres (PMC). Esta iniciativa reforçará a proteção dos interesses públicos, a integridade das informações e a continuidade das

atividades administrativas e democráticas, garantindo maior segurança e resiliência no ambiente digital da administração municipal.

1.3. Partes Interessadas/Público-Alvo

1.3.1. As partes interessadas incluem a Prefeitura Municipal de Cáceres, servidores municipais, gestores públicos e cidadãos beneficiados pelos serviços conectados. O público-alvo é composto pelas secretarias municipais, unidades externas, praças públicas e todos os usuários que utilizam os serviços municipais ou as redes públicas disponibilizadas.

2. DEMONSTRAÇÃO DA PREVISÃO DA CONTRATAÇÃO NO PLANO DE CONTRATAÇÕES ANUAL, SEMPRE QUE ELABORADO, DE MODO A INDICAR O SEU ALINHAMENTO COM O PLANEJAMENTO DA ADMINISTRAÇÃO

2.1. A contratação está alinhada às metas estratégicas de modernização, transformação digital e segurança da informação, promovendo serviços públicos mais eficientes e protegidos. Ela contribui para a inovação tecnológica, a conectividade e a sustentabilidade, de acordo com os objetivos do Plano Estratégico Municipal, incluindo a adesão às normas de governança e proteção de dados previstas na LGPD. A solução fortalece a infraestrutura tecnológica, essencial para atender às necessidades atuais e futuras do município. A necessidade desta contratação encontra-se respaldada na Lei nº14.133/21.

2.2. 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;

3. REQUISITOS DA CONTRATAÇÃO

3.1. A presente contratação visa à implementação de uma solução tecnológica abrangente que atenda integralmente aos requisitos estabelecidos, proporcionando segurança cibernética avançada, conectividade de alta disponibilidade e gestão eficiente da infraestrutura de rede da Prefeitura de Cáceres. A solução integra Firewall de Nova Geração (NGFW), recursos de Inteligência Artificial Preditiva e tecnologia SD-WAN, visando proteger a rede contra ameaças cibernéticas, ataques do tipo “Zero Day” e acessos não autorizados, assegurando a integridade, disponibilidade e continuidade das operações municipais.

3.2. Segurança Cibernética Avançada

- 3.2.1. Implementação de Firewall de Nova Geração (NGFW) para monitoramento do tráfego de entrada e saída da internet, identificando e neutralizando ameaças em tempo real, com latência inferior a 5 milissegundos.
- 3.2.2. Adoção de sistema de Inteligência Artificial Preditiva para análise comportamental da rede, possibilitando a identificação e neutralização automática de ameaças, sem necessidade de intervenção humana.
- 3.2.3. Proteção abrangente para toda a infraestrutura, incluindo firewalls, roteadores e redes Wi-Fi seguras implantadas nas unidades externas.
- 3.2.4. Garantia de proteção contra ataques “Zero Day”, mitigando vulnerabilidades desconhecidas.

3.3. Infraestrutura de Conectividade e Alta Disponibilidade

- 3.3.1. Provisionamento de links de internet com alta disponibilidade e redundância, conforme segue:
- 3.3.2. Sede: Link dedicado de acesso à internet, com bloco /29 e banda mínima garantida de 500 Mbps, utilizando dois links de ASN distintos e rotas diferenciadas, proporcionando resiliência e continuidade das operações críticas.
- 3.3.3. Unidades remotas: Links redundantes, sendo o primário com banda mínima de 150 Mbps (fibra óptica) e o secundário com banda mínima de 35 Mbps (fibra óptica e 4/5G), ambos com ASN e rotas distintos, garantindo conectividade ininterrupta.
- 3.3.4. Integração dos links diretamente ao NGFW, assegurando o gerenciamento eficiente do tráfego e aplicação das políticas de segurança.
- 3.3.5. Implementação da tecnologia SD-WAN para otimização da interconexão entre as unidades vinculadas às secretarias municipais, promovendo eficiência operacional, gestão centralizada do tráfego e segurança aprimorada, além de redundância automática para garantir a continuidade dos serviços essenciais, como o Wi-Fi social e as audiências telepresenciais.

3.4. Infraestrutura em Regime de Comodato e Gestão Centralizada

- 3.4.1. Fornecimento dos equipamentos necessários em regime de comodato, eliminando a necessidade de aquisição direta e garantindo maior economicidade e flexibilidade ao contratante.
- 3.4.2. Manutenção preventiva e corretiva, suporte técnico especializado e atualizações regulares de firmware e assinaturas de segurança, assegurando o desempenho contínuo da solução.
- 3.4.3. Disponibilização de software de gerenciamento integrado, permitindo a configuração, monitoramento e gestão centralizada das políticas de segurança, além da emissão de relatórios detalhados para auditorias e conformidade com a legislação vigente, especialmente em relação à proteção de dados.

3.5. Wi-Fi Seguro e Serviços Complementares

- 3.5.1. Implantação de redes Wi-Fi seguras e segregadas para uso exclusivo dos servidores municipais, garantindo maior produtividade e proteção das informações.
- 3.5.2. Autenticação baseada em usuário, integrada às políticas de segurança do NGFW.
- 3.5.3. Oferta de internet Wi-Fi gratuita para cidadãos nas unidades externas e praças municipais, com controle de acesso e limitação de banda para garantir qualidade de serviço e prevenir o uso inadequado.

3.6. Capacitação e Suporte Técnico Especializado

- 3.6.1. Capacitação da equipe do contratante, com treinamento especializado e emissão de certificação que ateste o domínio das funcionalidades da solução, reduzindo a dependência de suporte externo.
- 3.6.2. Suporte técnico com SLAs bem definidos, incluindo atendimento remoto e presencial para a resolução de incidentes, manutenção corretiva e suporte operacional conforme o nível de criticidade.

3.7. Expansibilidade, Conformidade e Resiliência Operacional

- 3.7.1. Capacidade de expansão da solução para atender ao crescimento futuro de tráfego, usuários e novas funcionalidades.

Assinado por 2 pessoas: GIRLÂNE VIEIRA PEREIRA e JERÔNIMO PEREIRA PEREIRA
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321> e informe o código 34C7-D880-59D2-E321

- 3.7.2. Garantia de aderência às regulamentações vigentes relacionadas à proteção de dados e segurança da informação.
- 3.7.3. Implementação de mecanismos de failover, redundância e backup, minimizando impactos em caso de falhas.
- 3.7.4. Ferramentas para supervisão em tempo real e geração de relatórios para análise de desempenho, auditorias e conformidade.
- 3.7.5. Configuração de políticas de tráfego e priorização de dados para garantir o desempenho ideal em aplicações críticas.

3.8. Resultados Esperados

- 3.8.1. Considerando a crescente necessidade de segurança digital e conectividade eficiente, estima-se que, ao longo de 12 (doze) meses, os resultados esperados sejam plenamente alcançados, proporcionando maior eficiência, resiliência e segurança às operações da Prefeitura de Cáceres, alinhando-se às melhores práticas de segurança da informação e contribuindo para a modernização da gestão pública.

4. ESTIMATIVAS DAS QUANTIDADES PARA A CONTRATAÇÃO

- 4.1. A quantificação dos serviços descritos neste Termo de Referência foi realizada com base em uma análise detalhada das necessidades operacionais da Prefeitura Municipal de Cáceres, levando em consideração a infraestrutura atual de Tecnologia da Informação e Comunicação (TIC) e as projeções de crescimento da demanda por serviços digitais. O dimensionamento visa assegurar a continuidade das atividades administrativas, a segurança da informação e a eficiência na comunicação entre a Sede da Prefeitura e seus Sites Remotos, que incluem unidades externas e praças públicas. Este enfoque busca garantir alta disponibilidade dos serviços públicos prestados à população.
- 4.2. O quantitativo de cada serviço foi estabelecido levando em conta a complexidade da rede institucional da Prefeitura, que se estende por uma vasta área geográfica, abrangendo tanto o perímetro urbano quanto áreas remotas do município.
- 4.3. O serviço de provimento de solução de Firewall de Nova Geração (NGFW) e SD-WAN, com alta disponibilidade, será implementado em 172 unidades, o que inclui a Sede da Prefeitura e os Sites Remotos. Este serviço visa garantir proteção cibernética avançada e uma conectividade segura entre as diversas unidades da rede institucional. A necessidade de alta disponibilidade é crucial para garantir a continuidade operacional e minimizar riscos de interrupções nos serviços essenciais à população.
- 4.4. A implementação de um serviço de segurança cibernética baseado em Inteligência Artificial Preditiva, com 2 unidades, abrange a Sede da Prefeitura e um ambiente de contingência. Este serviço será responsável por antecipar e mitigar ameaças cibernéticas, utilizando tecnologia de ponta para garantir a proteção da infraestrutura e a rápida resposta a incidentes.
- 4.5. A contratação de 2 links dedicados de acesso à internet com banda mínima garantida de 500 Mbps e redundância de ASN e rotas diferentes atenderá à Sede da Prefeitura, onde se concentram sistemas críticos e serviços

essenciais que demandam alta capacidade de tráfego de dados. Além disso, a contratação de 171 links de 150 Mbps e outros 171 links de 35 Mbps, destinados aos Sites Remotos, atenderá às diversas necessidades de conectividade, incluindo unidades externas e praças públicas, com foco na inclusão digital e na acessibilidade aos serviços de interesse público.

4.6. A implantação da solução e a capacitação da equipe técnica, ambos com quantidade unitária, são essenciais para garantir a adequada implementação da infraestrutura contratada, bem como o desenvolvimento de competências internas para sua gestão e manutenção. O treinamento especializado, com certificação, tem como objetivo qualificar os profissionais da Prefeitura para operar as novas tecnologias de forma eficiente e sustentável.

4.7. A consultoria em política de segurança da informação, também com quantitativo unitário, será fundamental para a elaboração de diretrizes estratégicas que assegurem a governança da TIC, alinhadas às melhores práticas do mercado e às exigências legais aplicáveis. Esse serviço impactará diretamente a cultura organizacional e as práticas de segurança da Prefeitura, promovendo a conformidade e a proteção dos dados.

4.8. A tabela a seguir apresenta as estimativas detalhadas para a contratação dos serviços:

ITEM	ESPECIFICAÇÃO	UNIDADE	QUANTIDADE
1	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)	Serviço	173
2	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	Serviço	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)	Serviço	2
4	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 150Mbps Sites Remotos (Fibra Óptica)	Serviço	171
5	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G)	Serviço	171
6	Implantação da Solução	Serviço	1
7	Capacitação especializada da equipe com emissão de certificação.	Treinamento	1
8	Consultoria Política de Segurança	Serviço	1

4.9. A distribuição dos serviços será organizada conforme a estrutura administrativa do município, considerando as diversas secretarias e suas unidades estratégicas. O quantitativo necessário foi dimensionado levando em conta a demanda operacional de cada local, garantindo que todos os pontos críticos sejam atendidos adequadamente.

4.9.1. A seguir, estão detalhadas as unidades centralizadas, descentralizadas e as praças públicas, com suas respectivas localizações e quantidades:

4.9.1.1. 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/u39WX2UzVeVQOWS28	1
	SMIL - OFICINA	https://maps.app.goo.gl/wQmT4CxnPbdKZUYC9	1
TOTAL			11

4.9.1.2. 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/DxdddTbATc7X73Bns5	1
	SMASC - CASA DE PASSAGEM	https://maps.app.goo.gl/WrVThbciHZooSfgX6	1
	SMASC - CENTRO DE MULTIPLO USO	https://maps.app.goo.gl/Lz5UoPyGg42jmUn8	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/WbNKuCbptlrDS5TE7	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/s5PAoUDUNHedzdk6	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

Assinado por 2 pessoas: GILRILANE VIEIRA PEREIRA e JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321 e informe o código 34C7-D880-59D2-E321

SME - EM JARDIM GUANABARA	https://goo.gl/maps/Rfg8wh2T7iw4NrbP6	1
SME - EM JARDIM PARAÍSO	https://goo.gl/maps/kkyMp6LAXieSyyvPW9	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/uyBXsZNDdszodCxxk6	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/QZKQCN7SU9D2qwg8	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/NSNEbdrq1cjknwX8	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/b3bCUzB8qzw7vRd77	1
SME - LARANJEIRA I	https://goo.gl/maps/jB1SZ3za3cdYev4a6	1
SME - SÃO FRANCISCO	https://maps.app.goo.gl/sxzj1LsfxfFEX7Zy6	1
UNIDADE DESCENTRALIZADA 4	-	1
UNIDADE DESCENTRALIZADA 5	-	1
UNIDADE DESCENTRALIZADA 6	-	1
UNIDADE DESCENTRALIZADA 7	-	1

Assinado por 2 pessoas: GIRLENE VIEIRA PEREIRA e JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321> e informe o código 34C7-D880-59D2-E321

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 LIMA	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/vYJEU1ufGKzoEeK7	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
SMTC	UNIDADE DESCENTRALIZADA 13	-	1
	UNIDADE DESCENTRALIZADA 14	-	1
	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

4.9.1.3. 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/qXAReBWJ7BQRpkm9	1
SMEAE - PRAÇA MAJOR JOÃO CARLOS	https://goo.gl/maps/Qcwn4CXJdT5VCWQ6	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/mJXKjDVOASbukgY37	1
SMEAE - RODOVIÁRIA	https://maps.app.goo.gl/8LyQniCzZ74f3oCC7	1
SMEAE - SÁDIA	https://maps.app.goo.gl/tc1GB5cCztjYFNtm9	1
PRAÇA MUNICIPAL 1		1
PRAÇA MUNICIPAL 2		1
PRAÇA MUNICIPAL 3		1

Assinado por 2 pessoas: GIRLANE VIEIRA PEREIRA e JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321 e informe o código 34C7-D880-59D2-E321

	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

4.10. As estimativas apresentadas neste documento têm como objetivo garantir a alocação adequada de recursos e a implementação eficaz das soluções de TIC para atender às necessidades da Prefeitura Municipal de Cáceres, visando à segurança, à continuidade das operações e à inclusão digital da população.

5. LEVANTAMENTO DE MERCADO, QUE CONSISTE NA ANÁLISE DAS ALTERNATIVAS POSSÍVEIS, E JUSTIFICATIVA TÉCNICA E ECONÔMICA DA ESCOLHA DO TIPO DE SOLUÇÃO A CONTRATAR

5.1. Contextualização da Necessidade

A crescente dependência da Tecnologia da Informação e Comunicação (TIC) para a prestação eficiente dos serviços públicos impõe desafios à administração pública, especialmente no que tange à segurança cibernética, à conectividade de alta disponibilidade e à gestão integrada da infraestrutura de rede. O avanço das ameaças digitais, aliado à complexidade crescente dos ambientes tecnológicos, exige soluções capazes de atender às demandas atuais e oferecer escalabilidade, resiliência e capacidade preditiva para mitigar riscos futuros.

No contexto da Prefeitura Municipal de Cáceres, a adoção de uma solução tecnológica robusta é essencial para garantir a continuidade dos serviços essenciais, proteger dados sensíveis da administração pública e dos cidadãos, além de otimizar os recursos financeiros por meio da gestão eficiente da infraestrutura de TIC. Para tanto, foi realizado um levantamento detalhado das opções disponíveis no mercado, considerando aspectos técnicos, operacionais e financeiros, visando identificar a alternativa que melhor atenda aos requisitos estratégicos do Município.

5.2. Histórico da Aquisição

Historicamente, a Prefeitura Municipal de Cáceres adotou modelos convencionais de aquisição de equipamentos e serviços de TIC, caracterizados pela compra direta de hardware e pela contratação de serviços de suporte técnico de forma fragmentada. Embora tenha atendido às necessidades em momentos específicos, esse modelo revelou-se limitado diante do aumento da demanda por serviços digitais mais seguros, eficientes e ágeis para resposta a incidentes.

As aquisições anteriores concentraram-se em soluções isoladas, com foco em equipamentos de segurança perimetral, como firewalls convencionais, roteadores básicos e conexões de rede dedicadas. A ausência de uma gestão integrada de segurança cibernética e de mecanismos avançados de monitoramento dificultou a detecção precoce de ameaças, aumentando a vulnerabilidade da infraestrutura crítica do Município.

Além disso, a gestão de múltiplos contratos com fornecedores distintos resultou em desafios relacionados à fragmentação da responsabilidade técnica, dificultando a resolução rápida de incidentes e comprometendo a eficiência operacional. Esse cenário evidenciou a necessidade de uma solução moderna e integrada, capaz

consolidar a segurança, a conectividade e a gestão em uma única plataforma, proporcionando maior agilidade, eficiência e controle.

5.3. Identificação das Opções Disponíveis

Com base na análise do mercado e nas necessidades específicas da Prefeitura, foram identificadas três opções viáveis para a modernização da infraestrutura de TIC, conforme apresentado a seguir:

SOLUÇÃO	CARACTERÍSTICAS PRINCIPAIS	VANTAGENS	DESVANTAGENS	CUSTO
Solução 01: Modelo Tradicional de Aquisição e Gestão Interna	- Aquisição direta de equipamentos (firewalls de última geração, switches, roteadores, etc.)	- Controle direto sobre os ativos de TIC	- Alto custo inicial de aquisição	Elevado (aquisição inicial + manutenção contínua)
	- Gestão e manutenção realizadas pela equipe interna	- Personalização das configurações conforme as necessidades	- Necessidade de constante atualização	
	- Suporte técnico terceirizado pontual		- Dependência de equipe interna altamente qualificada	
			- Maior tempo de resposta em falhas críticas	
Solução 02: Contratação de Serviços Segmentados	- Contratação de serviços especializados de fornecedores distintos (segurança, conectividade, suporte técnico)	- Flexibilidade na escolha de fornecedores	- Complexidade na gestão de múltiplos contratos	Moderado (contratos anuais de serviços)
	- Gestão interna da Prefeitura para coordenação dos contratos	- Possibilidade de negociação individual de contratos	- Falta de integração entre sistemas	
			- Risco de inconsistências na segurança cibernética	
Solução 03: Prestação de Serviços Integrados com Inteligência Artificial Preditiva (Escolhida)	- Fornecimento de equipamentos em comodato (NGFW, SD-WAN)	- Redução de custos iniciais	- Dependência do fornecedor, mitigada por SLAs rigorosos	Otimizado (mensalidade fixa com manutenção inclusa)
	- Gestão unificada da segurança cibernética com IA preditiva	- Alta disponibilidade e resiliência da rede		
	- Redundância de links de diferentes ASN	- Detecção proativa de ameaças		
	- Suporte técnico especializado 24/7	- Facilidade de gestão com contrato único		
	- Capacitação certificada da equipe interna			

5.4. Adequação ao Ambiente Tecnológico da Prefeitura

A análise da adequação das soluções ao ambiente tecnológico da Prefeitura de Cáceres evidenciou que a Solução 03 é a alternativa mais alinhada às necessidades atuais e futuras do Município.

Enquanto as Soluções 01 e 02 exigiriam investimentos adicionais em infraestrutura e capacitação da equipe interna, além de apresentarem maior complexidade na gestão e resposta a incidentes, a Solução 03 destaca-se pela oferta de uma abordagem integrada, com implantação unificada realizada por uma empresa homologada, credenciada e solidariamente vinculada ao fabricante, conforme previsto no edital.

A centralização dos serviços em um único fornecedor simplifica a gestão da infraestrutura de TIC, elimina a fragmentação da responsabilidade técnica e garante maior resiliência e escalabilidade, permitindo adaptações rápidas em caso de mudanças nas demandas da administração pública. Além disso, a utilização de Inteligência Artificial Preditiva possibilita a detecção e mitigação proativa de ameaças, aumentando significativamente a segurança da informação.

5.5. Justificativa Técnica e Econômica da Escolha

A escolha da Solução 03: Prestação de Serviços Integrados com Inteligência Artificial Preditiva justifica-se pelos seguintes fatores:

- **Eficiência Operacional:** A integração da segurança cibernética, conectividade e suporte técnico em uma única plataforma reduz a complexidade operacional e melhora a eficiência da gestão da infraestrutura de TIC.
- **Redução de Custos Iniciais:** O fornecimento dos equipamentos em regime de comodato elimina o alto investimento inicial necessário para aquisição direta, permitindo uma alocação mais eficiente dos recursos financeiros.
- **Alta Disponibilidade e Resiliência:** A redundância de links de diferentes ASN garante conectividade ininterrupta, essencial para a continuidade dos serviços públicos.
- **Segurança Avançada:** O uso de NGFW e SD-WAN com Inteligência Artificial Preditiva possibilita a detecção automatizada e a resposta proativa a ameaças, minimizando os riscos de ataques cibernéticos.
- **Suporte Técnico Especializado:** O suporte 24/7 com SLAs rigorosos assegura a rápida resolução de incidentes, reduzindo o impacto de eventuais falhas.
- **Escalabilidade e Flexibilidade:** A solução oferece capacidade de expansão para atender ao crescimento futuro da demanda, garantindo a sustentabilidade da infraestrutura de TIC.

Dessa forma, a contratação da Solução 03 representa a melhor relação custo-benefício para a Prefeitura Municipal de Cáceres, assegurando maior segurança, eficiência e continuidade dos serviços públicos, em conformidade com os requisitos estratégicos e normativos aplicáveis.

6. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

6.1. Comparação de Custos e Benefícios das Opções Disponíveis

A análise comparativa entre as três soluções avaliadas evidencia o melhor custo-benefício da Solução 03, considerando os investimentos diretos e os ganhos em eficiência operacional e segurança cibernética. A tabela a seguir resume os principais aspectos analisados:

ASPECTO AVALIADO	SOLUÇÃO 01: AQUISIÇÃO E GESTÃO INTERNA	SOLUÇÃO 02: SERVIÇOS SEGMENTADOS	SOLUÇÃO 03: SERVIÇOS INTEGRADOS COM IA PREDITIVA
Custo Inicial	R\$ 3.500.000,00	Não aplicável (serviços contínuos)	Não aplicável (equipamentos em comodato)
Custo Mensal	Não aplicável	R\$ 250.000,00	R\$ 208.333,33
Custo Anual	R\$ 3.500.000,00 + R\$ 200.000,00 (suporte)	R\$ 3.000.000,00	R\$ 2.500.000,00
Eficiência Operacional	Limitada (gestão interna)	Fragmentada (múltiplos fornecedores)	Alta (gestão centralizada e automatizada)

Segurança Cibernética	Básica (firewalls convencionais)	Moderada (proteção parcial)	Avançada (NGFW, SD-WAN e IA preditiva)
Resposta a Incidentes	Lenta (dependência da equipe interna)	Variável (conforme fornecedor)	Rápida (monitoramento 24/7 e SLAs rigorosos)
Escalabilidade	Limitada (infraestrutura fixa)	Moderada (expansão gradual)	Alta (infraestrutura flexível e integrada)

6.2. Estimativa de Custos

Com base nas especificações técnicas e operacionais de cada solução, a estimativa de custos mensais e anuais é apresentada na tabela abaixo:

SOLUÇÃO	CUSTO MENSAL (R\$)	CUSTO ANUAL (R\$)
Solução 01: Aquisição e Gestão Interna	Não aplicável	3.500.000,00 + 200.000,00 (manutenção anual)
Solução 02: Serviços Segmentados	250.000,00	3.000.000,00
Solução 03: Serviços Integrados com IA	208.333,33	2.500.000,00

6.3. Diante da análise técnica, operacional e financeira, conclui-se que a Solução 03: Serviços Integrados com Inteligência Artificial Preditiva representa a opção mais vantajosa para a Prefeitura Municipal de Cáceres, por oferecer:

- **Redução de Custos Iniciais:** Eliminação do alto investimento inicial devido ao fornecimento de equipamentos em comodato.
- **Custo Mensal Fixo:** Previsibilidade orçamentária, com valor fixo mensal de R\$ 208.333,33, incluindo todos os serviços necessários.
- **Segurança Cibernética Avançada:** Proteção proativa contra ameaças digitais por meio de IA preditiva.
- **Alta Eficiência Operacional:** Gestão centralizada, monitoramento contínuo e suporte técnico especializado 24/7.
- **Escalabilidade e Flexibilidade:** Infraestrutura adaptável às demandas futuras do Município.

Essa escolha assegura não apenas a proteção da infraestrutura de Tecnologia da Informação e Comunicação (TIC) da Prefeitura Municipal de Cáceres, mas também contribui para a sustentabilidade e continuidade dos serviços públicos digitais. A solução está alinhada às melhores práticas de governança e segurança da informação, proporcionando maior eficiência operacional, mitigação de riscos cibernéticos e atendimento às demandas crescentes da administração pública.

A vigência contratual será de 12 (doze) meses, contados a partir da emissão da Ordem de Serviço, com possibilidade de prorrogação por períodos iguais e sucessivos, conforme estabelecido no artigo 114 da Lei 14.133, de 2021. O prazo máximo para a manutenção do contrato é de até 15 (quinze) anos, assegurando a continuidade, estabilidade e qualidade dos serviços prestados, além de garantir o pleno funcionamento das atividades desempenhadas pela administração municipal ao longo do tempo.

7. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

7.1. 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.

7.2. 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.

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

7.3.1. **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.

7.3.2. **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.

7.4. 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.

7.4.1. Planejamento e Implantação

7.4.1.1. 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:

7.4.1.1.1. 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.

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

7.4.1.1.3. 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.

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

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

7.4.2. Operação e Manutenção

7.4.2.1. 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:

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

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

- 7.4.2.1.3. 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.
- 7.4.2.1.4. Consultoria contínua para aprimoramento da política de segurança da informação, com foco na proteção de dados, conformidade regulatória e mitigação de riscos cibernéticos.
- 7.4.2.1.5. Garantia de alta disponibilidade, com suporte a redundância de links e contingência operacional para evitar interrupções nos serviços municipais.

7.4.3. Evolução e Sustentabilidade da Solução

- 7.4.3.1. 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:
 - 7.4.3.1.1. Adoção de tecnologias emergentes para otimizar a performance e segurança da infraestrutura de TIC.
 - 7.4.3.1.2. Revisão periódica da estratégia de segurança cibernética, considerando as tendências de ameaças digitais e as melhores práticas do setor.
 - 7.4.3.1.3. Expansão escalável da solução, permitindo a incorporação de novas unidades e serviços de forma ágil e estruturada.
 - 7.4.3.1.4. Otimização do consumo de recursos tecnológicos, garantindo um uso eficiente da infraestrutura contratada e contribuindo para a sustentabilidade financeira e operacional do município.

7.5. Especificação do Produto

7.5.1. Funcionamento Geral da Solução

- 7.5.1.1. 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.
- 7.5.1.2. A contratação também inclui a prestação de serviço de acesso à internet nos Sites Remotos e na sede da Prefeitura Municipal de Cáceres MT.
- 7.5.1.3. A contratação deverá englobar o fornecimento de um conjunto de equipamentos de rede, incluindo recursos de IP para trabalhar em alta disponibilidade na Sede e cada equipamento deverá permitir no mínimo 4(quatro) conexões à Internet.
- 7.5.1.4. 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.
- 7.5.1.5. Os equipamentos SD-WAN da Sede deverão trabalhar em alta disponibilidade.

- 7.5.1.6. A relação dos Sites Remotos e da Central nos quais os serviços serão prestados encontra-se descrita no tópico 4.9 e seus subtópicos deste Termo de Referência.
- 7.5.1.7. 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.
- 7.5.1.8. 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.
- 7.5.1.9. 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.
- 7.5.1.10. 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.
- 7.5.1.11. A prestação dos serviços descritos em cada ITEM que trata o tópico 4.8 deverá ser considerada como entregue, a partir da assinatura do Termo de Recebimento Definitivo.
- 7.5.1.12. 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.
- 7.5.1.13. 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.
- 7.5.1.14. Não haverá aquisição de equipamentos, incluindo roteadores, modems, 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.

7.5.1.15. 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.

7.5.1.16. 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.

7.5.1.17. A CONTRATADA deverá também realizar repasse de conhecimento na modalidade presencial para a equipe técnica do CONTRATANTE sobre a solução implantada.

7.5.2. Topologia Da Solução

7.5.2.1. 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.

7.5.2.1.1. Estruturação dos Sites e Capacidade dos Links

7.5.2.1.1.1. 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.

7.5.2.1.1.1.1. **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 20 usuários simultaneamente. O tráfego nesses locais incluirá tanto o acesso aos sistemas institucionais da Prefeitura quanto a utilização de serviços públicos digitais pelos cidadãos.

7.5.2.1.1.1.2. **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.

7.5.2.1.1.2. 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.

7.5.2.1.2. Topologia Lógica da Solução

7.5.2.1.2.1. 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:

7.5.2.1.2.1.1. 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.

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

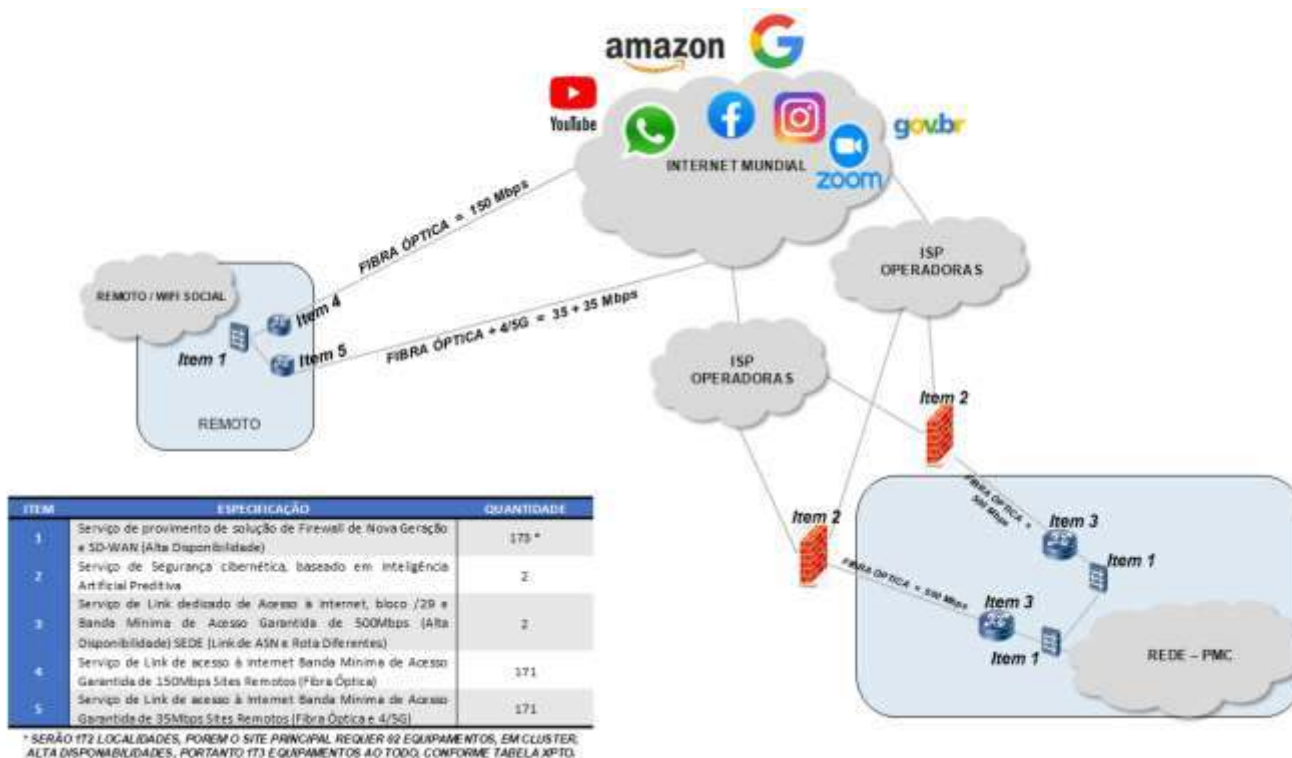
7.5.2.1.2.1.3. Dispositivos SD-WAN implementados na Sede e nos Sites Remotos, possibilitando gerenciamento eficiente do tráfego, redundância e otimização dos links de comunicação.

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

7.5.2.1.2.1.5. 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.

7.5.2.1.2.1.6. Consultoria especializada e capacitação da equipe técnica da Prefeitura, garantindo conhecimento sobre a administração da solução e autonomia na gestão da infraestrutura implantada.

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



7.5.3. Equipamentos e Funcionalidades Chave

7.5.3.1. Os equipamentos do ITEM 1, que trata o tópico 4.8, deverão ser entregues no formato e características técnicas bem como funcionalidades conforme especificações abaixo:

7.5.3.1.1. Appliance NGFW de 5 Gbps de Capacidade de Firewall

7.5.3.1.1.1. Características do Hardware

- 7.5.3.1.1.1.1. O equipamento deve se instalar em mesa ocupando no máximo 1U (44,45mm) da referida mesa;
- 7.5.3.1.1.1.2. Dispor de fonte de alimentação com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;
- 7.5.3.1.1.1.3. Deverão ser fornecidos todos os cabos de energia, serial (RS-232/RJ45), para instalação e funcionamento do dispositivo;
- 7.5.3.1.1.1.4. Possuir led indicador on/off, disco e devices de rede;
- 7.5.3.1.1.1.5. Possuir throughput mínimo de 5 Gbps para tráfego UDP;
- 7.5.3.1.1.1.6. Suportar no mínimo 4.000.000 (quatro milhões) conexões simultâneas;
- 7.5.3.1.1.1.7. Suportar no mínimo 37.000 (trinta e sete mil) novas conexões por segundo;
- 7.5.3.1.1.1.8. Possuir throughput mínimo de 300 Mbps para tráfego IPS/IDS;
- 7.5.3.1.1.1.9. Possuir throughput mínimo de 280 Mbps para tráfego VPN IPSEC com criptografia (AES-256);

- 7.5.3.1.1.1.10. Possuir throughput mínimo de 140 Mbps para tráfego VPN SSL com criptografia (AES-256);
- 7.5.3.1.1.1.11. Possuir throughput mínimo de 150 Mbps para SSL Inspection;
- 7.5.3.1.1.1.12. Possuir throughput mínimo de 200 Mbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);
- 7.5.3.1.1.1.13. 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;
- 7.5.3.1.1.1.14. Possuir dispositivo de armazenamento interno de no mínimo 64 GB padrão SSD e deve suportar expansão futura para, no mínimo, 120 GB;
- 7.5.3.1.1.1.15. 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;
- 7.5.3.1.1.1.16. Possuir pelo menos 1 (uma) portas USB para conexão de dispositivos externos;
- 7.5.3.1.1.1.17. Deve possuir modem interno 3G/4G/LTE para conexão de link de Internet. O modulo deverá estar incluso no valor do equipamento;

7.5.3.1.2. Appliance NGFW de 9.7 Gbps de Capacidade de Firewall

7.5.3.1.2.1. Características do Hardware

- 7.5.3.1.2.1.1. O equipamento deve se instalar em mesa ocupando máximo 1U (44,45mm) da referida mesa;
- 7.5.3.1.2.1.2. Dispor de fonte de alimentação com tensão de entrada 110V / 220V AC automática e frequência de 50-60 Hz;
- 7.5.3.1.2.1.3. Deverão ser fornecidos todos os cabos de energia, serial (RS-232/RJ45) ou similar, para instalação e funcionamento do dispositivo;
- 7.5.3.1.2.1.4. Possuir led indicador on/off, disco e devices de rede;
- 7.5.3.1.2.1.5. Possuir throughput mínimo de 9.7 Gbps para tráfego UDP;
- 7.5.3.1.2.1.6. Suportar no mínimo 6.000.000 (seis milhões) conexões simultâneas;

- 7.5.3.1.2.1.7. Suportar no mínimo 45.000 (quarenta e cinco mil) novas conexões por segundo;
- 7.5.3.1.2.1.8. Possuir throughput mínimo de 1.25 Gbps para tráfego IPS/IDS;
- 7.5.3.1.2.1.9. Possuir throughput mínimo de 2.0 Gbps para tráfego VPN IPSEC com criptografia (AES-256);
- 7.5.3.1.2.1.10. Possuir throughput mínimo de 1.2 Gbps para tráfego VPN SSL com criptografia (AES-256);
- 7.5.3.1.2.1.11. Possuir throughput mínimo de 700 Mbps para tráfego SSL Inspection;
- 7.5.3.1.2.1.12. Possuir throughput mínimo de 850 Mbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);
- 7.5.3.1.2.1.13. 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;
- 7.5.3.1.2.1.14. Possuir dispositivo de armazenamento interno de no mínimo 64 GB padrão SSD e deve suportar expansão futura para, no mínimo, 120 GB;
- 7.5.3.1.2.1.15. Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento;
- 7.5.3.1.2.1.16. Possuir pelo menos 1 (uma) porta USB para conexão de dispositivos externos;
- 7.5.3.1.2.1.17. A interface USB deve suportar o uso de modem 3G/4G/LTE para conexão de link de Internet;

7.5.3.1.3. Appliance NGFW de 11.8 Gbps de Capacidade de Firewall

7.5.3.1.3.1. Características do Hardware

- 7.5.3.1.3.1.1. O equipamento deve se instalar em mesa ocupando máximo 1U (44,45mm) da referida mesa;
- 7.5.3.1.3.1.2. Dispor de fonte de alimentação com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;
- 7.5.3.1.3.1.3. Deverão ser fornecidos todos os cabos de energia, serial (RS-232/RJ45) ou similar, para instalação e funcionamento do dispositivo;
- 7.5.3.1.3.1.4. Possuir led indicador on/off, disco e devices de rede;

- 7.5.3.1.3.1.5. Possuir throughput mínimo de 11.8 Gbps para tráfego UDP;
- 7.5.3.1.3.1.6. Suportar no mínimo 7.000.000 (sete milhões) conexões simultâneas;
- 7.5.3.1.3.1.7. Suportar no mínimo 52.000 (cinquenta e duas mil) novas conexões por segundo;
- 7.5.3.1.3.1.8. Possuir throughput mínimo de 1.5 Gbps para tráfego IPS/IDS;
- 7.5.3.1.3.1.9. Possuir throughput mínimo de 2.5 Gbps para tráfego VPN IPSEC com criptografia (AES-256);
- 7.5.3.1.3.1.10. Possuir throughput mínimo de 1.5 Gbps para tráfego VPN SSL com criptografia (AES-256);
- 7.5.3.1.3.1.11. Possuir throughput mínimo de 900 Mbps para tráfego SSL Inspection;
- 7.5.3.1.3.1.12. Possuir throughput mínimo de 1.0 Gbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);
- 7.5.3.1.3.1.13. 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;
- 7.5.3.1.3.1.14. Possuir dispositivo de armazenamento interno de no mínimo 120 GB padrão SSD;
- 7.5.3.1.3.1.15. Permitir acesso a interface de gerenciamento CLI fisicamente no equipamento;
- 7.5.3.1.3.1.16. Possuir pelo menos 1 (uma) porta USB para conexão de dispositivos externos;
- 7.5.3.1.3.1.17. A interface USB deve suportar o uso de modem 3G/4G/LTE para conexão de link de Internet;
- 7.5.3.1.4. Appliance NGFW de 19.4 Gbps de Capacidade de Firewall**
- 7.5.3.1.4.1. Características do Hardware**
- 7.5.3.1.4.1.1. Deverá ser entregue dois equipamentos idênticos para atender a funcionalidade de cluster;
- 7.5.3.1.4.1.2. O equipamento deve se instalar em rack com largura padrão de 19 polegadas, padrão EIA-310, ocupando no máximo (44,45mm) do referido rack;

- 7.5.3.1.4.1.3. Dispor de fonte de alimentação interna com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;
- 7.5.3.1.4.1.4. Possuir painel/led indicador on/off, disco e devices de rede;
- 7.5.3.1.4.1.5. Possuir throughput de no mínimo 19.4 Gbps para tráfego UDP;
- 7.5.3.1.4.1.6. Suportar no mínimo 8.200.000 (oito milhões e duzentas mil) conexões simultâneas;
- 7.5.3.1.4.1.7. Suportar no mínimo 65.000 (sessenta e cinco mil) novas conexões por segundo;
- 7.5.3.1.4.1.8. Possuir throughput mínimo de 3.0 Gbps para tráfego IPS/IDS;
- 7.5.3.1.4.1.9. Possuir throughput mínimo de 3.0 Gbps para tráfego VPN IPSEC com criptografia (AES-256);
- 7.5.3.1.4.1.10. Possuir throughput mínimo de 1.8 Gbps para tráfego VPN SSL com criptografia (AES-256);
- 7.5.3.1.4.1.11. Possuir throughput mínimo de 1.3 Gbps para tráfego SSL Inspection;
- 7.5.3.1.4.1.12. Possuir throughput mínimo de 2.5 Gbps para tráfego NGFW (habilitadas as funcionalidades de Firewall, IPS e Controle de Aplicativo);
- 7.5.3.1.4.1.13. 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, de preferência seja, não será aceito equipamento com porta do tipo switch;
- 7.5.3.1.4.1.14. Possuir dispositivo de armazenamento interno de no mínimo 120 GB padrão SSD;
- 7.5.3.1.4.1.15. Permitir acesso a interface de gerenciamento de rede fisicamente no equipamento;
- 7.5.3.1.4.1.16. Possuir no mínimo 1 (uma) porta USB para conexão de dispositivos externos;
- 7.5.3.1.4.1.17. A interface USB deve suportar o uso de modem 3G/4G/LTE para conexão de link de Internet;

7.5.3.2. Especificações Gerais de Software NGFW Para Todos os Itens

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

7.5.3.2.1.1. Características Gerais

- 7.5.3.2.1.1.1. 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.
- 7.5.3.2.1.1.2. 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.
- 7.5.3.2.1.1.3. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
- 7.5.3.2.1.1.4. Todos os recursos listados neste termo de referência deverão ser suportado e estar disponíveis na versão mais atual do software fornecido;
- 7.5.3.2.1.1.5. 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);
- 7.5.3.2.1.1.6. Interface em português, espanhol e inglês;
- 7.5.3.2.1.1.7. Suportar notificação de vencimento da licença na janela de alertas com os dias restantes da data vencimento;
- 7.5.3.2.1.1.8. Suportar acesso à Web por HTTP e CLI por TELNET;
- 7.5.3.2.1.1.9. Permitir alterar a porta padrão para os acessos a interface de administração via HTTP, HTTPs e CLI;
- 7.5.3.2.1.1.10. Atualização de modo “offline”, onde pode ser baixado a base do fabricante e posteriormente fazer o upload do arquivo na solução.
- 7.5.3.2.1.1.11. Restore de Snapshot sem executar o Wizard e sem licenciamento;
- 7.5.3.2.1.1.12. 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;
- 7.5.3.2.1.1.13. Suportar segundo fator de autenticação (2FA/MFA) via token / OTP (One Time Password);

- 7.5.3.2.1.1.14. Deve suportar sistemas virtuais;
- 7.5.3.2.1.1.15. 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;
- 7.5.3.2.1.1.16. Qualquer interface de rede do equipamento deverá ser utilizada como gerenciamento, ou seja, não deve haver nenhuma interface exclusiva para a função de gerenciamento;
- 7.5.3.2.1.1.17. O sistema deve permitir o acesso à interface de gerenciamento WEB por qualquer interface de rede configurada;
- 7.5.3.2.1.1.18. O software deverá ser fornecido em sua versão mais atualizada, não sendo permitido qualquer tipo de comprovação futura.
- 7.5.3.2.1.1.19. Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução.
- 7.5.3.2.1.1.20. Todos os recursos detalhados no termo de referência deverão ser providos por um único software.
- 7.5.3.2.1.1.21. Tanto os Gateways de Segurança bem como a Gerência Centralizada deverão suportar monitoramento através de SNMP v1, v2 e v3.
- 7.5.3.2.1.1.22. Deverá possuir uma janela para monitoramento do tráfego de rede com informações do throughput e da quantidade de conexões simultâneas;
- 7.5.3.2.1.1.23. A Solução deverá prover inspeção SSL;
- 7.5.3.2.1.1.24. Deve suportar cluster do tipo Failover (HA) com replicação da tabela de estado;
- 7.5.3.2.1.1.25. Suportar a utilização de um proxy para atualização de software e licenciamento e deverá permitir as seguintes opções de configuração:
- a) Endereço do servidor;
 - b) Porta do servidor;
 - c) Usuário;
 - d) Senha;
- 7.5.3.2.1.1.26. 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.

- 7.5.3.2.1.1.27. 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;
- 7.5.3.2.1.1.28. 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;
- 7.5.3.2.1.1.29. 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;
- 7.5.3.2.1.1.30. Deverá possuir um painel centralizado para exportação e agendamento de relatórios e deverá permitir exportá-los nos formatos: HTML, PDF, CSV;
- 7.5.3.2.1.1.31. Implementar protocolo de coleta de informações de fluxos que circulam pelo equipamento, como Netflow v5, v9 e v10 (IPFIX);
- 7.5.3.2.1.1.32. 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;
- 7.5.3.2.1.1.33. Deve implementar o protocolo ECMP;
- 7.5.3.2.1.1.34. 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 perdidos na transmissão.

- 7.5.3.2.1.1.35. Deve possuir suporte ao protocolo de encapsulamento de redes MPLS;
- 7.5.3.2.1.1.36. Esta condição deve permitir conectar links MPLS diretamente no equipamento sem a necessidade de estar plugado a um segundo roteador/dispositivo.
- 7.5.3.2.1.1.37. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;
- 7.5.3.2.1.1.38. 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;

7.5.3.2.1.2. Recursos Gerais de Firewall

- 7.5.3.2.1.2.1. Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas;
- 7.5.3.2.1.2.2. 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;
- 7.5.3.2.1.2.3. Possibilitar a visualização dos países de origem e destino nos logs de eventos, de acessos e ameaças.
- 7.5.3.2.1.2.4. 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;
- 7.5.3.2.1.2.5. O sistema deve permitir configurar o período ou número de cópias que deseja manter no repositório remoto e executar a manutenção de período automaticamente.
- 7.5.3.2.1.2.6. As cópias de segurança devem ser salvas compactadas e criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;
- 7.5.3.2.1.2.7. 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;
- 7.5.3.2.1.2.8. Deve possibilitar a restauração do snapshot através interface web de qualquer ponto remoto, de modo

contribuir para uma restauração imediata sem a necessidade de reinicialização do sistema;

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

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

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

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

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

7.5.3.2.1.2.14. Possuir ferramenta de diagnóstico do tipo tcpdump;

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

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

7.5.3.2.1.2.17. 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.

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

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

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

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

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

7.5.3.2.1.2.23. 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.

7.5.3.2.1.2.24. Deverá suportar aplicações multimídia como: H.323, SIP,



- 7.5.3.2.1.2.25. Possuir tecnologia de firewall do tipo Stateful;
- 7.5.3.2.1.2.26. Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo-passivo;
- 7.5.3.2.1.2.27. Permitir o funcionamento em modo transparente tipo “bridge”;
- 7.5.3.2.1.2.28. Permitir a criação de mínimo 4090 VLANs no padrão IEEE 802.1q por interface de rede;
- 7.5.3.2.1.2.29. Possuir conexão entre estação de gerência e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando);
- 7.5.3.2.1.2.30. Deverá suportar forwarding de multicast;
- 7.5.3.2.1.2.31. Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP;
- 7.5.3.2.1.2.32. Permitir o agrupamento de serviços;
- 7.5.3.2.1.2.33. Possuir mecanismo de anti-spoofing;
- 7.5.3.2.1.2.34. Possuir a funcionalidade de balanceamento e contingência de links;
- 7.5.3.2.1.2.35. 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.
- 7.5.3.2.1.2.36. Permitir a configuração de regras de entrada baseado em zona de rede, possibilitando habilitar recursos de autenticação e restrição por origem baseado em IP.
- 7.5.3.2.1.2.37. Deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e mensagens instantâneas, suportando ao menos: Yahoo! Messenger, MSN Messenger, ICQ, Telegram, Whatsapp, WeChat, Snapchat BitTorrent, UTorrent, Vuze, eDonkey, GNUTella, Skype e Microsoft Teams.
- 7.5.3.2.1.2.38. A solução deverá suportar nativamente o recurso SIMP (nic.br) medidor de Internet.

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

- 7.5.3.2.1.3.2. A configuração de proteção DOS deve estar disponível para habilitar em modo global e por política de segurança;
- 7.5.3.2.1.3.3. Possuir recurso de validação das políticas de segurança para identificar regras duplicadas ou que se ofusquem;
- 7.5.3.2.1.3.4. 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.
- 7.5.3.2.1.3.5. Deverá permitir implementar filtros de IPS, WEB Filter, Threat Protection, SSL Inspection, Application Control, assim como definir roteamento de aplicativos por SD-Wan, limitação de taxa de DOS por pacotes em uma única política.
- 7.5.3.2.1.3.6. Exibir na própria política a visualização de quais módulos estão habilitados, sem que seja necessário a edição da regra de proteção.
- 7.5.3.2.1.3.7. Possibilitar a edição de objetos vinculados, sem a necessidade de recriar a política.
- 7.5.3.2.1.3.8. Possibilitar a duplicação de uma política, otimizando tempo de configuração;
- 7.5.3.2.1.4. **Identificação de Usuário**
- 7.5.3.2.1.4.1. 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, TACACS e Radius;
- 7.5.3.2.1.4.2. 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;
- 7.5.3.2.1.4.3. Para usuários não registrados ou não reconhecidos domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador (Captive Portal), sem a necessidade de agente;
- 7.5.3.2.1.4.4. Deve possuir Captive Portal com suporte a Autenticação Social (Facebook, Twitter, Google);
- 7.5.3.2.1.4.5. A solução deverá ser capaz de identificar nome do usuário, login, máquina/computador registrados no Microsoft Active Directory;

7.5.3.2.1.4.6. 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)

7.5.3.2.1.4.7. 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.

7.5.3.2.1.4.8. 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.

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

7.5.3.2.1.5. **Das Funcionalidades Da Vpn:**

7.5.3.2.1.5.1. VPN baseada em appliance;

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

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

7.5.3.2.1.5.4. Possuir suporte a VPNs IPsec site-to-site;

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

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

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

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

7.5.3.2.1.5.9. 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;

7.5.3.2.1.5.10. Possuir suporte a VPN SSL;



- Assinado por 2 pessoas:
 1. SRA. JEREMIAS PEREIRA LEITE
 2. SRA. PEREIRA LEITE
 Para verificar a validade das assinaturas, acesse <https://caceres1doc.com.br/verificacao/34C7-D880-59D2-E321> e informe o código 34C7-D880-59D2-E321

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

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

7.5.3.2.1.6. SD-WAN:

7.5.3.2.1.6.1. 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;

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

7.5.3.2.1.6.3. Suportar modo de duplicação de pacotes de dados pelo link 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;

7.5.3.2.1.6.4. Permitir utilizar VPN IPsec para interligar unidades remotas;

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

7.5.3.2.1.6.6. 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;

7.5.3.2.1.6.7. 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;

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

- 7.5.3.2.1.6.9. 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.
- 7.5.3.2.1.6.10. O recurso de SD-WAN deverá permitir o monitoramento de, no mínimo 03 (três) endereços alvos para verificar a disponibilidade e desempenho do link;
- 7.5.3.2.1.6.11. 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;
- 7.5.3.2.1.6.12. A solução deverá suportar os seguintes métodos de seleção de link:
- a) Failover;
 - b) Load Balance;
 - c) Spillover;
 - d) Dynamic Selection;
- 7.5.3.2.1.6.13. 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.
- 7.5.3.2.1.6.14. 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;
- 7.5.3.2.1.7. Das Funcionalidades de QoS**
- 7.5.3.2.1.7.1. Adotar solução de Qualidade de Serviço baseada em appliance;
- 7.5.3.2.1.7.2. 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;
- 7.5.3.2.1.7.3. Permitir modificação de valores DSCP;
- 7.5.3.2.1.7.4. Limitar individualmente a banda utilizada por programas de compartilhamento de arquivos do tipo peer-to-peer;

- 7.5.3.2.1.7.5. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
- 7.5.3.2.1.7.6. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;
- 7.5.3.2.1.7.7. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;
- 7.5.3.2.1.7.8. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino;
- 7.5.3.2.1.7.9. Deverá controlar (limitar ou expandir) individualmente a banda utilizada por endereço IP de origem e destino;

7.5.3.2.1.8. Alta Disponibilidade

- 7.5.3.2.1.8.1. Possuir mecanismo de Alta Disponibilidade operando em modo Ativo/Standby, com as implementações de Fail Over.
- 7.5.3.2.1.8.2. O Sincronismo dos servidores deve ser por interface exclusiva de Heartbeat;
- 7.5.3.2.1.8.3. 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;
- 7.5.3.2.1.8.4. Deverá suportar a persistências de sessão de usuários e conexões estabelecidas, entre os membros da Alta Disponibilidade;

7.5.3.2.2. Das Funcionalidades de Controle de Aplicação e Web Proxy

7.5.3.2.2.1. Controle de Aplicações

- 7.5.3.2.2.1.1. As funcionalidades abaixo devem ser baseadas em appliance:
- 7.5.3.2.2.1.2. Deverá reconhecer no mínimo 4000 aplicações;
- 7.5.3.2.2.1.3. Deverá possuir, no mínimo, 19 categorias para classificação de aplicações;
- 7.5.3.2.2.1.4. Deverá possuir categoria exclusiva, no mínimo, para as seguintes tipos de aplicações como:
 - a) P2P;
 - b) Web;
 - c) Transferência de arquivos;
 - d) Social;

- 7.5.3.2.2.1.5. Deverá permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;
- 7.5.3.2.2.1.6. Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;
- 7.5.3.2.2.1.7. Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;
- 7.5.3.2.2.1.8. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;
- 7.5.3.2.2.1.9. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;
- 7.5.3.2.2.1.10. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- 7.5.3.2.2.1.11. Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino;
- 7.5.3.2.2.1.12. Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.

7.5.3.2.2.2. Filtro de Conteúdo Web

- 7.5.3.2.2.2.1. Possuir solução de filtro de conteúdo web integrado a solução de segurança
- 7.5.3.2.2.2.2. Possuir pelo menos 80 categorias para classificação de sites web
- 7.5.3.2.2.2.3. Possuir base mínima contendo, 48 milhões de sites internet web já registrados e classificados;
- 7.5.3.2.2.2.4. 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;
- 7.5.3.2.2.2.5. Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;
- 7.5.3.2.2.2.6. Possuir sistema de cache interno, armazenando requisições WEB em disco local e memória;
- 7.5.3.2.2.2.7. Deve permitir a definição do tamanho mínimo dos objetos salvos em cache no disco;
- 7.5.3.2.2.2.8. Deve permitir a definição do tamanho máximo dos objetos salvos em cache em memória;
- 7.5.3.2.2.2.9. Deve atender a estrutura de navegação através de hierarquia de proxy com e sem autenticação;
- 7.5.3.2.2.2.10. Possibilitar a integração com servidores de cache WEB externos;
- 7.5.3.2.2.2.11. Deve ser capaz de armazenar cache dinâmicos para as atualizações Microsoft Windows Update, Youtube, Sourceforge Downloads, Facebook, Google Maps;
- 7.5.3.2.2.2.12. Deve possuir a capacidade de excluir URL's específicas do cache web, configurável por listas de palavras chaves com suporte inclusive a expressões regulares;
- 7.5.3.2.2.2.13. Integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;
- 7.5.3.2.2.2.14. Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory, LDAP, TACACS+ e Radius;
- 7.5.3.2.2.2.15. Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança da contratante;
- 7.5.3.2.2.2.16. Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;
- 7.5.3.2.2.2.17. Deverá permitir o bloqueio de URLs inválidas cujo campo CN do certificado SSL não contém um domínio válido;
- 7.5.3.2.2.2.18. Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web;

- 7.5.3.2.2.19. Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;
- 7.5.3.2.2.20. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;
- 7.5.3.2.2.21. Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem;
- 7.5.3.2.2.22. Possuir Logs e Relatórios de tempo de navegação de sites web - Domínios Web;
- 7.5.3.2.2.23. Possuir recurso capaz de controlar e restringir o acesso a sites com base em seus nomes de domínio, conhecido como DNS Content Filter;

7.5.3.2.2.3. Recursos do Proxy

- 7.5.3.2.2.3.1. Deverá funcionar em modo Proxy Explícito para HTTP, HTTPS, FTP, POP3 e SMTP e em Proxy Transparente;
- 7.5.3.2.2.3.2. A solução deve ser capaz de identificar o comportamento do protocolo SSH onde pode ser feito através da inspeção do protocolo;
- 7.5.3.2.2.3.3. Deverá permitir configurar a porta do Proxy Explícito;
- 7.5.3.2.2.3.4. O equipamento deverá poder suportar funcionalidades de antispam sem a necessidade de equipamento dedicado.

7.5.3.2.3. Das Funcionalidades da Detecção de Intrusão e ATP

7.5.3.2.3.1. Das Funcionalidades da Detecção de Intrusão

- 7.5.3.2.3.1.1. A Detecção de Intrusão deverá ser baseada em appliance;
- 7.5.3.2.3.1.2. Possuir no mínimo 82.000 (oitenta e duas mil) assinaturas ou regras de IPS/IDS;
- 7.5.3.2.3.1.3. Permitir a criação de assinaturas customizadas pelo administrador do NGFW;
- 7.5.3.2.3.1.4. O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;
- 7.5.3.2.3.1.5. Possuir tecnologia de detecção baseada em assinatura;
- 7.5.3.2.3.1.6. Deverá suportar a implantação em modo Gateway, inline e em modo sniffer;
- 7.5.3.2.3.1.7. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e destino da comunicação, além da ação tomada pelo dispositivo.

- 7.5.3.2.3.1.8. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação.
- 7.5.3.2.3.1.9. 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.
- 7.5.3.2.3.1.10. Possuir opção para administrador as listas de Blacklist, Whitelist e Quarentena com suporte a endereços IPv6.
- 7.5.3.2.3.1.11. Possuir capacidade de remontagem de pacotes para identificação de ataques;
- 7.5.3.2.3.1.12. 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;
- 7.5.3.2.3.1.13. 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;
- 7.5.3.2.3.1.14. Mecanismos de detecção/proteção de ataques;
- 7.5.3.2.3.1.15. Reconhecimento de padrões;
- 7.5.3.2.3.1.16. Análise de protocolos;
- 7.5.3.2.3.1.17. Detecção de anomalias;
- 7.5.3.2.3.1.18. Detecção de ataques de RPC (Remote procedure call);
- 7.5.3.2.3.1.19. Proteção contra-ataques de Windows ou NetBios;
- 7.5.3.2.3.1.20. Proteção contra-ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);
- 7.5.3.2.3.1.21. Proteção contra-ataques DNS (Domain Name System);
- 7.5.3.2.3.1.22. Proteção contra-ataques a FTP, SSH, Telnet e rlogin;
- 7.5.3.2.3.1.23. Proteção contra-ataques de ICMP (Internet Control Message Protocol);
- 7.5.3.2.3.1.24. Alarmes na console de administração;
- 7.5.3.2.3.1.25. Alertas via correio eletrônico;
- 7.5.3.2.3.1.26. 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;

- 7.5.3.2.3.1.27. Capacidade de resposta/logs ativa a ataques;
- 7.5.3.2.3.1.28. Terminação de sessões via TCP resets;
- 7.5.3.2.3.1.29. Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
- 7.5.3.2.3.1.30. O Sistema de detecção de Intrusos deverá atenuar os efeitos dos ataques de negação de serviços;
- 7.5.3.2.3.1.31. Possuir filtros de ataques por anomalias;
- 7.5.3.2.3.1.32. Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;
- 7.5.3.2.3.1.33. Permitir filtros de anomalias de protocolos;
- 7.5.3.2.3.1.34. Suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;
- 7.5.3.2.3.1.35. Suportar verificação de ataque nas camadas de aplicação;

7.5.3.2.3.2. Das Funcionalidades Do Threat Protection

- 7.5.3.2.3.2.1. Possuir funções de Antivírus, Anti-spyware;
- 7.5.3.2.3.2.2. 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;
- 7.5.3.2.3.2.3. Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.)
- 7.5.3.2.3.2.4. Permitir o bloqueio de download de arquivos por extensão e tipo de arquivo;

7.5.3.2.4. Solução de Gerenciamento Centralizado de Firewall

7.5.3.2.4.1. Funcionalidades de Gerenciamento

- 7.5.3.2.4.1.1. 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;
- 7.5.3.2.4.1.2. A solução de gerenciamento centralizado deve possibilitar o gerenciamento de todos os Firewall contratados.
- 7.5.3.2.4.1.3. A solução de gerenciamento centralizado deverá ser do mesmo fabricante da solução de segurança.
- 7.5.3.2.4.1.4. 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;

- 7.5.3.2.4.1.5. Centralizar a administração de regras e políticas do(s) cluster(s), usando uma única interface de gerenciamento;
- 7.5.3.2.4.1.6. A solução deverá permitir seu gerenciamento por: CLI (Command Line Interface) via SSH, Web GUI utilizando protocolo HTTPS ou console gráfica;
- 7.5.3.2.4.1.7. 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;
- 7.5.3.2.4.1.8. A solução deve incluir a opção de segmentar a base de regras utilizando rótulos ou títulos de seção para organizar melhor a política facilitando a localização e gestão do administrador;
- 7.5.3.2.4.1.9. 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.
- 7.5.3.2.4.1.10. Deve possibilitar a realização de “backup” e restauração de dados.
- 7.5.3.2.4.1.11. Deve possibilitar a gerência de “logs”, realizando configurações de relatórios de todos os “firewalls” integrados.
- 7.5.3.2.4.1.12. Deve permitir buscas e realizar análise de usuários e grupos, rastreando toda a sua atividade e uso da internet;
- 7.5.3.2.4.1.13. O gerenciamento deve permitir/possuir:
- 7.5.3.2.4.1.14. Criação e administração de políticas de Firewall, Controle de aplicação e IPS, Antivírus e Anti-Malware, Filtro de URL e prevenção contra ameaças avançadas;
- 7.5.3.2.4.1.15. Monitoração de logs;
- 7.5.3.2.4.1.16. Debugging;

- 7.5.3.2.4.1.17. Deve permitir usar palavras chaves para facilitar identificação de regras;
- 7.5.3.2.4.1.18. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
- 7.5.3.2.4.1.19. Autenticação integrada à base de dados local;
- 7.5.3.2.4.1.20. Deve possuir ferramenta para localização de objetos (por exemplo: endereço IP, Range de IP, subrede) na base de regras;
- 7.5.3.2.4.1.21. Criação de regras que fiquem ativas em horário definido;
- 7.5.3.2.4.1.22. Habilidade de upgrade via interface de gerenciamento;
- 7.5.3.2.4.1.23. 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;
- 7.5.3.2.4.1.24. Controle sobre todos os equipamentos da plataforma de proteção em uma única console, com administração de privilégios e funções;
- 7.5.3.2.4.1.25. Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de proteção;
- 7.5.3.2.4.1.26. Deve permitir a criação de objetos e políticas compartilhadas;
- 7.5.3.2.4.1.27. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões Leitura/Escrita e somente Leitura;
- 7.5.3.2.4.1.28. Solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credenciais;
- 7.5.3.2.4.1.29. A solução deve permitir gerenciar templates customização visual e marca do produto pelo sistema de gerenciamento centralizado e permitir aplicar nos NGFW 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);

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

7.5.3.2.4.1.31. 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.

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

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

7.5.3.2.4.1.34. 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.

7.5.3.2.4.1.35. Suportar API para integração com sistemas de terceiros;

7.5.3.2.4.2. Alta Disponibilidade

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

7.5.3.2.4.2.2. O sistema de cluster deve suportar utilizar 02 (duas) interfaces como heartbeat;

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

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

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

7.5.3.2.4.3. Armazenamento e Gerenciamento de Logs e Eventos

- 7.5.3.2.4.3.1. 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;
- 7.5.3.2.4.3.2. 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.
- 7.5.3.2.4.3.3. 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.
- 7.5.3.2.4.3.4. Deverá prover análise de tráfego de rede de modo centralizado;
- 7.5.3.2.4.3.5. Deve possuir análise de tráfego de rede e ameaças por geolocalização;
- 7.5.3.2.4.3.6. Deverá ser capaz de receber os logs e eventos com o objetivo de prover os seguintes tipos de análises:
- 7.5.3.2.4.3.7. Análise de ameaças e incidentes de segurança;
- 7.5.3.2.4.3.8. Análise de tráfego e uso de categorias Web;
- 7.5.3.2.4.3.9. Análise de tráfego e uso de aplicativos;
- 7.5.3.2.4.3.10. Análise de tráfego e ameaças por usuário;
- 7.5.3.2.4.3.11. Análise de desempenho de políticas de segurança;
- 7.5.3.2.4.3.12. A solução ofertada deve ser capaz de fazer o gerenciamento centralizado de logs, consolidação de logs, arquivamento de logs, busca avançada de logs;
- 7.5.3.2.4.3.13. Deverá possuir ferramenta para salvar consultas avançadas;
- 7.5.3.2.4.3.14. Deve possuir relatórios personalizados;
- 7.5.3.2.4.3.15. Deverá ser capaz de efetuar o arquivamento de relatórios;
- 7.5.3.2.4.3.16. Deve possuir agendamento de relatórios;
- 7.5.3.2.4.3.17. Os Relatórios deverão, no mínimo, serem exportados em formatos flexíveis (PDF, CSV);
- 7.5.3.2.4.3.18. Logs e Relatórios de tempo de navegação de sites web Domínios Web;
- 7.5.3.2.4.3.19. Permitir o envio de relatórios por e-mail;
- 7.5.3.2.4.3.20. Relatório por Dispositivo/Consolidado;

7.5.3.2.5. Tabela de Distribuição do Item 1 que trata o tópico 4.8.

SUBTÓPICO DO TR N°	DESCRIÇÃO	QTDE
7.5.3.1.1	APPLIANCE NGFW DE 5 GBPS DE CAPACIDADE DE FIREWALL	157
7.5.3.1.2	APPLIANCE NGFW DE 9.7 GBPS DE CAPACIDADE DE FIREWALL	11
7.5.3.1.3	APPLIANCE NGFW DE 11.8 GBPS DE CAPACIDADE DE FIREWALL	3
7.5.3.1.4	APPLIANCE NGFW DE 19.4 GBPS DE CAPACIDADE DE FIREWALL	2
7.5.3.2.4	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE FIREWALL	1

7.5.3.3. A solução de segurança cibernética de bloqueio de ameaças, conforme ITEM 2 que trata o tópico 4.8, deve possuir as seguintes características:

7.5.3.3.1. Interface e Gestão:

- 7.5.3.3.1.1. Deve ser instalado em equipamento com S.O. Linux, Unix ou BSD.
- 7.5.3.3.1.2. Deve ter uma interface amigável para configuração e gestão.
- 7.5.3.3.1.3. Não deve possuir endereçamento IP nas interfaces pelas quais passam o tráfego internet.
- 7.5.3.3.1.4. Não deve permitir a identificação da existência da solução.
- 7.5.3.3.1.5. Não ser suscetível à exploração externa de possíveis vulnerabilidades no software.
- 7.5.3.3.1.6. Deve permitir instalação de forma transparente, sem necessidade de alterações nas configurações lógicas de rede, IP ou do roteamento do ambiente atual.
- 7.5.3.3.1.7. Deve atuar diretamente no tráfego de entrada da internet.
- 7.5.3.3.1.8. Deve proporcionar proteção abrangente para toda a infraestrutura, desde o firewall podendo incluir os roteadores à internet.
- 7.5.3.3.1.9. O aumento de latência no tráfego de rede não deve ser superior a 5 milésimos de segundo.
- 7.5.3.3.1.10. Deve permitir comunicação com a internet através de proxy.
- 7.5.3.3.1.11. Deve possuir painel para configuração de mecanismo para detecção de acesso indesejado.
- 7.5.3.3.1.12. Deve possuir painel para configuração de origens confiáveis.
- 7.5.3.3.1.13. Deve possuir mecanismo de autoproteção.
- 7.5.3.3.1.14. Deve possuir log de auditoria de tudo que foi feito na solução, devendo no mínimo identificar user, data-hora e atividade realizada.
- 7.5.3.3.1.15. Deve armazenar no mínimo os últimos 8.000 registros de log de auditoria.

7.5.3.3.2. Inteligência Artificial Avançada:

- 7.5.3.3.2.1. Deve ser uma solução baseada em Inteligência Artificial Preditiva.
- 7.5.3.3.2.2. Deve ser capaz de analisar padrões de comportamento no tráfego internet.
- 7.5.3.3.2.3. Deve identificar origens maliciosas e neutralizá-las imediatamente automaticamente, sem intervenção humana.

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

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

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

7.5.3.3.2.7. Deve possuir capacidade de aprendizado de acessos indesejados.

7.5.3.3.3. Taxa de Falso Positivo:

7.5.3.3.3.1. 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.

7.5.3.3.4. Proteção Contra Ataques de "Zero Day":

7.5.3.3.4.1. 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.

7.5.3.3.5. Visibilidade:

7.5.3.3.5.1. Deve fornecer visibilidade das origens maliciosas dos ataques.

7.5.3.3.5.2. Deve fornecer visibilidade das tentativas de acessos bloqueadas.

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

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

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

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

7.5.3.3.5.7. 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.

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

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

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

7.5.3.3.6. Relatórios e Integrações:

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

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

7.5.3.3.6.3. 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.

7.5.3.3.6.4. 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.

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

7.5.3.3.6.6. Deve permitir exportar os relatórios para PDF.

7.5.3.3.7. Especificações Técnicas do Equipamento

7.5.3.3.7.1. O equipamento físico deve atender aos seguintes requisitos:

7.5.3.3.7.1.1. Dimensões e Montagem:

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

7.5.3.3.7.1.2. Conectividade:

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

7.5.3.3.7.1.2.2. Deve ter porta console para configuração local.

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

7.5.3.3.7.1.3. Alimentação elétrica:

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

7.5.3.4. Os serviços e equipamentos do ITEM 3 que trata o tópico 4.8 deverão ser entregues no formato e características técnicas bem como funcionalidades conforme especificações abaixo:

7.5.3.4.1. 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 links 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 links não haver impacto na operação como um todo.

- 7.5.3.4.2. 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.
- 7.5.3.4.3. 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.
- 7.5.3.4.4. 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.
- 7.5.3.4.5. 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.
- 7.5.3.4.6. O acesso entre a operadora e o ambiente de TI da CONTRATANTE deverá ser feito exclusivamente por meio de fibra óptica da CONTRATADA.
- 7.5.3.4.7. Devem transportar pacotes IPv4 e IPv6 com no mínimo 1500 bytes sem exigência de fragmentação dos mesmos na camada 3 do modelo OSI.
- 7.5.3.4.8. Os links devem suportar IPv6, sendo necessário o fornecimento de endereçamento para as redes internas do CONTRATANTE.
- 7.5.3.4.9. Deverão ser fornecidos 1 (roteador) por link dedicado que irá compor o ambiente de alta disponibilidade.
- 7.5.3.4.10. Deverá suportar todos os protocolos de roteamento necessários para suportar conexões WANs em ambiente de alta disponibilidade (OSPF, BGP, RIP etc).
- 7.5.3.4.11. Cada equipamento deve possuir no mínimo 2 (duas) interfaces WAN de 1 Gbps (duas) ou mais interfaces LAN de 1 Gbps.
- 7.5.3.4.12. Possuir LEDs de diagnóstico sobre alimentação, atividade e diagnóstico das portas

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

7.5.3.5. Os serviços e equipamentos dos ITENS 4 e 5 que trata o tópico 4.8 deverão ser entregues no formato e características técnicas bem como funcionalidades conforme especificações abaixo:

- 7.5.3.5.1. As velocidades de acesso à internet contratadas serão classificadas da seguinte maneira:
 - 7.5.3.5.1.1. Link principal (item 4 que trata o tópico 4.8): 150Mbps
 - 7.5.3.5.1.2. Link redundante (item 5 que trata o tópico 4.8): 75Mbps
 - 7.5.3.5.1.2.1. A CONTRATADA deverá comprovar que possui capacidade de operar com dois circuitos distintos, em fibra óptica.
 - 7.5.3.5.1.2.2. A CONTRATADA deverá comprovar que possui capacidade operacional através de redes espectrais.
- 7.5.3.5.2. A CONTRATADA deverá garantir largura de banda simétrica (download/upload) de 100% da velocidade contratada, em link único para o link principal (Item 4 que trata o tópico 4.8), não sendo aceita a agregação de múltiplos links para atingir a velocidade contratada.
- 7.5.3.5.3. 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 que trata o tópico 4.8), 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 links em comento, para atingir a velocidade contratada.
- 7.5.3.5.4. A localização e classificação de cada unidade está relacionada nos itens 4.9.1.1, 4.9.1.2 e 4.9.1.3
- 7.5.3.5.5. 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.
- 7.5.3.5.6. 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.

7.5.3.6. Requisitos Tecnológicos Mínimos Para Suportar a Conectividade das Praças

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

7.5.3.6.1.1. **Conectividade:**

- 7.5.3.6.1.1.1. 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;
- 7.5.3.6.1.1.2. Deve possuir 1 porta LAN ethernet 100/1000Base-T em conector RJ45 e com reconhecimento automático de crossover MDI/MDIX;
- 7.5.3.6.1.1.3. 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;
- 7.5.3.6.1.1.4. Deve possuir 2 rádios operando nas frequências de 2,4GHz e 5GHz simultaneamente;
- 7.5.3.6.1.1.5. Deve possuir rádio Bluetooth Low-Energy (BLE) integrado ao equipamento;
- 7.5.3.6.1.1.6. Deve possuir antenas omnidirecionais internas ao equipamento com ganho mínimo de 5 dBi na frequência de 2,4GHz, 6 dBi na frequência de 5GHz;
- 7.5.3.6.1.1.7. Não serão aceitos equipamentos com antenas aparentes (externas ao ponto de acesso) que sejam rosqueáveis, permitindo a remoção das antenas;
- 7.5.3.6.1.1.8. Deve possuir LEDs indicadores de conectividade;

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

- 7.5.3.6.1.2.1. IEEE 802.11a/b/g/n/ac/ax;
- 7.5.3.6.1.2.2. Dupla banda 2,4 e 5GHz simultâneas;
- 7.5.3.6.1.2.3. Deve operar em MIMO 2x2 com suporte a 2 spatial stream e suporte a MU-MIMO;
- 7.5.3.6.1.2.4. 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)

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

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

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

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

a) Access Point;

b) Wireless Mesh;

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

7.5.3.6.1.2.10. Deverá selecionar dinamicamente os canais de operação;

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

7.5.3.6.1.3. Gerenciamento

7.5.3.6.1.3.1. Deve suportar gerenciamento SNMP v2c;

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

7.5.3.6.1.3.3. Deve permitir acesso remoto a console via HTTP e HTTPS;

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

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

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

7.5.3.6.1.3.7. Deve suportar plataforma em nuvem que permita o gerenciamento de pontos de acesso de diferentes fabricantes;

7.5.3.6.1.4. Segurança

7.5.3.6.1.4.1. Deve suportar autenticação através de servidor RADIUS;

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

7.5.3.6.1.4.3. Deve suportar WPA/WPA2 (PSK);

7.5.3.6.1.4.4. Deve suportar WPA3;

7.5.3.6.1.4.5. Deve permitir bloqueio da divulgação do SSID;

7.5.3.6.1.5. Gerais

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

- 7.5.3.6.1.5.2. Deve possuir a classificação IP68 de resistência a intempéries;
- 7.5.3.6.1.5.3. Deve permitir montagem em parede ou poste;
- 7.5.3.6.1.5.4. Deve suportar temperatura de operação entre - 40°C a 60°C;
- 7.5.3.6.1.5.5. Deve suportar sistema operacional em conformidade com o OpenWiFi da Telecom Infra Project;
- 7.5.3.6.1.5.6. 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;
- 7.5.3.6.1.5.7. A controladora deve permitir que o access point seja controlado simultaneamente com access points de diferentes fabricantes
- 7.5.3.6.1.5.8. 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
- 7.5.3.6.1.5.9. A empresa fornecedora deverá possuir atestado de capacidade de implementação de solução equivalente com ecossistema OpenWiFi

7.5.3.6.2. Ponto de Acesso Indoor Wi-Fi 6 2x2

7.5.3.6.2.1. Conectividade

- 7.5.3.6.2.1.1. Deve possuir, no mínimo, 1 porta uplink ethernet 100/1000/2.5G Base-T em conector RJ45 com suporte à alimentação PoE compatível com o padrão IEEE 802.3af e com reconhecimento automático de crossover MDI/MDIX;
- 7.5.3.6.2.1.2. Deve possuir 1 porta LAN ethernet 100/1000Base-T em conector RJ45 e com reconhecimento automático crossover MDI/MDIX;
- 7.5.3.6.2.1.3. 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;
- 7.5.3.6.2.1.4. Deve possuir 1 porta USB;
- 7.5.3.6.2.1.5. Deve possuir 2 rádios operando nas frequências de 2,4GHz e 5GHz simultaneamente;

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

7.5.3.6.2.1.7. 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;

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

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

7.5.3.6.2.2. Funcionalidades WLAN Deve Atender aos Seguintes Padrões:

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

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

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

7.5.3.6.2.2.4. 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)

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

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

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

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

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

a) Access Point;

b) Wireless Mesh;

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

7.5.3.6.2.2.11. Deverá selecionar dinamicamente os canais de operação

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

7.5.3.6.2.3. Gerenciamento

7.5.3.6.2.3.1. Deve suportar gerenciamento SNMP v2c;

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

7.5.3.6.2.3.3. Deve permitir acesso remoto a console via HTTP e HTTPS;

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

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

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

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

7.5.3.6.2.4. Segurança

7.5.3.6.2.4.1. Deve suportar autenticação através de servidor RADIUS;

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

7.5.3.6.2.4.3. Deve suportar WPA/WPA2 (PSK);

7.5.3.6.2.4.4. Deve suportar WPA3;

7.5.3.6.2.4.5. Deve permitir bloqueio da divulgação do SSID;

7.5.3.6.2.4.6. Desempenho

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

7.5.3.6.2.5. Gerais

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

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

7.5.3.6.2.5.3. Deve permitir a instalação de trava tipo Kensington;

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

7.5.3.6.2.5.5. Possuir certificado válido de homologação emitido pela Anatel.

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

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

7.5.3.6.2.5.8. 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;

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

7.5.3.6.2.5.10. 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

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

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

7.5.3.6.3.1. Conectividade

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

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

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

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

7.5.3.6.3.2. PoE

7.5.3.6.3.2.1. 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;

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

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

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

7.5.3.6.3.3. Controle

- 7.5.3.6.3.3.1. Deve suportar Jumbo Frames de 12K;
- 7.5.3.6.3.3.2. Deve suportar até 4K VLANs segundo o protocolo IEEE 802.1Q, por porta e por protocolo;
- 7.5.3.6.3.3.3. Deve suportar implementação de VLANs Privativas;
- 7.5.3.6.3.3.4. Deve suportar implementação de Voice VLANs;
- 7.5.3.6.3.3.5. Deve implementar suporte a QinQ;
- 7.5.3.6.3.3.6. Possuir no mínimo oito filas em hardware para priorização de tráfego por porta;
- 7.5.3.6.3.3.7. Implementar QoS com base no protocolo 802.1p e DSCP;
- 7.5.3.6.3.3.8. Deve implementar controle de fluxo com o protocolo 802.3X e Back Pressure;
- 7.5.3.6.3.3.9. Deve implementar IGMP Snooping v1, v2 e v3;
- 7.5.3.6.3.3.10. Deve implementar IGMP Filtering, Immediate Leave e Querier;
- 7.5.3.6.3.3.11. Deve implementar MLD Snooping;
- 7.5.3.6.3.3.12. Deve possibilitar a limitação de Broadcast, Multicast e Unicast;
- 7.5.3.6.3.3.13. Deve implementar o gerenciamento de banda com valores distintos para entrada e saída;
- 7.5.3.6.3.3.14. Deve implementar os mecanismos de controle de fila: (Strict Priority) e WRR (Weighted Round Robin);

7.5.3.6.3.4. Disponibilidade

- 7.5.3.6.3.4.1. Implementar o protocolo Spanning Tree (802.1D);
- 7.5.3.6.3.4.2. Implementar o protocolo Rapid Spanning Tree (802.1w);
- 7.5.3.6.3.4.3. Deve implementar o protocolo Multiple Spanning Tree (802.1s);
- 7.5.3.6.3.4.4. Deve suportar detecção de laço (loopback detection);
- 7.5.3.6.3.4.5. Deve implementar BPDU Guard/Filter e ROOT Guard;
- 7.5.3.6.3.4.6. Deve suportar até 8 grupos de agregação dinâmicos padrão LACP ou estático de até 8 portas GbE;

7.5.3.6.3.5. Gerenciamento

- 7.5.3.6.3.5.1. Deve possuir suporte a pilha dupla de protocolo IPv4/IPv6;
- 7.5.3.6.3.5.2. Deve suportar gerenciamento SNMP v1, v2c e v3;

- 7.5.3.6.3.5.3. Deve permitir configuração dos parâmetros IP através de serviço DHCP Cliente;
- 7.5.3.6.3.5.4. Deve permitir acesso remoto a console via Telnet, SSHv2, HTTP e HTTPS;
- 7.5.3.6.3.5.5. 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);
- 7.5.3.6.3.5.6. Deve permitir acesso local a console CLI;
- 7.5.3.6.3.5.7. Deve permitir atualização e provisionamento automáticos, podendo este ser executado por sistema de gestão externo sendo, neste caso, necessário proporcionar a solução completa;
- 7.5.3.6.3.5.8. Deve suportar os grupos 1, 2, 3 e 9 de RMON;
- 7.5.3.6.3.5.9. Deve suportar o protocolo LLDP (IEEE 802.1ab);
- 7.5.3.6.3.5.10. Deve permitir armazenar no mínimo duas imagens de firmware em memória flash interna;
- 7.5.3.6.3.5.11. Deve permitir a atualização de firmware via HTTP, TFTP ou FTP em memória tipo flash;
- 7.5.3.6.3.5.12. Deve permitir armazenar no mínimo duas configurações distintas em memória flash interna;
- 7.5.3.6.3.5.13. Deve permitir salvar as configurações em um computador local (backup) via HTTP, TFTP ou FTP;
- 7.5.3.6.3.5.14. Deve suportar espelhamento de tráfego;
- 7.5.3.6.3.5.15. Deve suportar SNMP over IPv6;
- 7.5.3.6.3.5.16. Deve suportar HTTP over IPv6;
- 7.5.3.6.3.5.17. Deve suportar IPv6 remote ping;
- 7.5.3.6.3.5.18. Deve suportar NTP ou SNTP;
- 7.5.3.6.3.5.19. Deve implementar log de eventos em memória flash e permitir a gravação em servidor externo padrão Syslog;
- 7.5.3.6.3.6. Segurança**
- 7.5.3.6.3.6.1. Deve possuir proteção a ataques Denial of Service;
- 7.5.3.6.3.6.2. Deve suportar autenticação local e através de servidor RADIUS e TACACS+;
- 7.5.3.6.3.6.3. Deve implementar segurança de acesso através do protocolo IEEE 802.1X e autenticação por MAC;

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

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

7.5.3.6.3.6.6. Deve suportar implementação de VLANs para visitantes;

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

7.5.3.6.3.6.8. Deve suportar DHCP snooping;

7.5.3.6.3.6.9. Deve suportar IP Source Guard;

7.5.3.6.3.6.10. Deve possuir Port Security ou funcionalidade similar;

7.5.3.6.3.6.11. Deve possuir Dynamic ARP Inspection ou funcionalidade similar;

7.5.3.6.3.6.12. Deve implementar MAC based ACL;

7.5.3.6.3.7. **Desempenho**

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

7.5.3.6.3.7.2. Deve chavear no mínimo 59 Mpps;

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

7.5.3.6.3.7.4. Funções camada 3

7.5.3.6.3.7.5. Deve implementar rotas estáticas;

7.5.3.6.3.7.6. Deve implementar o protocolo RIP;

7.5.3.6.3.8. **Padronização**

7.5.3.6.3.8.1. 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)

7.5.3.6.3.9. **Gerais**

- 7.5.3.6.3.9.1. Deve possuir fonte de alimentação interna operando em tensões de 100 a 240 V e em frequências de 50 a 60 Hz automaticamente;
- 7.5.3.6.3.9.2. Deve vir acompanhado do kit de suporte específico para montagem em Rack de 19;
- 7.5.3.6.3.9.3. O equipamento deverá ocupar uma unidade de rack;
- 7.5.3.6.3.9.4. Deve possuir temperatura de operação de 0° C a 50° C;
- 7.5.3.6.3.9.5. Deve possuir sistema operacional OpenLan Switching (OLS) em conformidade com as especificações da Telecom Infra Project (TIP);
- 7.6. 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.
- 7.7. O caráter confidencial das informações dos usuários será garantido, não podendo ser compartilhado, em nenhuma hipótese, inclusive para uso comercial, publicitário ou estatístico.
- 7.8. 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.
- 7.9. O SSID da rede não poderá associar o nome do eventual contratante privado.
- 7.10. O formato do SSID será definido pela Prefeitura Municipal de Cáceres / Coordenação de Tecnologia da Informação (CTI).
- 7.11. 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.
- 7.12. 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.
- 7.13. Ao pressionar o botão destinado à conexão com a internet pela primeira vez, ele será transferido para a página de cadastro definido pela Contratante;
- 7.14. Que os usuários não tenham acesso a equipamentos de outros usuários conectados à rede WI-FI.
- 7.15. 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.

- 7.16. 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.
- 7.17. 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.
- 7.18. 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.
- 7.19. 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.
- 7.20. Cada aparelho de acesso das Praças deverá aceitar até 500 conexões simultâneas, dividindo assim a banda de internet 100mbs igualmente para os visitantes.
- 7.21. 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.
- 7.22. 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).
- 7.23. 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 anomalias na operação da infraestrutura de comunicação da rede Wi-Fi
- 7.24. A Contratada deverá fornecer uma banda de internet de 150 Mbps dedicada para cada ponto instalado.
- 7.25. O funcionamento de cada praça ofertada será por 24 (vinte e quatro) horas por dia, durante 7 (sete) dias por semana.
- 7.26. 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.
- 7.27. 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, 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.

8. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO

8.1. Tendo em vista a complexidade e a natureza integrada dos serviços e soluções tecnológicas especificadas neste Termo de Referência, bem como os requisitos de negócio previamente estabelecidos, conclui-se que o parcelamento da contratação não é viável.

Essa decisão fundamenta-se na necessidade de garantir a uniformidade, compatibilidade técnica e integração plena dos diversos componentes da solução, abrangendo serviços de segurança cibernética com Inteligência Artificial Preditiva, implementação da tecnologia Next Generation Firewall (NGFW), soluções SD-WAN, fornecimento de links dedicados, conectividade para unidades externas, suporte técnico contínuo e capacitação especializada da equipe do Contratante.

O fracionamento da contratação poderia comprometer a eficiência operacional, ocasionando divergências técnicas, dificuldades na gestão unificada das políticas de segurança e riscos à continuidade dos serviços críticos. Ressalta-se que a interdependência entre os serviços e equipamentos fornecidos exige uma responsabilidade técnica centralizada, garantindo que incidentes ou falhas sejam tratados de forma ágil e coordenada.

Além disso, para garantir a fluidez na implantação dos serviços, a execução deverá ser realizada por uma única empresa homologada, credenciada e solidariamente vinculada ao fabricante, assegurando a conformidade com os padrões técnicos exigidos e o cumprimento integral dos prazos estabelecidos no Edital.

Dessa forma, a contratação de forma global, sob a responsabilidade de um único fornecedor, apresenta-se como a alternativa mais eficiente e segura, proporcionando coerência na execução, atendimento integral aos requisitos de negócio e otimização dos recursos públicos, em conformidade com os princípios da economicidade, eficiência e continuidade do serviço público.

ASPECTO	PARCELAMENTO DA CONTRATAÇÃO	CONTRATAÇÃO GLOBAL (ÚNICO FORNECEDOR)
Uniformidade e Compatibilidade Técnica	Risco de divergências técnicas entre fornecedores distintos	Maior compatibilidade e integração entre os componentes
Gestão das Políticas de Segurança	Dificuldade na gestão unificada e riscos de inconsistência	Gestão centralizada e padronização das políticas de segurança
Resposta a Incidentes e Suporte Técnico	Resolução mais lenta devido à divisão de responsabilidades	Resposta ágil e coordenada com SLA rigoroso
Eficiência Operacional	Possibilidade de falhas na comunicação entre fornecedores	Maior eficiência operacional e continuidade dos serviços
Gestão Administrativa	Aumento da carga administrativa para coordenação de múltiplos contratos	Simplificação da gestão com um único contrato
Conformidade com Padrões Técnicos do Edital	Maior dificuldade em garantir a conformidade entre fornecedores distintos	Garantia de conformidade com os padrões técnicos exigidos
Riscos de Descontinuidade dos Serviços	Maior risco de interrupção devido à falta de integração	Continuidade assegurada por um fornecedor responsável
Otimização dos Recursos Públicos	Possível aumento de custos devido à fragmentação da contratação	Melhor relação custo-benefício com redução de despesas
Execução do Projeto e Cumprimento de Prazos	Risco de atrasos devido à necessidade de coordenação entre diferentes partes	Execução fluida e cumprimento dos prazos estabelecidos

Essa abordagem evidencia que a contratação global oferece vantagens significativas em termos de eficiência, segurança e otimização dos recursos públicos, consolidando-se como a solução mais adequada para atender às necessidades da Prefeitura Municipal de Cáceres.

9. DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS EM TERMOS DE ECONOMICIDADE E DE MELHOR APROVEITAMENTO DOS RECURSOS HUMANOS, MATERIAIS E FINANCEIROS DISPONÍVEIS

9.1. O sucesso da execução deste contrato será medido por sua capacidade de gerar resultados tangíveis em termos de economicidade, eficiência e otimização dos recursos públicos. Com a adoção de critérios rigorosos de avaliação e indicadores de desempenho, espera-se não apenas alcançar a melhor utilização dos recursos humanos, materiais e financeiros, mas também garantir que a entrega dos serviços seja realizada com o mais alto nível de qualidade e dentro dos prazos estabelecidos.

9.1.1. Critérios de Acompanhamento e Avaliação dos Resultados

A implementação dos critérios de acompanhamento será essencial para garantir a transparência e a responsabilização de todas as partes envolvidas na execução do contrato. Os principais pontos a serem observados incluem:

- **Relatório de Publicação:** A cada 30 dias, a Contratada deverá apresentar um relatório detalhado, que inclua as atividades executadas, dados sobre a execução dos serviços e observações técnicas. Caso o relatório não atenda aos requisitos estabelecidos, será solicitado à Contratada que refaça e apresente uma versão corrigida no prazo estipulado.
- **Aferição pelo Fiscal:** O Fiscal responsável realizará uma análise rigorosa dos serviços prestados, verificando a conformidade com as especificações contratuais e garantindo que os prazos e padrões técnicos sejam atendidos.
- **Identificação de Irregularidades:** Caso sejam identificadas falhas na documentação ou na execução dos serviços, a Contratada será formalmente notificada para que proceda com as devidas correções dentro do prazo de 5 (cinco) dias úteis, sob pena de aplicação das penalidades previstas.
- **Avaliação da Qualidade dos Serviços:** A qualidade dos serviços será monitorada mensalmente, assegurando que as obrigações contratuais sejam cumpridas de acordo com os padrões estabelecidos, com a eficiência exigida.

9.1.1.1. Tabela: Critérios de Acompanhamento e Avaliação

CRITÉRIO DE ACOMPANHAMENTO	DESCRIÇÃO	PERIODICIDADE	RESPONSÁVEL	OBJETIVO
Relatório de Publicação	Relatório detalhado sobre as atividades realizadas, dados e ocorrências	Mensal	Contratada	Garantir a transparência e rastreabilidade dos serviços
Aferição pelo Fiscal	Verificação da execução dos serviços conforme o Termo de Referência	Mensal	Fiscal Designado	Assegurar que os serviços atendam aos requisitos técnicos
Identificação de Irregularidades	Correção de falhas na documentação e execução de serviços	Quando necessário	Fiscal Designado	Garantir a conformidade com o contrato e a legislação
Avaliação de Qualidade dos Serviços	Avaliação contínua da qualidade dos serviços conforme as especificações	Mensal	Fiscal Designado	Assegurar que os padrões técnicos e operacionais sejam atendidos

9.1.2. Resultados Pretendidos e Benefícios Esperados

Os resultados esperados com a execução do contrato visam a otimização dos recursos públicos e a melhoria na prestação dos serviços. Os principais benefícios esperados incluem:

- **Maximização da Utilização dos Recursos Públicos:** A implementação de soluções integradas e a gestão centralizada dos serviços visam evitar desperdícios e garantir que os recursos materiais, financeiros e humanos sejam utilizados da forma mais eficiente possível.
- **Redução de Custos Operacionais:** A contratação de um único fornecedor e a centralização dos serviços evitarão custos adicionais relacionados à gestão de múltiplos contratos e fornecedores, reduzindo a complexidade e aumentando a eficiência.
- **Eficiência na Execução:** A gestão integrada e o acompanhamento constante garantirão que as atividades sejam realizadas dentro do prazo, com qualidade e com o melhor aproveitamento dos recursos disponíveis.
- **Segurança e Continuidade:** A contratação de serviços com tecnologia de ponta, como segurança cibernética avançada e soluções de conectividade, assegurará a continuidade das operações essenciais, além de manter os serviços protegidos contra ameaças externas.

9.1.2.1. Tabela: Resultados Esperados e Benefícios

RESULTADO ESPERADO	BENEFÍCIO ESPERADO	INDICADOR DE SUCESSO
Maximização da Utilização dos Recursos	Uso mais eficiente de recursos materiais, financeiros e humanos	Redução de custos operacionais em até 10%
Redução de Custos Operacionais	Eliminação de contratos fragmentados e custos relacionados à gestão	Diminuição do número de fornecedores e contratos
Eficiência na Execução dos Serviços	Melhoria nos prazos de entrega e na qualidade dos serviços prestados	Cumprimento de 100% dos prazos acordados
Segurança e Continuidade	Garantia da proteção dos serviços e continuidade das operações críticas	100% de uptime nas operações essenciais

9.1.3. Demonstrativo dos Indicadores e Metas de Desempenho

9.1.3.1. A avaliação do desempenho será feita por meio de indicadores claros e metas estabelecidas para medir o sucesso do contrato. Estes indicadores serão essenciais para garantir que os objetivos de economicidade e eficiência sejam atingidos.

INDICADOR DE DESEMPENHO	META DE RESULTADO	PERIODICIDADE	CRITÉRIO DE SUCESSO
Relatório de Publicação	Apresentação dentro do prazo de 30 dias e completo	Mensal	100% de conformidade na entrega de relatórios
Aferição dos Serviços	Conformidade total com as especificações contratuais	Mensal	100% de conformidade nas aferições dos serviços
Identificação de Irregularidades	Correção de falhas em até 5 dias úteis	Conforme necessário	100% de falhas corrigidas dentro do prazo estipulado
Avaliação da Qualidade dos Serviços	Superar 95% de conformidade com os padrões exigidos	Mensal	95% de conformidade com os padrões técnicos
Aproveitamento de Recursos Públicos	Redução de 10% nos custos operacionais totais	Contínuo	Redução de 10% nos custos totais

9.1.3.2. Tabela: Indicadores e Metas de Desempenho

INDICADOR	META DE DESEMPENHO	PERIODICIDADE	OBJETIVO
Relatório de Publicação	100% dos relatórios entregues no prazo	Mensal	Assegurar a transparência e rastreabilidade

Aferição de Serviços	Conformidade total nas aferições realizadas	Mensal	Garantir a execução conforme especificado
Identificação de Irregularidades	Correção de falhas no prazo de 5 dias úteis	Conforme necessário	Agilidade na resolução de falhas e inconsistências
Avaliação da Qualidade	Superar 95% de conformidade com os padrões técnicos	Mensal	Garantir a qualidade constante dos serviços
Aproveitamento de Recursos Públicos	Redução de 10% nos custos totais operacionais	Contínuo	Maximizar a utilização de recursos disponíveis

9.2. A abordagem estruturada para o acompanhamento e a avaliação dos resultados da contratação tem como objetivo primordial garantir a economicidade e a eficiência na utilização dos recursos públicos. Com o uso de indicadores de desempenho claros e metas rigorosas, será possível maximizar o aproveitamento dos recursos materiais, humanos e financeiros, além de assegurar que os serviços sejam prestados com qualidade e dentro dos parâmetros exigidos. A implementação bem-sucedida desse modelo de gestão resultará em uma gestão pública mais eficiente, segura e econômica, alinhada com os princípios da administração pública.

10. INDICAÇÃO DAS RESTRIÇÕES INTERNAS E DAS PROVIDÊNCIAS A SEREM ADOTADAS PREVIAMENTE À CELEBRAÇÃO DO CONTRATO

10.1. A contratação dos serviços descritos neste estudo preliminar representa uma iniciativa estratégica para a Prefeitura Municipal de Cáceres-MT, com o objetivo de assegurar elevados níveis de segurança cibernética, eficiência operacional e qualidade na prestação dos serviços públicos. Para garantir a eficácia dessa contratação, é fundamental que a Administração tome providências essenciais antes da celebração do contrato.

10.1.1. Providências Preparatórias

Antes da formalização do contrato, as seguintes ações devem ser adotadas:

- **Verificação da Disponibilidade Orçamentária e Financeira:** A Administração deve assegurar que os recursos financeiros necessários estão disponíveis, conforme o orçamento aprovado para o exercício, garantindo a viabilidade da contratação.
- **Análise da Conformidade Técnica:** A solução a ser contratada deve ser rigorosamente analisada quanto à sua adequação às necessidades do município e à conformidade com os requisitos técnicos especificados no Termo de Referência.
- **Adequação às Normativas Vigentes:** Deve-se garantir que a contratação esteja em conformidade com a legislação vigente, incluindo a Lei nº 14.133/2021 e outras normas relacionadas à gestão pública, assegurando legalidade e transparência no processo.
- **Observância dos Princípios Administrativos:** Durante o processo de contratação, a Administração deve observar os princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência, essenciais para a boa gestão pública.

10.1.2. Instrumento Contratual e Transparência

Será elaborado um instrumento contratual que estabelecerá de forma clara e detalhada as obrigações e responsabilidades das partes envolvidas, garantindo a transparência do processo e a segurança jurídica dos envolvidos. Esse contrato deverá refletir as expectativas da Administração, alinhando as soluções tecnológicas inovadoras, confiáveis e sustentáveis às necessidades da Prefeitura de Cáceres.

cumprimento das disposições legais aplicáveis será rigorosamente observado, garantindo que a contratação esteja em consonância com as diretrizes estratégicas da Administração Pública e as melhores práticas de governança.

10.1.3. Capacitação da Equipe para Fiscalização e Gestão Contratual

Além das providências legais e operacionais, será planejada a capacitação da equipe responsável pela fiscalização e gestão do contrato. Essa capacitação incluirá treinamentos sobre a gestão de contratos administrativos, acompanhamento de indicadores de desempenho e análise de conformidade com os termos contratuais. A preparação da equipe de fiscalização é essencial para garantir a correta execução dos serviços contratados, assegurar a utilização eficiente dos recursos públicos e garantir a transparência na prestação de contas.

10.1.4. Tabela: Providências a Serem Adotadas pela Administração

PROVIDÊNCIA	DESCRIÇÃO	RESPONSÁVEL	PRAZO
Verificação Orçamentária e Financeira	Assegurar a disponibilidade de recursos no orçamento	Administração	Antes da celebração
Análise de Conformidade Técnica	Verificar a adequação técnica da solução às necessidades do município	Administração	Antes da celebração
Adequação às Normativas Vigentes	Garantir conformidade com a legislação e normas aplicáveis	Administração	Antes da celebração
Observância dos Princípios Administrativos	Assegurar o cumprimento dos princípios da gestão pública	Administração	Durante o processo
Elaboração do Instrumento Contratual	Definir claramente as obrigações e responsabilidades das partes	Administração	Antes da celebração
Planejamento da Capacitação	Planejar e executar treinamentos para a equipe de fiscalização	Administração	Antes da celebração

10.2. As providências a serem adotadas previamente à celebração do contrato são essenciais para garantir que a contratação seja realizada de forma eficiente, legal e transparente, alinhada aos objetivos estratégicos da Prefeitura de Cáceres. A capacitação da equipe de fiscalização e gestão contratual, aliada ao planejamento e à análise rigorosa da conformidade técnica e financeira, contribuirá para o sucesso da implementação das soluções tecnológicas, garantindo a eficiência no uso dos recursos públicos e a continuidade da prestação de serviços públicos de qualidade.

11. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

11.1. Definição de Contratações Correlatas e Interdependentes

As contratações correlatas são aquelas cujos objetos apresentam características semelhantes ou estão diretamente relacionadas entre si, podendo ser agrupadas ou tratadas de forma conjunta devido à sua natureza compatível. Já as contratações interdependentes referem-se àquelas que, embora possam ter objetos distintos, estão diretamente conectadas à execução do objeto principal, de modo que a realização de uma contratação depende da efetivação da outra para garantir a plena satisfação da necessidade da Administração.

11.2. Necessidade de Contratações Correlatas e Interdependentes

Ao realizar a análise das necessidades da Administração Municipal, visando à contratação da solução integrada de segurança cibernética com Inteligência Artificial preditiva, tecnologia Next Generation Firewall (NGFW).

soluções SD-WAN, fornecimento de links dedicados, conectividade para unidades externas, suporte técnico contínuo e capacitação da equipe interna, constatou-se a inexistência de outras contratações correlatas ou interdependentes necessárias para o pleno atendimento ao objeto pretendido. Em outras palavras, a solução contratada é suficientemente abrangente para garantir a eficácia da proteção da infraestrutura de TIC e a continuidade dos serviços digitais de forma independente.

11.3. Justificativa para a Ausência de Necessidade de Outras Contratações

A solução proposta já contempla todos os serviços e componentes necessários para assegurar o funcionamento pleno da infraestrutura tecnológica da Prefeitura, eliminando a necessidade de contratações adicionais. O escopo da contratação inclui o fornecimento de equipamentos, a implementação das tecnologias de segurança e conectividade, além do suporte técnico especializado e da capacitação contínua da equipe interna, garantindo a autonomia da Administração Municipal na gestão dos serviços contratados.

Além disso, a empresa vencedora do certame será integralmente responsável pela entrega, integração e manutenção de todos os elementos da solução, conforme especificado no objeto do contrato, assegurando a uniformidade e a compatibilidade técnica dos serviços prestados. Dessa forma, não há dependência de serviços externos ou aquisições complementares para viabilizar a plena execução do objeto contratado.

11.4. Diante do exposto, verifica-se que não há necessidade de contratações correlatas ou interdependentes para a execução do objeto em questão. A solução de segurança cibernética, conectividade e suporte técnico, a ser fornecida pela empresa contratada, abrange todos os recursos indispensáveis para garantir a proteção da infraestrutura de TIC da Prefeitura e a continuidade dos serviços públicos digitais, de forma eficaz, integrada e econômica.

12. DESCRIÇÃO DE POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS MITIGADORAS, INCLUÍDOS REQUISITOS DE BAIXO CONSUMO DE ENERGIA E DE OUTROS RECURSOS, BEM COMO LOGÍSTICA REVERSA PARA DESFAZIMENTO E RECICLAGEM DE BENS E REFUGOS

12.1. Possíveis Impactos Ambientais

A implementação da solução integrada de segurança cibernética com Inteligência Artificial preditiva, tecnologia Next Generation Firewall (NGFW), soluções SD-WAN, fornecimento de links dedicados, conectividade para unidades externas e suporte técnico contínuo pode gerar impactos ambientais, especialmente em relação ao consumo de energia e ao descarte de materiais eletrônicos obsoletos. Esses impactos podem ser classificados da seguinte forma:

- **Consumo de Energia:** A operação contínua dos servidores, equipamentos de segurança e dispositivos de conectividade pode resultar em aumento do consumo de energia elétrica, especialmente para manter a infraestrutura tecnológica em funcionamento.
- **Geração de Resíduos Eletrônicos:** O descarte de equipamentos antigos e componentes danificados durante a instalação e manutenção gera resíduos eletrônicos que demandam descarte adequado.

- **Uso de Recursos Naturais:** A fabricação e o transporte dos equipamentos envolvem o uso de recursos naturais, como metais e plásticos, além do consumo de energia durante o processo produtivo e logístico.

12.2. Medidas Mitigadoras

Para mitigar os impactos ambientais decorrentes da implementação da solução, serão adotadas as seguintes medidas:

12.2.1. Requisitos de Baixo Consumo de Energia:

- Os equipamentos fornecidos deverão possuir certificação de eficiência energética, visando minimizar o consumo de energia elétrica.
- A solução SD-WAN, ao otimizar a transmissão de dados, contribuirá para a redução do consumo energético nas unidades externas.
- Implementação de dispositivos com funcionalidades de economia de energia, incluindo modos de suspensão automática fora do horário de expediente.

12.2.2. Recursos Sustentáveis e Eficiência Operacional:

- O fornecimento dos equipamentos será realizado em regime de comodato, garantindo que, ao final do ciclo de vida útil, os dispositivos retornem à fornecedora para reciclagem ou reaproveitamento.
- Seleção de fornecedores que utilizem materiais recicláveis e adotem práticas sustentáveis em seus processos de produção e transporte.

12.2.3. Logística Reversa e Reciclagem de Bens e Refugos:

- A empresa contratada será responsável pela implementação de um sistema de logística reversa para o retorno dos equipamentos obsoletos, garantindo o descarte ambientalmente correto conforme as normas vigentes.
- Equipamentos não reaproveitáveis serão encaminhados para empresas especializadas na reciclagem de componentes eletrônicos, minimizando o impacto ambiental.

12.2.4. Tabela de Medidas Mitigadoras

IMPACTO AMBIENTAL	MEDIDA MITIGADORA
Consumo excessivo de energia	- Uso de equipamentos com certificação de eficiência energética.
	- Otimização do tráfego de dados via solução SD-WAN.
Geração de resíduos eletrônicos	- Logística reversa para reciclagem ou reaproveitamento de componentes.
	- Redução do descarte por meio do regime de comodato.
Uso excessivo de recursos naturais na fabricação	- Seleção de fornecedores com práticas sustentáveis e materiais recicláveis.
Descarte inadequado de equipamentos antigos	- Encaminhamento dos resíduos a empresas certificadas para reciclagem de eletrônicos.

12.3. O processo de implementação da solução integrada de segurança cibernética foi planejado para minimizar os impactos ambientais associados ao consumo de energia e ao descarte de equipamentos. As medidas adotadas garantem o uso eficiente dos recursos naturais, o descarte responsável dos resíduos eletrônicos e a redução da pegada ecológica da Prefeitura Municipal de Cáceres, assegurando o cumprimento das responsabilidades ambientais e promovendo a sustentabilidade em suas operações tecnológicas.

13. VIGÊNCIA DA CONTRATAÇÃO

13.1. 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 nº 14.133, de 2021.

14. FUNDAMENTAÇÃO LEGAL

- Constituição Federal de 1988;
- Lei nº 14.133/21;
 - Artigo 11, inciso IV;
 - Artigo 114;
 - Artigo 141, inciso III, parágrafo 1º, inciso III;
- Decreto Municipal nº 665/24.

15. POSICIONAMENTO CONCLUSIVO SOBRE A ADEQUAÇÃO DA CONTRATAÇÃO PARA O ATENDIMENTO DA NECESSIDADE A QUE SE DESTINA

15.1. No contexto da formulação e execução de políticas públicas eficazes, a segurança cibernética configura-se como elemento imprescindível para a modernização administrativa e a proteção dos ativos institucionais, notadamente diante da crescente digitalização dos serviços ofertados à população. Nesse cenário, a presente contratação revela-se plenamente justificada e estratégica, haja vista os aspectos técnicos, operacionais e financeiros analisados neste estudo preliminar. A análise de custo-benefício demonstra-se altamente favorável, considerando que todos os requisitos essenciais foram devidamente mapeados, com especial atenção à previsão do prazo necessário para a implantação integral e a plena operacionalização da solução tecnológica no âmbito da Administração Municipal.

Ressalte-se que o processo de contratação em curso encontra-se rigorosamente em conformidade com os preceitos legais e normativos estabelecidos na Lei nº 14.133/2021, na Constituição Federal e no Decreto Municipal nº 665/2024, evidenciando a observância aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência. Tal alinhamento não apenas garante a segurança jurídica do certame, como também reforça a transparência e a responsabilidade administrativa, pilares fundamentais da governança pública.

Convém destacar que o município de Cáceres tem avançado de forma significativa na disponibilização de serviços públicos digitais, proporcionando ao cidadão acesso facilitado e seguro à internet, consolidando, assim, como referência em modernização administrativa. A presente contratação contribuirá diretamente para a continuidade desse processo de transformação digital, assegurando a proteção das informações institucionais e o aprimoramento da eficiência operacional dos órgãos municipais, em consonância com as melhores práticas de segurança da informação.

Diante do exposto, a Secretaria Municipal Especial de Assuntos Estratégicos manifesta-se de forma favorável à viabilidade da presente contratação, recomendando a sua efetivação por meio de pregão eletrônico, tendo como critério de julgamento o menor valor global. Tal diretriz alinha-se aos princípios da economicidade.

eficiência e modernização da Administração Pública, garantindo a sustentabilidade operacional, a otimização dos recursos públicos e a continuidade dos serviços essenciais prestados à população, em plena consonância com o interesse público e os objetivos estratégicos do município de Cáceres.

Cáceres-MT, 25 de fevereiro de 2025.

GIRLANE VIEIRA PEREIRA
Coordenadora de Informações Sistêmicas e Tecnologia de Informação

JEREMIAS PEREIRA LEITE
Secretário Municipal Especial de Assuntos Estratégicos

Assinado por 2 pessoas: GIRLANE VIEIRA PEREIRA e JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321>

MAPA DE RISCOS

DESCRIÇÃO DO OBJETO		
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.		
FASES DA ANÁLISE		
(x) Planejamento da Contratação	(x) Seleção do Fornecedor	(x) Gestão do Contrato

1. PLANEJAMENTO

RISCO 01		
Probabilidade:	() Baixo	(x) Médio () Alto
Impacto:	() Baixo	() Médio (x) Alto
ID	Dano	
1.	Contratação não atende as necessidades	
ID	Ação Preventiva	Responsável
1.	Participação ativa do setor requisitante nas atividades da equipe	Coordenação de Tecnologia de Informação
2.	Acompanhamento e controle, supervisão efetiva	Fiscal de contrato
ID	Ação de Contingência	Responsável
1.	Planejamento para uma nova contratação adequada e rescisão do atual contrato	Coordenação de Tecnologia de Informação / Setor de Compras SMEAE

RISCO 02		
Probabilidade:	() Baixo	(x) Médio () Alto
Impacto:	() Baixo	() Médio (x) Alto
ID	Dano	
1.	Quantificação inadequada da demanda	
ID	Ação Preventiva	Responsável
1.	Requisitar de forma precisa sua real necessidade	Coordenação de Tecnologia de Informação
ID	Ação de Contingência	Responsável
1.	Verificar de forma precisa o quantitativo demandado	Coordenação de Tecnologia de Informação
2.1	Planejamento para uma nova contratação adequada e rescisão do atual contrato	Coordenação de Tecnologia de Informação / Setor de Compras SMEAE

RISCO 03		
Probabilidade:	() Baixo	(x) Médio () Alto
Impacto:	() Baixo	() Médio (x) Alto
ID	Dano	

1.	Descrição inadequada do objeto	
ID	Ação Preventiva	Responsável
1.	Descrição de objeto sucinta, mas objetiva, de acordo com o padrão usual no mercado	Coordenação de Tecnologia de Informação
ID	Ação de Contingência	Responsável
1.	Planejamento para uma nova contratação adequada e rescisão do atual contrato	Coordenação de Tecnologia de Informação / Setor de Compras SMEAE

RISCO 04		
Probabilidade:	() Baixo	() Médio (x) Alto
Impacto:	() Baixo	() Médio (x) Alto
ID	Dano	
1.	Atraso no processo administrativo de contratação	
ID	Ação Preventiva	Responsável
1.	Planejamento de nova contratação antes de vencer o contrato vigente	Coordenação de Tecnologia de Informação
ID	Ação de Contingência	Responsável
1.	Verificar o motivo do atrasado e corrigir	Setor de Aquisição

RISCO 05		
Probabilidade:	(x) Baixo	() Médio () Alto
Impacto:	() Baixo	() Médio (x) Alto
ID	Dano	
1.	Prazo insuficiente para a adequada realização do planejamento da contratação	
ID	Ação Preventiva	Responsável
1.	Planejamento de nova contratação com antecedência de mínimo 4 meses antes de vencer o contrato	Coordenação de Tecnologia de Informação
ID	Ação de Contingência	Responsável
1.	Verificar o motivo do atrasado e corrigir	Setor de Aquisição

2. SELEÇÃO DO FORNECEDOR

RISCO 01		
Probabilidade:	() Baixo	(x) Médio () Alto
Impacto:	() Baixo	() Médio (x) Alto
Id	Dano	
1.	Atraso ou suspensão no processo licitatório em face de impugnações	
Id	Ação Preventiva	Responsável
1.	Edital de acordo com a legislação	Setor de Aquisição
Id	Ação de Contingência	Responsável
1.	O verificar o motivo da impugnação encaminhar para PGM e retificar o edital quando for necessário	Setor de Aquisição / PGM

RISCO 02		
Probabilidade:	() Baixo	(x) Médio () Alto
Impacto:	() Baixo	() Médio (x) Alto
ID	Dano	
1.	Incapacidade operacional da contratada em atender as demandas	
ID	Ação Preventiva	Responsável

1.	O Edital deve prever a exigência de atestado de capacidade técnica compatível com o objeto a ser licitado em quantidade e complexidade	Pregoeiro e equipe de apoio
2.	Capacitar pregoeiro (a)	Gestor da pasta
ID	Ação de Contingência	Responsável
1.	Fazer notificações a empresa, aplicar sanções	Fiscal de Contrato / PGM / Gestor da pasta
2.	Planejamento para uma nova contratação e rescisão do atual contrato	Coordenação de Tecnologia de Informação / Setor de Compras SMEAE

RISCO 03		
Probabilidade:	(x) Baixo	() Médio () Alto
Impacto:	() Baixo	() Médio (x) Alto
ID	Dano	
1.	Edital e anexos com redação inadequada	
ID	Ação Preventiva	Responsável
1.	Revisão do Edital e anexos	Controladoria / PGM / Equipe de apoio da licitação
ID	Ação de Contingência	Responsável
1.	Revogação/anulação da licitação	Gestor da Pasta
2.	Cancelamento da Contratação	Secretaria demandante
3.	Planejamento para uma nova contratação	Coordenação de Tecnologia de Informação / Setor de Compras SMEAE

RISCO 04		
Probabilidade:	(x) Baixo	() Médio () Alto
Impacto:	() Baixo	() Médio (x) Alto
ID	Dano	
1.	Aceitação de proposta em desacordo com o Edital	
ID	Ação Preventiva	Responsável
1.	Capacitar pregoeiro e equipe de apoio	Gestor da pasta
ID	Ação de Contingência	Responsável
1.	Revogação/anulação da licitação	Pregoeiro / Gestor da pasta
2.	Planejamento para uma nova contratação	Coordenação de Tecnologia de Informação / Setor de Compras SMEAE

RISCO 05		
Probabilidade:	(x) Baixo	() Médio () Alto
Impacto:	() Baixo	() Médio (x) Alto
ID	Dano	
1.	Contratação de fornecedor com baixa qualificação técnica	
ID	Ação Preventiva	Responsável
1.	O Edital deve prever a exigência de atestado de capacidade técnica compatível com o objeto a ser licitado em quantidade e complexidade	Setor de Aquisição
2.	Capacitar pregoeiro e equipe de apoio do pregão	Gestor da pasta
ID	Ação de Contingência	Responsável
1.	Revogação/anulação da licitação	Pregoeiro / Gestor da pasta

2.	Planejamento para uma nova contratação	Coordenação de Tecnologia de Informação / Setor de Compras SMEAE
----	--	--

3. GESTÃO DE CONTRATO

RISCO 01		
Probabilidade:	() Baixo	(x) Médio () Alto
Impacto:	() Baixo	(x) Médio () Alto
ID	Dano	
1.	Fiscalização ineficiente do contrato	
ID	Ação Preventiva	Responsável
1.	Capacitar o fiscal	Gestor da Pasta.
2.	Fiscal de contrato com tempo hábil para desempenhar as funções de fiscalização	Fiscal de contrato / Gestor da Pasta
3.	Acompanhamento da Coordenação de Contratos das atividades do fiscal de contrato	Coordenação de Tecnologia de Informação
4.	Documentar o acompanhamento da fiscalização nos autos do processo	Fiscal de contrato
ID	Ação de Contingência	Responsável
1.	Verificar se está sendo feita a real fiscalização do contrato	Gestor da pasta

RISCO 02		
Probabilidade:	() Baixo	() Médio (x) Alto
Impacto:	() Baixo	() Médio (x) Alto
ID	Dano	
1.	Descumprimento das obrigações contratuais pela contratada	
ID	Ação Preventiva	Responsável
1.	Previsão de garantia contratual no Edital e anexos	Setor de Aquisição
2.	Solicitação/exigência de garantia contratual	Setor de Aquisição
3.	Acompanhamento da execução do contrato em relação ao cumprimento das obrigações contratados	Fiscal do contrato / Gestor da pasta
ID	Ação de Contingência	Responsável
1.	Notificar a empresa pelo descumprimento das obrigações	Fiscal do contrato / Gestor da pasta
2.	Proceder à aplicação de sanções administrativas	Gestor da pasta
3.	Planejamento para uma nova contratação e rescisão do atual contrato	Coordenação de Tecnologia de Informação / Setor de Compras SMEAE

RISCO 03		
Probabilidade:	() Baixo	(x) Médio () Alto
Impacto:	() Baixo	() Médio (x) Alto
ID	Dano	
1.	Falta de dotação orçamentária para execução do contrato.	
ID	Ação Preventiva	Responsável
1.	Previsão no PCA e LOA	Coordenação de Tecnologia de Informação
2.	Acompanhamento da execução do orçamento	Coordenação de Tecnologia de Informação
ID	Ação de Contingência	Responsável
1.	Acompanhamento da execução do orçamento	Gestor da pasta

4. CONCLUSÃO DO GESTOR

Diante do exposto, a Secretaria Municipal Especial de Assuntos Estratégicos manifesta-se de forma favorável à viabilidade da presente contratação, recomendando a sua efetivação por meio de pregão eletrônico, tendo como critério de julgamento o menor valor global. Tal diretriz alinha-se aos princípios da economicidade, eficiência e modernização da Administração Pública, garantindo a sustentabilidade operacional, a otimização dos recursos públicos e a continuidade dos serviços essenciais prestados à população, em plena consonância com o interesse público e os objetivos estratégicos do município de Cáceres.

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

Assinado por 2 pessoas: GIRLANE VIEIRA PEREIRA e JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321>

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
1	257560-4	609340	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)	Serviço	173
2		481647	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	Serviço	2
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
4		26484	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 150Mbps Sites Remotos (Fibra Óptica)	Serviço	171
5		26557	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G)	Serviço	171
6	339905-2	1988	Implantação da Solução	Serviço	1
7	404876-8	16837	Capacitação especializada da equipe com emissão de certificação.	Treinamento	1
8	332679-9	27340	Consultoria Política de Segurança	Serviço	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 nº 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.

Assinado por: JANEIRO PEREIRA LIMA
Para verificar a validade das assinaturas, acesse <https://caceres.mt.gov.br/verificacao/34C7-D880-59D2-E321> e informe o código 34C7-D880-59D2-E321

- 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, modems, 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.

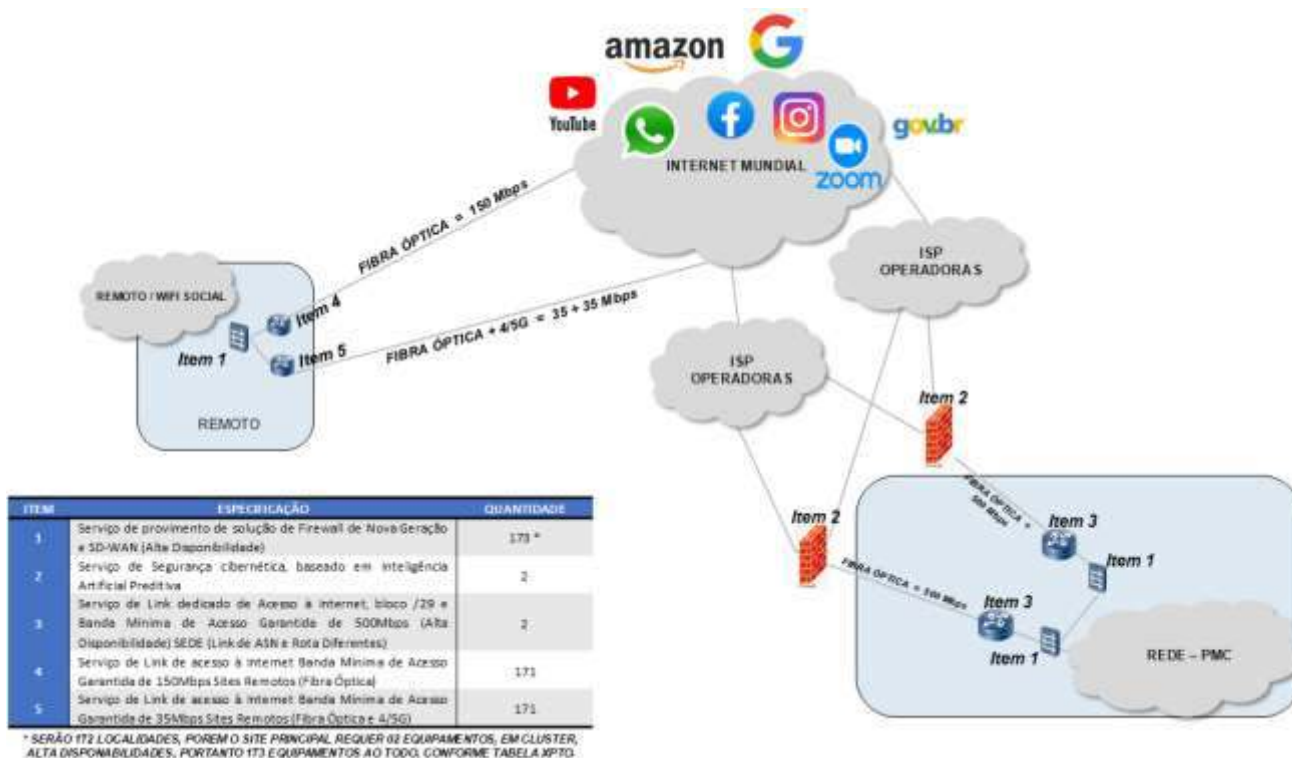
4.5.2.1.1.2. A configuração dos links de internet e a implementação da tecnologia SD-WAN asseguram balanceamento inteligente do tráfego, priorização de pacotes críticos e segurança reforçada para as comunicações entre as unidades.

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:

Assinado por 2 pessoas: GIRLANE VIEIRA PEREIRA e JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321>



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: GILRILANE PEREIRA LEITE
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321>

- 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 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 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 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 a 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 de 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:



- 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;

4.5.3.2.1.1.29. 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;

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

4.5.3.2.1.1.33. Deve implementar o protocolo ECMP;

Assinado por 2 pessoas: GILRANE VIEIRA PEREIRA e JEREMIAS PEREIRA
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321>
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321>



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;

4.5.3.2.1.2.1. 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, integridade, 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 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 fornecer.

Assinado por: GILRILANE PEREIRA JENIAS PEREIRA
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321>



- 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 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 SIMPL (nic.br) medidor de Internet.

Assinado por 2 pessoas: GILRANE VIEIRA PEREIRA, e JEREMIAS PEREIRA LEITE
 Para verificar a validade das assinaturas, acesse <https://ltda.com.br/verificacao/3447-D880-59D2-E321> e informe o código 3447-D880-59D2-E321

- 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, LDAS, 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;

Assinado por 2 pessoas: JEREMIAS PEREIRA LEITE e JEREMIAS PEREIRA LEITE. Para verificar a validade das assinaturas, acesse https://caceres.mt.gov.br/verificacao/34C7-D880-59D2-E321 e informe o código 34C7-D880-59D2-E321

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 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;

Assinado por 2 pessoas: GIRLANE VIEIRA PEREIRA, SUJEREMIAS PEREIRA DE
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321> e informe o código 34C7-D880-59D2-E321

- 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 capazes 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 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 roteamento, entre o peer (NGFW local) e o host;

Assinado por: ANE VIEIRA PEREIRA e JEREMIAS PEREIRA
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321>

- 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 por 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 usuários 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;

Assinado por 2 pessoas: GIRILANE VIEIRA PEREIRA e JEREMIAS PEREIRA. Para verificar a validade das assinaturas, acesse <https://caceres.mt.gov.br/verificacao/34C7-D880-59D2-E321>

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 à 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:

Assinado por: JAILANE PEREIRA e JEREMIAS PEREIRA
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321>

- 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;

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

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

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

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

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

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

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

4.5.3.2.2.23. 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 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;

Assinado por 2 pessoas: GILVANE VIEIRA PEREIRA e JEREMIAS PEREIRA
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321>

- 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);

Assinado por: GIRILANE VIEIRA PEREIRA e JEREMIAS PEREIRA
Para verificar a validade das assinaturas, acesse <https://caceres.mt.gov.br/verificacao/34C7-D880-59D2-E321>

- 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 da 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.

Assinado por 2 pessoas: GUILANE VIEIRA PEREIRA e JESSICA PEREIRA
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321> e informe o código 34C7-D880-59D2-E321

- 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;

Assinado por 2 pessoas: GILRILANE VEIIRA PEREIRA, JEREMIAS PEREIRA
Para verificar a validade das assinaturas, acesse <https://caceres.mt.gov.br/verificacao/34C7-D880-59D2-E321> e informe o código 34C7-D880-59D2-E321

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 credenciais;

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 (Identity Provider - IDP) estabelecendo 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

Assinado por 2 pessoas: 02/09/2025 10:47:46
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321>

- 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 heartbeat;
- 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 entregue 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;

Assinado por 2 pessoas: GIRILANE VIEIRA PEREIRA e JEREMIAS PEREIRA
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321>

- 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 de 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 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 possuem "assinatura de identificação" ou "patch de correção" dos fabricantes e 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.



- #### 4.5.3.3.6. Relatórios e Integrações:

- #### 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 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 o 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

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:

Assinado por 2 pessoas: GILVANE VIEIRA PEREIRA e JEREMIAS PEREIRA LEITE. Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321> e informe o código 34C7-D880-59D2-E321

- 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 do 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 NTP ou SNTP;

Assinado por 2 pessoas: GILRILANE PEREIRA e JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321> e informe o código 34C7-D880-59D2-E321

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

Assinado por 2 pessoas: GUILANE VELOSO PEREIRA e JEREMIAS PEREIRA
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321>

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 simultaneamente;
- 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)

Assinado por 2 pessoas: GIRILANE VIEIRA PEREIRA, JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321>

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 permita 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;

Assinado por 2 pessoas: GÍRLANE VIEIRA PEREIRA e JEREMIAS PEREIRA. Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321>

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

Assinado por 2 pessoas: GIRILANE PEREIRA ALMEIDA, PEREIRA ALMEIDA, PEREIRA ALMEIDA
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321> e informe o código 34C7-D880-59D2-E321

- 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;

Assinado por 2 pessoas: GURILANE VIEIRA e JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321>

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, SSH, HTTP e HTTPS;

4.5.3.6.3.5.5. Deve permitir configuração através de plataforma de gerenciamento em nuvem com suporte a OpenLine 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);

Assinado por 2 pessoas: GILRILANE PEREIRA e JEREMIAS PEREIRA. Para verificar a validade das assinaturas, acesse <https://caceres.mt.gov.br/verificacao/34C7-D880-59D2-E321>

- 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;

Assinado por 2 pessoas: GILVANE VIEIRA PEREIRA e JEREMIAS PEREIRA. Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321> e informe o código 34C7-D880-59D2-E321

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 Teleco 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 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.



- Assinado por 2 pessoas: GIRLENE VIEIRA PEREIRA e 10 PEREMIAS PEREIRA. Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321> e informe o código 34C7-D880-59D2-E321.



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 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.

Assinado por 2 pessoas: GIRLANE VIEIRA PEREIRA e JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse <https://caceres.mt.gov.br/verificacao/34C7-D880-59D2-E321> e informe o código 34C7-D880-59D2-E321

- 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.

Assinado por 2 pessoas: GILVANE VIEIRA PEREIRA e JENIFERAS PEREIRA LACERDA. Para verificar a validade das assinaturas, acesse <https://caceres.mt.gov.br/verificacao/34C7-D880-59D2-E321> e informe o código 34C7-D880-59D2-E321

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, 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	Não Emergencial	Até 24 horas	Conforme cronograma	Suporte remoto ou presencial agendado.

	equipamentos.				
--	---------------	--	--	--	--

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.

Assinado por 2 pessoas: GIRLANE VIEIRA PEREIRA e JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321> e informe o código 34C7-D880-59D2-E321

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 (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 incluam 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:

Assinado por 2 pessoas: GILBERTO VIEIRA PEREIRA e JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321>

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

Assinado por 2 pessoas: GILBERTO VIEIRA PEREIRA e JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321> e informe o código 34C7-D880-59D2-E321

- 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 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 pelo 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 CONTRATADA, 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.

Assinado por 2 pessoas: MIRLANE VIEIRA PEREIRA e JEREMIAS PEREIRA ALLEITE
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321> e informe o código 34C7-D880-59D2-E321

- 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 é 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



7.2.1.3.2. Unidades Descentralizadas

Assinado por 2 pessoas: GILRANE VIEIRA PEREIRA LEITE



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/EMEBFPfRm6Tb62a8	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/uyBXsZNDDszodCxx6	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/QZKQCN7SU9D2qwg8d	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/NSNEbdrq1cjknwX8	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/P32RY2iPJ7VLC9p7	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/b3bCUzB8qzw7vRd77	1

Assinado por 2 pessoas: GILRILANE VIEIRA PEREIRA e JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321 e informe o código 34C7-D880-59D2-E321

	SME - LARANJEIRA I	https://goo.gl/maps/jB1SZ3za3cdYev4a6	<u>1</u>
	SME - SÃO FRANCISCO	https://maps.app.goo.gl/sxzj1LsfXkFEX7Zy6	<u>1</u>
	UNIDADE DESCENTRALIZADA 4	-	<u>1</u>
	UNIDADE DESCENTRALIZADA 5	-	<u>1</u>
	UNIDADE DESCENTRALIZADA 6	-	<u>1</u>
	UNIDADE DESCENTRALIZADA 7	-	<u>1</u>
SMADE	SMADE	https://maps.app.goo.gl/zYaMoX5jtfJ1VQ2h8	<u>1</u>
	UNIDADE DESCENTRALIZADA 8	-	<u>1</u>
SMEL	SMEL - CIE	https://maps.app.goo.gl/Kkk4g4zUipLG7RDw6	<u>1</u>
	SMEL - DIDI PROFETA	https://maps.app.goo.gl/wUmbU83AgrRCFAjy6	<u>1</u>
	UNIDADE DESCENTRALIZADA 9	-	<u>1</u>
SMIL	SMIL - AEROPORTO	https://maps.app.goo.gl/N6nKAp5k4TpbGE1n6	<u>1</u>
	UNIDADE DESCENTRALIZADA 10	-	<u>1</u>
SMS	SMS - SECRETARIA DE SAUDE	https://maps.app.goo.gl/VWf4EYS5mnNdMk85A	<u>1</u>
	SMS - CAPS, AMBULATÓRIO DERMATOLÓGICO, LABORATORIO MUNICIPAL, ALMOXARIFADO, CMS	https://maps.app.goo.gl/3YsQdJ4PJUVqd6nG7	<u>1</u>
	SMS - CAPSI INFANTO JUVENIL	https://maps.app.goo.gl/NRE6n76fGEMAzey9	<u>1</u>
	SMS - CENTRO DE ESPECIALIDADES MEDICAS CEM	https://maps.app.goo.gl/zkjGjchEE1wsL14r8	<u>1</u>
	SMS - CENTRO DE SAUDE REFERENCIAL	https://maps.app.goo.gl/Z5MEaMJi68dU5hrG6	<u>1</u>
	SMS - CENTRO REAB DOM AQUINO CORREA CACERES CER II	https://maps.app.goo.gl/VhCQc4YayPyXp7sj8	<u>1</u>
	SMS - CEO	https://maps.app.goo.gl/wZMwZd1mfqVrkuRW6	<u>1</u>
	SMS - CTA CENTRO DE TESTAGEM E ACONSELHAMENTO SAE CACERES	https://maps.app.goo.gl/QPC3oTbJjodwapDV7	<u>1</u>
	SMS - FARMACIA BASICA DA SMS	https://maps.app.goo.gl/YwUSzHzPiKE5h3Vy8	<u>1</u>
	SMS - FROTAS	https://maps.app.goo.gl/UQZEQZxDpudbq1wH7	<u>1</u>
	SMS - POSTO DE SAUDE DA PAIOL	https://maps.app.goo.gl/PHsDSTgdLW1CdkacA	<u>1</u>
	SMS - POSTO DE SAUDE DE VILA APARECIDA	https://maps.app.goo.gl/uGRnxEjReD6jHpJ9A	<u>1</u>
	SMS - POSTO DE SAUDE DO LIMAO	https://maps.app.goo.gl/CfPip6ysDGqhiWmT6	<u>1</u>
	SMS - POSTO DE SAUDE HORIZONTE DOESTE	https://maps.app.goo.gl/6bkzEYMH7wQsigL49	<u>1</u>
	SMS - POSTO DE SAUDE LARANJEIRAS	https://maps.app.goo.gl/XpkQdasWsWE86U9q6?g_st=aw	<u>1</u>
	SMS - POSTO DE SAUDE PROF VERA LYGIA	https://maps.app.goo.gl/f6PfkXjMQjTudKqZ8	<u>1</u>

Assinado por 2 pessoas: GILRILANE VIEIRA PEREIRA e JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321>

	BALDO FACAO		
	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/vYJEU1ufGKzoEeK7	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

Assinado por 2 pessoas: GIRLANE VIEIRA PEREIRA e JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321> e informe o código 34C7-D880-59D2-E321

	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/qXAReBWJ7BQRpkm9	1
	SMEAE - PRAÇA MAJOR JOÃO CARLOS	https://goo.gl/maps/Qcwn4CXJdT5VCWQ6	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	https://goo.gl/maps/pA2tyTfhq8jqo5Fk7	1

Assinado por 2 pessoas: GIRILANE VIEIRA PEREIRA e JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321> e informe o código 34C7-D880-59D2-E321



Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321> e informe o código 34C7-D880-59D2-E321

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 o aprimoramento da política de segurança da informação do município.

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.

- ## 8.6. Fiscalização

- 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);

- 8.6.2.2. Identificada qualquer inexactidão 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 aprezadas, 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 apostilamentos e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário ([Art. 3º, 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, a 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 elaborar 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 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 recorrente 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: $TER = (QE / TTQ) * 100$ Sendo: TER = Indicador de taxa de erro; TTQ = Quantidade total de quadros enviados ou recebidos em um determinado período; QE = 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 CONTRATADA 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 na 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 de 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, 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

Assinado por 2 pessoas: GIRILANE PEREIRA e JEREMIAS PEREIRA. Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321> e informe o código 34C7-D880-59D2-E321

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	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 ocorrerem 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 do 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 circunstâncias 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 nº 089/2024.

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 aque-

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\$ 100,00 (cem reais) 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 nº 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] [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 contratado ou concorre;

10.2.1.2.7. Caso o fornecedor seja considerado isento dos tributos [Estadual/Distrital] [Municipal/Distrital] relacionados ao objeto contratual, deverá comprovar

Assinado por: GILRILANE PEREIRA JEREMIAS PEREIRA
Para verificar a validade das assinaturas, acesse https://caceres.mt.gov.br/verificacao/34C7-D880-59D2-E321

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 econômica 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 econômica financeira dos licitantes e para efeito de garantia ao adimplemento do contrato a ser posteriormente 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 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:

Assinado por 2 pessoas: GILNE VIEIRA PEREIRA e JEREMIAS PEREIRA
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321>

- 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 CONSÓRCIO

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 discricionariedade 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 empresas 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

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

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

Assinado por 2 pessoas: GIRLANE VIEIRA PEREIRA e JEREMIAS PEREIRA LEITE
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/34C7-D880-59D2-E321>



VERIFICAÇÃO DAS ASSINATURAS



Código para verificação: 34C7-D880-59D2-E321

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



GIRLANE VIEIRA PEREIRA (CPF 024.XXX.XXX-66) em 20/03/2025 08:26:23 GMT-04:00

Papel: Parte

Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)



JEREMIAS PEREIRA LEITE (CPF 045.XXX.XXX-72) em 20/03/2025 08:34:04 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/34C7-D880-59D2-E321>

Memorando 6.530/2025

De: Wellyngton M. - SMEAE - CTI

Para: SMEAE - Compras - Gerência de Compras - A/C Andressa C.

Data: 25/02/2025 às 18:09:55

Prezada;

Considerando a crescente necessidade de garantir a proteção das informações e dados da Administração Pública Municipal contra ameaças cibernéticas, é imprescindível a adoção de soluções eficazes de segurança digital, especialmente em um contexto de modernização e digitalização dos serviços públicos;

Considerando que a locação de um sistema de firewall especializado e serviços de segurança cibernética são medidas urgentes para proteger a infraestrutura de TI e garantir a continuidade das operações administrativas, além de assegurar a conformidade com as normas legais de segurança digital;

Considerando que a contratação de empresa especializada, com experiência comprovada, permitirá a implementação de soluções adequadas à realidade do município e garantirá eficiência, confiabilidade e proteção contra ataques cibernéticos.

Diante da necessidade de proteção e modernização dos sistemas municipais, solicito a abertura imediata do processo licitatório para contratação de empresa especializada na prestação de serviços de locação de firewall e segurança cibernética, com base no critério do menor valor global, conforme os ditames da Lei nº 14.133/2021, a fim de assegurar a proteção dos dados e a continuidade dos serviços públicos digitais.

—
At.te

Wellyngton de Barros Maciel

Analista de Sistemas

Anexos:

ETP_FIREWALL_2025_FINAL.docx

MAPA_DE_RISCO_FIREWALL_2025_FINAL.docx

TR_FIREWALL_2025_FINAL.docx

Memorando 1- 6.530/2025

De: Wellyngton M. - SMEAE - CTI

Para: SMEAE - Compras - Gerência de Compras - A/C Andressa C.

Data: 26/02/2025 às 12:50:53

Prezada;

Em tempo encaminho Mapa de Risco alterado.

—

At.te

Wellyngton de Barros Maciel

Analista de Sistemas

Anexos:

MR_FIREWALL_2025_FINAL.docx

Memorando 2- 6.530/2025

De: Wellyngton M. - SMEAE - CTI

Para: SMEAE - Compras - Gerência de Compras - A/C Andressa C.

Data: 18/03/2025 às 10:24:43

Prezada;

Em tempo encaminhando as Cotações.

—

At.te

Wellyngton de Barros Maciel

Analista de Sistemas

Anexos:

COTACAO_Inovasete_Tecnologia_Ltda.pdf

COTACAO_Rede_EXS.pdf

COTACAO_Trin_Informatica_Eireli.pdf

PAINEL_1.pdf

PAINEL_2.pdf

RADAR_1.pdf

PROPOSTA COMERCIAL

Objeto: Contratação de empresa especializada na prestação de serviços de segurança cibernética com Inteligência Artificial Preditiva, compreendendo o fornecimento, em regime de comodato, instalação e configuração de Next Generation Firewall (NGFW) e SD-WAN, bem como a disponibilização de redundância de conectividade por meio de links primário e secundário de ASN e rotas distintos.

Item	Especificação	UNIDADE	Quantidade	Valor Unitário Mensal*	Valor Total Anual
1	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)	Serviço	173	R\$ 129.750,00 (R\$ 750,00)	R\$ 1.557.000,00
2	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	Serviço	2	R\$ 37.000,00 (R\$ 18.500,00)	R\$ 444.000,00
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)	Serviço	2	R\$ 7.000,00 (R\$ 3.500,00)	R\$ 84.000,00
4	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 150Mbps Sites Remotos (Fibra Óptica)	Serviço	171	R\$ 42.750,00 (R\$ 250,00)	R\$ 513.000,00
5	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G)	Serviço	171	R\$ 25.650,00 (R\$ 150,00)	R\$ 307.800,00
6	Implantação da Solução	Serviço	1	R\$ 350.000,00	R\$ 350.000,00
7	Capacitação especializada da equipe com emissão de certificação.	Treinamento	1	R\$ 8.500,00	R\$ 8.500,00
8	Consultoria Política de Segurança	Serviço	1	R\$ 35.000,00	R\$ 35.000,00

* Os valores entre parêntesis correspondem ao valor unitário. Sem parêntesis correspondem ao valor mensal do item.

Total da Proposta: R\$ 3.299.300,00 (Três milhões, duzentos e noventa e nove mil e trezentos reais).

Dados Bancários:
Banco de Brasília S.A. (BRB) - 070 - Agência 0164 - Conta 164009250-9

Declaramos ter pleno conhecimento das condições e peculiaridades inerentes à natureza dos trabalhos, assumindo total responsabilidade pela ocorrência de eventuais prejuízos em virtude de sua omissão na verificação das condições descritas neste termo, com vistas a proteger o interesse da Administração na fase de execução do contrato, nos termos do Acórdão 1.174/2008 – Plenário – TCU, em não havendo vistoria.

A contratação abrangerá, ainda, a manutenção contínua, o suporte técnico especializado, a disponibilização de software de gerenciamento, a garantia de conectividade segura para unidades externas e praças públicas, além da capacitação certificada da equipe técnica e o atendimento técnico especializado. O objeto da contratação visa assegurar alta disponibilidade, segurança, eficiência e sustentabilidade na prestação dos serviços demandados pelo Município de Cáceres.

Brasília, 17 de março de 2025.

Documento assinado digitalmente
gov.br **ALAN MATHEUS TORRES DOS REIS**
Data: 17/03/2025 14:01:41-0300
Verifique em <https://validar.iti.gov.br>

Alan Matheus Torres dos Reis
Sócio-Administrador

À

Prefeitura Municipal de Cáceres

Secretaria Municipal de Assuntos Estratégicos

Av. Brasil, nº 119, Jardim Celeste (COC), Cáceres/MT, CEP: 78210-906

CNPJ: 03.214.145/0001-83

A/C, Gerente de TI da Prefeitura de Cáceres

Proposta Comercial

A EXS agradece a oportunidade de apresentar sua proposta para o fornecimento de Serviços de Cibersegurança para a Prefeitura de Cáceres.

Nos sentimos honrados em poder prestar nosso apoio e conhecimento na busca das soluções mais adequadas ao seu negócio, agregando tecnologia e serviços de qualidade às suas necessidades.

Estamos à disposição para esclarecer quaisquer dúvidas, com o objetivo de alinhar nossa proposta as suas necessidades.

Atenciosamente, Roselane Almeida
Administradora, *Rede EXS*

1. Apresentação

A EXS é uma empresa brasileira, sediada em Brasília, licenciada pela ANATEL como operadora SCM e SAC.

Nossos serviços contemplam Cibersegurança e conectividade para corporativo e governo.

2. Objetivo

Apresentar uma solução de conectividade à internet com base em tecnologia de última geração proporcionando alta qualidade na comunicação e uma melhor experiência.

3. Descrição do Serviço e Condições Comerciais

Fornecimento de serviços de Firewall de Nova Geração, Segurança Cibernética baseada em Inteligência Artificial, link de Internet e Transferência de Conhecimento.

Item	Especificação	UNIDADE	Quantidade	Valor Unitário Mensal	Valor Total Anual
1	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)	Serviço	173	R\$ 112.450,00	R\$ 1.349.400,00
2	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	Serviço	2	R\$ 33.000,00	R\$ 396.000,00
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)	Serviço	2	R\$ 8.000,00	R\$ 96.000,00
4	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 150Mbps Sites Remotos (Fibra Óptica)	Serviço	171	R\$ 39.330,00	R\$ 471.960,00
5	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G)	Serviço	171	R\$ 32.319,00	R\$ 387.828,00
6	Implantação da Solução	Serviço	1	R\$ 300.000,00	R\$ 300.000,00
7	Capacitação especializada da equipe com emissão de certificação.	Treinamento	1	R\$ 8.500,00	R\$ 8.500,00
8	Consultoria Política de Segurança	Serviço	1	R\$ 35.000,00	R\$ 35.000,00

4. Confidencialidade

Todos as informações obtidas por meio dessa negociação são confidenciais, as partes se obrigam a manter o mais absoluto sigilo com relação a toda e qualquer informação, dados, sistemas, dentre outros, que venha ter acesso, a partir do recebimento desta proposta comercial, exceto nos caso de compras governamentais.

5. Considerações finais

CNPJ: 23.935.457/0001-03

E-mails/contatos: roselane@redeexs.com.br / financeiro@redeexs.com.br / 21-991959540

Emissão da proposta: 18/03/2025

Validade da Proposta: 60(sessenta) dias.

ROSELANE GONZALEZ DO
NASCIMENTO
ALMEIDA:07894477702

Assinado de forma digital por
ROSELANE GONZALEZ DO NASCIMENTO
ALMEIDA:07894477702
Dados: 2025.03.18 00:00:26 -03'00'



SECRETARIA MUNICIPAL ESPECIAL DE ASSUNTOS ESTRATEGICOS

PESQUISA DE PREÇO		
Nome Fantasia: PREFEITURA MUNICIPAL DE CÁCERES		
Endereço: <i>Av. Brasil, nº 119, Jardim Celeste (COC), Cáceres/MT, CEP: 78210-906</i>		
CNPJ: <i>03.214.145/0001-83</i>		
E-mail: <i>cacerescsti@gmail.com</i>	Contato: <i>(65) 99948-4477</i>	
DADOS DA EMPRESA		
Nome Fantasia: Trin Informática Eireli ME		
Razão Social trin Informática		
CNPJ: 27.784.894/0001-04	Optante pelo simples: (X) Sim () Não	
Insc. Est.:	Insc. Mun.: 4427963	
Endereço: Rua T-36 3385 Qd 146 Lt 8 1004	Bairro: Setor Bueno	
Cidade: Goiânia	CEP: 74223-052	
E-mail: lucas.trin.informatica@gmail.com	Telefone: (62) 98338-9022	
Banco:Banco do Brasil	Nº Agência: 367-0	Conta Bancária nº: 110161-7

ITEM	ESPECIFICAÇÃO	UNIDADE	QUANTIDADE	VALOR UNITÁRIO MENSAL	VALOR TOTAL ANUAL
1	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)	Serviço	173	R\$132.000,00	R\$1.584.000,00
2	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	Serviço	2	R\$50.000,00	R\$600.000,00
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)	Serviço	2	R\$7.250,00	R\$ 87.000,00
4	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 150Mbps Sites Remotos (Fibra Óptica)	Serviço	171	R\$44.000,00	R\$528.000,00
5	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G)	Serviço	171	R\$26.500,00	R\$ 318.000,00
6	Implantação da Solução	Serviço	1	R\$ 340.000,00	R\$ 340.000,00
7	Capacitação especializada da equipe com emissão de certificação.	Treinamento	1	R\$ 8.250,00	R\$8.250,00
8	Consultoria Política de Segurança	Serviço	1	R\$37.000,00	R\$ 37.000,00

27.784.894/0001-04
TRIN INFORMATICA EIRELI
R T 36, 3385 QD 146 L8E 1004
SETOR BUENO - 74.223-052
GOIÂNIA - GO

Goiânia 17/03/2025



MENOR

R\$ 11.863,58

Objeto da Compra

27740, 26972, 21172, 27120 Pregão Eletrônico - Aquisição de solução de Firewall de rede (NGFW) Next Generation Firewall de Borda em Cluster e Endpoint do fabricante Check Point Software Technologies Ltda, subscrição de licenças, com fornecimento de appliances, licenciamento, software de gerenciamento, serviços de instalação e configuração, suporte técnico e treinamento para a solução ofertada

Registros apresentados: 1 a 5

Identificação da Compra	Número do Item	Modalidade	Código do CATSERV	Descrição do Item	Descrição Complementar	Unidade de Fornecimento	Quantidade Ofertada	Valor Unitário	Fornecedor	Órgão	UASG	Data da Compra
90070/2024	00004	Pregão	26972	SERVICOS DE INSTALACAO, TRANSICAO E CONFIGURACAO / PARAMETRIZACAO DE SOFTWARE		PONTO DE FUNÇÃO	10	R\$11863,58	CONTACTA SEGURANCA EM CONECTIVIDADE LTDA	JUSTICA ELEITORAL	070017 - TRIBUNAL REGIONAL ELEITORAL DO RIO DE JANEIRO	09/12/2024
90070/2024	00007	Pregão	21172	TREINAMENTO QUALIFICACAO PROFISSIONAL		UN	1	R\$64982,12	CONTACTA SEGURANCA EM CONECTIVIDADE LTDA	JUSTICA ELEITORAL	070017 - TRIBUNAL REGIONAL ELEITORAL DO RIO DE JANEIRO	09/12/2024
90070/2024	00005	Pregão	27120	SERVICOS DE MANUTENCAO DE EQUIPAMENTOS DE COMUNICACAO DE DADOS E COMUTACAO TELEFONICA		UNIDADE	1	R\$96830,04	CONTACTA SEGURANCA EM CONECTIVIDADE LTDA	JUSTICA ELEITORAL	070017 - TRIBUNAL REGIONAL ELEITORAL DO RIO DE JANEIRO	09/12/2024
90070/2024	00002	Pregão	26972	SERVICOS DE INSTALACAO, TRANSICAO E CONFIGURACAO / PARAMETRIZACAO DE SOFTWARE		UST	2	R\$910000	CONTACTA SEGURANCA EM CONECTIVIDADE LTDA	JUSTICA ELEITORAL	070017 - TRIBUNAL REGIONAL ELEITORAL DO RIO DE JANEIRO	09/12/2024

Fonte: www.planejamento.gov.br

90070/2024	00006	Pregão	27740	SERVICOS DE GARANTIA DE EQUIPAMENTOS DE TIC		UNIDADE	1	R\$958992,87	CONTACTA SEGURANCA EM CONECTIVIDADE LTDA	JUSTICA ELEITORAL	070017 - TRIBUNAL REGIONAL ELEITORAL DO RIO DE JANEIRO	09/12/2024
------------	-------	--------	-------	---	--	---------	---	--------------	--	-------------------	--	------------



MENOR

R\$ 415,50

27740, 27510 Pregão Eletrônico - Contratação de serviços de licenciamento\, garantia e suporte técnico por 36 (trinta e seis) meses para equipamentos Firewall (NGFW) Fortigate FG-3200D\, bem como serviços técnicos de operação assistida\, sob demanda.

Registros apresentados: 1 a 2

Identificação da Compra	Número do Item	Modalidade	Código do CATSERV	Descrição do Item	Descrição Complementar	Unidade de Fornecimento	Quantidade Ofertada	Valor Unitário	Fornecedor	Órgão	UASG	Data da Compra
90003/2024	00002	Pregão	27510	CONTRATOS DE PRESTACAO DE SERVICOS DE ASSISTENCIA TECNICA E CIENTIFICA		UN	300	R\$415,50	VERY TECNOLOGIA LTDA	MINISTERIO DA EDUCACAO	150004 - SUBSECRETARIA DE TEC INFORMACÃO E COMUNICAÇÃO	27/12/2024
90003/2024	00001	Pregão	27740	SERVICOS DE GARANTIA DE EQUIPAMENTOS DE TIC		UN	4	R\$817000	VERY TECNOLOGIA LTDA	MINISTERIO DA EDUCACAO	150004 - SUBSECRETARIA DE TEC INFORMACÃO E COMUNICAÇÃO	27/12/2024

Fonte: painel de preços planejados cor.br



Relatório Resumido

Relatório gerado em: 18/03/2025 08:33:26
Quantidade total de registros: 4

Filtros aplicados

Nome Fiscalizado: SEC. EST. DO MEIO AMBIENTE
Objeto da licitação: AQUISIÇÃO DE SOLUÇÃO DE PROTEÇÃO DE REDE NEXT GENERATION FIREWALL(NGFW)\, EM CLUSTER\, CONTEMPLANDO O HARDWARE\, SOFTWARE\, LICENCIAMENTO\, IMPLANTAÇÃO.
Nome do Material: EQUIPAMENTO DE PROTECAO DE REDE, SERVICIO DE CONSULTORIA NA AREA DE INFORMATICA, SERVICIO DE SUPORTE

Valor Máximo Unit do Material
R\$761000,00

Média Saneada Global
R\$315618,22

Mediana Valor Unit do Material
R\$347003,25

	Fiscalizado	Modalidade	Cód. Licitação	Cód. Material	Material	Descrição	Qtd. Material	Uni. Fornecimento	Valor Unit	CNPJ/CPF Fornecedor	Nome Fornecedor	Data Homologação
1	SEC. EST. DO MEIO AMBIENTE	Pregão eletrônico (Bens e serviços comuns)	00000000013/2022	262447-8	EQUIPAMENTO DE PROTECAO DE REDE	(262447-8) EQUIPAMENTO DE PROTECAO DE REDE - FIREW..	3	UNIDADE	R\$ 171.858,00	01.181.242/0002-72	COMPWIRE INFORMATICA S/A	25/05/2022
2	SEC. EST. DO MEIO AMBIENTE	Pregão eletrônico (Bens e serviços comuns)	00000000013/2022	324821-6	SERVICIO DE CONSULTORIA NA AREA DE INFORMATICA	(324821-6) SERVICIO DE CONSULTORIA NA AREA DE INFOR..	2	UNIDADE	R\$ 205.006,50	01.181.242/0002-72	COMPWIRE INFORMATICA S/A	25/05/2022
3	SEC. EST. DO MEIO AMBIENTE	Pregão eletrônico (Bens e serviços comuns)	00000000013/2022	00062233	SERVICIO DE SUPORTE	(00062233) SERVICIO DE SUPORTE - TECNICO MENSAL, CO..	2	UNIDADE	R\$ 489.000,00	01.181.242/0002-72	COMPWIRE INFORMATICA S/A	25/05/2022
4	SEC. EST. DO MEIO AMBIENTE	Pregão eletrônico (Bens e serviços comuns)	00000000013/2022	340815-9	SERVICIO DE SUPORTE	(340815-9) SERVICIO DE SUPORTE - DO TIPO TESTE DE S..	1	UNIDADE	R\$ 761.000,00	01.181.242/0002-72	COMPWIRE INFORMATICA S/A	25/05/2022

Memorando 3- 6.530/2025

De: Wellyngton M. - SMEAE - CTI

Para: SMEAE - Compras - Gerência de Compras - A/C Andressa C.

Data: 18/03/2025 às 16:17:31

Prezada;

Em tempo encaminho os e-mails de cotação com fornecedores.

—

At.te

Wellyngton de Barros Maciel

Analista de Sistemas

Anexos:

E_MAIL_BRAVA_INTERNET.pdf

E_MAIL_DUNET_FIBRAS.pdf

E_MAIL_INOVASETE_TECNOLOGIA_1.pdf

E_MAIL_INOVASETE_TECNOLOGIA_2.pdf

E_MAIL_REDE_EXS.pdf

E_MAIL_SEEG_FIBRAS.pdf

E_MAIL_TRIN_INFORMATICA.pdf



1 mensagem

5 de março de 2025 às 16:08

Para: central@bravainternet.com.br

Prezado(s),

Cumprimentando-o(s) cordialmente, solicitamos a apresentação de **COTAÇÃO** para a contratação de empresa especializada na prestação de serviços de **segurança cibernética com Inteligência Artificial Preditiva**, compreendendo o **fornecimento, em regime de comodato, instalação e configuração de Next Generation Firewall (NGFW) e SD-WAN**, bem como a disponibilização de **redundância de conectividade** por meio de links **primário e secundário** de ASN e rotas distintas.

A contratação abrangerá, ainda, a **manutenção contínua**, o **suporte técnico especializado**, a disponibilização de **software de gerenciamento**, a garantia de **conectividade segura para unidades externas e praças públicas**, além da **capacitação certificada da equipe técnica** e o **atendimento técnico especializado**. O objeto da contratação visa assegurar **alta disponibilidade, segurança, eficiência e sustentabilidade** na prestação dos serviços demandados pelo Município de Cáceres.

As condições e especificações encontram-se detalhadas na **planilha de cotação** anexa. Assim, solicitamos o envio da cotação conforme os requisitos estabelecidos.

—

At.te

Coordenação de Tecnologia da Informação

Município de Cáceres

Tel: +55 65 9948-4477



PLANILHA COTAÇÃO.docx

155K



CTI CÁCERES <cacerescti@gmail.com>

COTAÇÃO - SEGURANÇA CIBERNÉTICA

1 mensagem

CTI CÁCERES <cacerescti@gmail.com>

5 de março de 2025 às 16:13

Para: atendimento01@dunetfibras.com.br

Prezado(s),

Cumprimentando-o(s) cordialmente, solicitamos a apresentação de **COTAÇÃO** para a contratação de empresa especializada na prestação de serviços de **segurança cibernética** com **Inteligência Artificial Preditiva**, compreendendo o **fornecimento, em regime de comodato, instalação e configuração de Next Generation Firewall (NGFW) e SD-WAN**, bem como a disponibilização de **redundância de conectividade** por meio de links **primário e secundário** de ASN e rotas distintas.

A contratação abrangerá, ainda, a **manutenção contínua**, o **suporte técnico especializado**, a disponibilização de **software de gerenciamento**, a garantia de **conectividade segura** para **unidades externas e praças públicas**, além da **capacitação certificada da equipe técnica** e o **atendimento técnico especializado**. O objeto da contratação visa assegurar **alta disponibilidade, segurança, eficiência e sustentabilidade** na prestação dos serviços demandados pelo Município de Cáceres.

As condições e especificações encontram-se detalhadas na **planilha de cotação** anexa. Assim, solicitamos o envio da cotação conforme os requisitos estabelecidos.

--

At.te

Coordenação de Tecnologia da Informação

Município de Cáceres

Tel: +55 65 9948-4477



PLANILHA COTAÇÃO.docx

155K



CTI CÁCERES <cacerescti@gmail.com>

COTAÇÃO - SEGURANÇA CIBERNÉTICA

1 mensagem

CTI CÁCERES <cacerescti@gmail.com>

5 de março de 2025 às 16:06

Para: sandro.araujo@camoa.com.br

Prezado(s),

Cumprimentando-o(s) cordialmente, solicitamos a apresentação de **COTAÇÃO** para a contratação de empresa especializada na prestação de serviços de **segurança cibernética** com **Inteligência Artificial Preditiva**, compreendendo o **fornecimento, em regime de comodato, instalação e configuração de Next Generation Firewall (NGFW) e SD-WAN**, bem como a disponibilização de **redundância de conectividade** por meio de links **primário e secundário** de ASN e rotas distintas.

A contratação abrangerá, ainda, a **manutenção contínua**, o **suporte técnico especializado**, a disponibilização de **software de gerenciamento**, a garantia de **conectividade segura** para **unidades externas e praças públicas**, além da **capacitação certificada da equipe técnica** e o **atendimento técnico especializado**. O objeto da contratação visa assegurar **alta disponibilidade, segurança, eficiência e sustentabilidade** na prestação dos serviços demandados pelo Município de Cáceres.

As condições e especificações encontram-se detalhadas na **planilha de cotação** anexa. Assim, solicitamos o envio da cotação conforme os requisitos estabelecidos.

--

At.te

Coordenação de Tecnologia da Informação

Município de Cáceres

Tel: +55 65 9948-4477



PLANILHA COTAÇÃO.docx

155K



CTI CÁCERES <cacerescti@gmail.com>

COTAÇÃO - SEGURANÇA CIBERNÉTICA

2 mensagens

CTI CÁCERES <cacerescti@gmail.com>

5 de março de 2025 às 16:06

Para: governo@camoa.com.br

Prezado(s),

Cumprimentando-o(s) cordialmente, solicitamos a apresentação de **COTAÇÃO** para a contratação de empresa especializada na prestação de serviços de **segurança cibernética** com **Inteligência Artificial Preditiva**, compreendendo o **fornecimento, em regime de comodato, instalação e configuração de Next Generation Firewall (NGFW) e SD-WAN**, bem como a disponibilização de **redundância de conectividade** por meio de links **primário e secundário** de ASN e rotas distintas.

A contratação abrangerá, ainda, a **manutenção contínua**, o **suporte técnico especializado**, a disponibilização de **software de gerenciamento**, a garantia de **conectividade segura** para **unidades externas e praças públicas**, além da **capacitação certificada da equipe técnica** e o **atendimento técnico especializado**. O objeto da contratação visa assegurar **alta disponibilidade, segurança, eficiência e sustentabilidade** na prestação dos serviços demandados pelo Município de Cáceres.

As condições e especificações encontram-se detalhadas na **planilha de cotação** anexa. Assim, solicitamos o envio da cotação conforme os requisitos estabelecidos.

--

At.te

Coordenação de Tecnologia da Informação

Município de Cáceres

Tel: +55 65 9948-4477



PLANILHA COTAÇÃO.docx

155K

Sandro Araújo <sandro.araujo@camoa.com.br>

17 de março de 2025 às 13:43

Para: CTI CÁCERES <cacerescti@gmail.com>, "governo@camoa.com.br"

<governo@camoa.com.br>

Segue Proposta Comercial contemplando a planilha de cotação enviada.

Atenciosamente,

Sandro Araújo

Inovasete Tecnologia

De: CTI CÁCERES <cacerescti@gmail.com>

Enviado: quarta-feira, 5 de março de 2025 17:06

Para: governo@camoa.com.br <governo@camoa.com.br>

Assunto: COTAÇÃO - SEGURANÇA CIBERNÉTICA

[Texto das mensagens anteriores oculto]



CTI CÁCERES <cacerescti@gmail.com>

COTAÇÃO - SEGURANÇA CIBERNÉTICA

2 mensagens

CTI CÁCERES <cacerescti@gmail.com>

5 de março de 2025 às 16:05

Para: diretoria@redeexs.com.br

Prezado(s),

Cumprimentando-o(s) cordialmente, solicitamos a apresentação de **COTAÇÃO** para a contratação de empresa especializada na prestação de serviços de **segurança cibernética** com **Inteligência Artificial Preditiva**, compreendendo o **fornecimento, em regime de comodato, instalação e configuração de Next Generation Firewall (NGFW) e SD-WAN**, bem como a disponibilização de **redundância de conectividade** por meio de links **primário e secundário** de ASN e rotas distintas.

A contratação abrangerá, ainda, a **manutenção contínua**, o **suporte técnico especializado**, a disponibilização de **software de gerenciamento**, a garantia de **conectividade segura** para **unidades externas e praças públicas**, além da **capacitação certificada da equipe técnica** e o **atendimento técnico especializado**. O objeto da contratação visa assegurar **alta disponibilidade, segurança, eficiência e sustentabilidade** na prestação dos serviços demandados pelo Município de Cáceres.

As condições e especificações encontram-se detalhadas na **planilha de cotação** anexa. Assim, solicitamos o envio da cotação conforme os requisitos estabelecidos.

--

At.te

Coordenação de Tecnologia da Informação

Município de Cáceres

Tel: +55 65 9948-4477



PLANILHA COTAÇÃO.docx

155K

Régis Daniel <regis.daniel@redeexs.com.br>

17 de março de 2025 às 23:41

Para: CTI CÁCERES <cacerescti@gmail.com>

Cc: diretoria@redeexs.com.br

À Coordenação de Tecnologia da Informação,

Espero encontrá-los bem!

Segue proposta comercial conforme solicitado.

At.te.,

Régis Daniel

[Texto das mensagens anteriores oculto]

 **18.03.2025.PropostaComercial.PrefCaceres.pdf**
479K



CTI CÁCERES <cacerescti@gmail.com>

COTAÇÃO - SEGURANÇA CIBERNÉTICA

1 mensagem

CTI CÁCERES <cacerescti@gmail.com>

5 de março de 2025 às 16:16

Para: financeiro@seegfibras.com.br

Prezado(s),

Cumprimentando-o(s) cordialmente, solicitamos a apresentação de **COTAÇÃO** para a contratação de empresa especializada na prestação de serviços de **segurança cibernética** com **Inteligência Artificial Preditiva**, compreendendo o **fornecimento, em regime de comodato, instalação e configuração de Next Generation Firewall (NGFW) e SD-WAN**, bem como a disponibilização de **redundância de conectividade** por meio de links **primário e secundário** de ASN e rotas distintas.

A contratação abrangerá, ainda, a **manutenção contínua**, o **suporte técnico especializado**, a disponibilização de **software de gerenciamento**, a garantia de **conectividade segura** para **unidades externas e praças públicas**, além da **capacitação certificada da equipe técnica** e o **atendimento técnico especializado**. O objeto da contratação visa assegurar **alta disponibilidade, segurança, eficiência e sustentabilidade** na prestação dos serviços demandados pelo Município de Cáceres.

As condições e especificações encontram-se detalhadas na **planilha de cotação** anexa. Assim, solicitamos o envio da cotação conforme os requisitos estabelecidos.

--

At.te

Coordenação de Tecnologia da Informação

Município de Cáceres

Tel: +55 65 9948-4477



PLANILHA COTAÇÃO.docx

155K



CTI CÁCERES <cacerescti@gmail.com>

COTAÇÃO - SEGURANÇA CIBERNÉTICA

2 mensagens

CTI CÁCERES <cacerescti@gmail.com>

5 de março de 2025 às 16:07

Para: lucas.trin.informatica@gmail.com

Prezado(s),

Cumprimentando-o(s) cordialmente, solicitamos a apresentação de **COTAÇÃO** para a contratação de empresa especializada na prestação de serviços de **segurança cibernética com Inteligência Artificial Preditiva**, compreendendo o **fornecimento, em regime de comodato, instalação e configuração de Next Generation Firewall (NGFW) e SD-WAN**, bem como a disponibilização de **redundância de conectividade** por meio de links **primário e secundário** de ASN e rotas distintas.

A contratação abrangerá, ainda, a **manutenção contínua**, o **suporte técnico especializado**, a disponibilização de **software de gerenciamento**, a garantia de **conectividade segura** para **unidades externas e praças públicas**, além da **capacitação certificada da equipe técnica** e o **atendimento técnico especializado**. O objeto da contratação visa assegurar **alta disponibilidade, segurança, eficiência e sustentabilidade** na prestação dos serviços demandados pelo Município de Cáceres.

As condições e especificações encontram-se detalhadas na **planilha de cotação** anexa. Assim, solicitamos o envio da cotação conforme os requisitos estabelecidos.

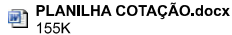
—

At.te

Coordenação de Tecnologia da Informação

Município de Cáceres

Tel: +55 65 9948-4477



Lucas França <lucas.trin.informatica@gmail.com>

Para: CTI CACERES <cacerescti@gmail.com>

Prezados Senhores

Bom dia, conforme solicitado enviamos em anexo nossa melhor proposta para a contratação de empresa especializada na prestação de serviços de **seg. Artificial Preditiva**, compreendendo o **fornecimento, em regime de comodato, instalação e configuração de Next Generation Firewall (NGFW) e SD de redundância de conectividade** por meio de links **primário e secundário** de ASN e rotas distintas..

Ficamos à inteira disposição para qualquer dúvida.

Lucas França
Consultor de Vendas
(62)3251-6464



 Proposta 20250317 PM Cáceres.pdf
484K

Memorando 4- 6.530/2025

De: Wellyngton M. - SMEAE - CTI

Para: SMEAE - Compras - Gerência de Compras - A/C Andressa C.

Data: 20/03/2025 às 08:41:01

Prezada;

Em tempo encaminho ETP corrigido.

At.te

Wellyngton de Barros Maciel

Analista de Sistemas

Anexos:

ETP_FIREWALL_2025_FINAL2.docx

Memorando 5- 6.530/2025

De: Wellyngton M. - SMEAE - CTI

Para: SMEAE - Compras - Gerência de Compras - A/C Andressa C.

Data: 07/04/2025 às 09:04:48

Prezada,

Considerando a identificação de inconsistências no preenchimento das cotações, especificamente no que tange ao campo *Valor Unitário Mensal*, o qual apresentou-se de forma confusa e em desacordo com o solicitado, encaminhamos, por meio deste, as referidas cotações devidamente corrigidas, acompanhadas dos respectivos e-mails que formalizaram a solicitação de retificação junto aos proponentes.

Permanecemos à inteira disposição para prestar quaisquer esclarecimentos adicionais que se fizerem necessários ao regular prosseguimento do feito.

—
At.te

Wellyngton de Barros Maciel

Analista de Sistemas

Anexos:

COTACAO_Inovasete_Tecnologia_Ltda_2.pdf

COTACAO_Rede_EXS_2.pdf

COTACAO_Trin_Informatica_Eireli_2.pdf

E_MAIL_INOVASETE_TECNOLOGIA_1_1.pdf

E_MAIL_REDE_EXS_1.pdf

E_MAIL_TRIN_INFORMATICA_1.pdf

À
 Prefeitura Municipal de Cáceres
 Secretaria Municipal de Assuntos Estratégicos
 Av. Brasil, nº 119, Jardim Celeste (COC), Cáceres/MT, CEP: 78210-906
 CNPJ: 03.214.145/0001-83

PROPOSTA COMERCIAL

Identificação da Empresa: Inovasete Tecnologia Ltda
 CNPJ: 10.365.200/0001-00
 Endereço: SHN Quadra 1 Cj A Sl 1414 - Asa Norte - Brasília-DF - 70.701-000
 Telefone: 61.3255.1253

Objeto: Contratação de empresa especializada na prestação de serviços de segurança cibernética com Inteligência Artificial Preditiva, compreendendo o fornecimento, em regime de comodato, instalação e configuração de Next Generation Firewall (NGFW) e SD-WAN, bem como a disponibilização de redundância de conectividade por meio de links primário e secundário de ASN e rotas distintas.

Item	Especificação	UNIDADE	Qtde	Valor Unitário / Mensal	Valor Total Mensal	Valor Total Anual
1	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)	Serviço	173	R\$ 750,00	R\$ 129.750,00	R\$ 1.557.000,00
2	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	Serviço	2	R\$ 18.500,00	R\$ 37.000,00	R\$ 444.000,00
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)	Serviço	2	R\$ 3.500,00	R\$ 7.000,00	R\$ 84.000,00
4	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 150Mbps Sites Remotos (Fibra Óptica)	Serviço	171	R\$ 250,00	R\$ 42.750,00	R\$ 513.000,00
5	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G)	Serviço	171	R\$ 150,00	R\$ 25.650,00	R\$ 307.800,00
6	Implantação da Solução	Serviço	1	R\$ 350.000,00	-	-
7	Capacitação especializada da equipe com emissão de certificação.	Treinamento	1	R\$ 8.500,00	-	-
8	Consultoria Política de Segurança	Serviço	1	R\$ 35.000,00	-	-
	Total de Valores de Pagamento Único			R\$ 393.500,00	-	-
	Total de Valores de Pagamento Mensal				R\$ 242.150,00	R\$ 2.905.800,00

Total da Proposta: R\$ 3.299.300,00 (Três milhões, duzentos e noventa e nove mil e trezentos reais).

SHN Quadra 1 Cj A Sl 1414 - Asa Norte - Brasília-DF - 70.701-000
 61.3255.1253

Declaramos ter pleno conhecimento das condições e peculiaridades inerentes à natureza dos trabalhos, assumindo total responsabilidade pela ocorrência de eventuais prejuízos em virtude de sua omissão na verificação das condições descritas neste termo, com vistas a proteger o interesse da Administração na fase de execução do contrato, nos termos do Acórdão 1.174/2008 – Plenário – TCU, em não havendo vistoria.

Dados Bancários:

Banco de Brasília S.A. (BRB) - 070 - Agência 0164 - Conta 164009250-9

A contratação abrangerá, ainda, a manutenção contínua, o suporte técnico especializado, a disponibilização de software de gerenciamento, a garantia de conectividade segura para unidades externas e praças públicas, além da capacitação certificada da equipe técnica e o atendimento técnico especializado. O objeto da contratação visa assegurar alta disponibilidade, segurança, eficiência e sustentabilidade na prestação dos serviços demandados pelo Município de Cáceres.

Brasília, 04 de abril de 2025.

Documento assinado digitalmente

gov.br

ALAN MATHEUS TORRES DOS REIS

Data: 04/04/2025 10:48:26-0300

Verifique em <https://validar.itj.gov.br>

Alan Matheus Torres dos Reis
Sócio-Administrador

À

Prefeitura Municipal de Cáceres

Secretaria Municipal de Assuntos Estratégicos

Av. Brasil, nº 119, Jardim Celeste (COC), Cáceres/MT, CEP: 78210-906

CNPJ: 03.214.145/0001-83

A/C, Gerente de TI da Prefeitura de Cáceres

Proposta Comercial

A EXS agradece a oportunidade de apresentar sua proposta para o fornecimento de Serviços de Cibersegurança para a Prefeitura de Cáceres.

Nos sentimos honrados em poder prestar nosso apoio e conhecimento na busca das soluções mais adequadas ao seu negócio, agregando tecnologia e serviços de qualidade às suas necessidades.

Estamos à disposição para esclarecer quaisquer dúvidas, com o objetivo de alinhar nossa proposta as suas necessidades.

No imp de:

Atenciosamente, Roselane Almeida
Administradora, *Rede EXS*

REGIS DANIEL Assinado de forma digital
por REGIS DANIEL
ALMEIDA:704 ALMEIDA:70470260025
70260025 Dados: 2025.04.07
01:19:04 -03'00'

1. Apresentação

A EXS é uma empresa brasileira, sediada em Brasília, licenciada pela ANATEL como operadora SCM e SAC.

Nossos serviços contemplam Cibersegurança e conectividade para corporativo e governo.

2. Objetivo

Apresentar uma solução de conectividade à internet com base em tecnologia de última geração proporcionando alta qualidade na comunicação e uma melhor experiência.

3. Descrição do Serviço e Condições Comerciais

Fornecimento de serviços de Firewall de Nova Geração, Segurança Cibernética baseada em Inteligência Artificial, link de Internet e Transferência de Conhecimento.

Item	Especificação	UNIDADE	Quantidade	Valor Unitário Mensal	Valor Total Anual
1	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)	Serviço	173	R\$ 650,00	R\$ 1.349.400,00
2	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	Serviço	2	R\$ 16.500,00	R\$ 396.000,00
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)	Serviço	2	R\$ 4.000,00	R\$ 96.000,00
4	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 150Mbps Sites Remotos (Fibra Óptica)	Serviço	171	R\$ 230,00	R\$ 471.960,00
5	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G)	Serviço	171	R\$ 189,00	R\$ 387.828,00
6	Implantação da Solução	Serviço	1	R\$ 300.000,00	R\$ 300.000,00
7	Capacitação especializada da equipe com emissão de certificação.	Treinamento	1	R\$ 8.500,00	R\$ 8.500,00
8	Consultoria Política de Segurança	Serviço	1	R\$ 35.000,00	R\$ 35.000,00

4. Confidencialidade

Todas as informações obtidas por meio dessa negociação são confidenciais, as partes se obrigam a manter o mais absoluto sigilo com relação a toda e qualquer informação, dados, sistemas, dentre outros, que venha ter acesso, a partir do recebimento desta proposta comercial, exceto nos casos de compras governamentais.

5. Considerações finais

CNPJ: 23.935.457/0001-03

E-mails/contatos: roselane@redeexs.com.br / financeiro@redeexs.com.br / 21-991959540

Emissão da proposta: 07/04/2025

Validade da Proposta: 60(sessenta) dias.

Proposta

Conforme solicitado em vosso e-mail de 05 de março de 2025, estamos apresentando abaixo nossa proposta para contratação de empresa especializada na prestação de serviços de **segurança cibernética com Inteligência Artificial Preditiva**, compreendendo o **fornecimento, em regime de comodato, instalação e configuração de Next Generation Firewall (NGFW) e SD-WAN**, bem como a disponibilização de **redundância de conectividade** por meio de links **primário e secundário** de ASN e rotas distintas.

PRAZO - O prazo desta proposta é 90 dias.

FORMAS DE PAGAMENTO - Conforme condições do edital.

DADOS DO PROPONENTE Razão Social: Trin Informatica Eireli.

CNPJ: 27.784.894/0001-04

Endereço: Rua T 36, 3385 Qd 146 L8 - 1004

Goiânia / GO, Brasil / CEP 74223-052

Goiânia 04 de Abril de 2025





SECRETARIA MUNICIPAL ESPECIAL DE ASSUNTOS ESTRATÉGICOS

PESQUISA DE PREÇO		
Nome Fantasia: PREFEITURA MUNICIPAL DE CÁCERES		
Endereço: <i>Av. Brasil, nº 119, Jardim Celeste (COC), Cáceres/MT, CEP: 78210-906</i>		
CNPJ: <i>03.214.145/0001-83</i>		
E-mail: <i>cacerescsti@gmail.com</i>	Contato: <i>(65) 99948-4477</i>	
DADOS DA EMPRESA		
Nome Fantasia: Trin Informática Eireli ME		
Razão Social trin Informática		
CNPJ: 27.784.894/0001-04	Optante pelo simples: (X) Sim () Não	
Insc. Est.:	Insc. Mun.: 4427963	
Endereço: Rua T-36 3385 Qd 146 Lt 8 1004	Bairro: Setor Bueno	
Cidade: Goiânia	CEP: 74223-052	
E-mail: lucas.trin.informatica@gmail.com	Telefone: (62) 98338-9022	
Banco:Banco do Brasil	Nº Agência: 367-0	Conta Bancária nº: 110161-7

ITEM	ESPECIFICAÇÃO	UNIDADE	QUANTIDADE	VALOR UNITÁRIO MENSAL	VALOR TOTAL ANUAL
1	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)	Serviço	173	R\$ 763,00	R\$1.583.988,00
2	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	Serviço	2	R\$25.000,00	R\$600.000,00
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)	Serviço	2	R\$3.625,00	R\$ 87.000,00
4	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 150Mbps Sites Remotos (Fibra Óptica)	Serviço	171	R\$257,30	R\$527.979,60
5	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G)	Serviço	171	R\$154,97	R\$ 317.998,44
6	Implantação da Solução	Serviço	1	R\$ 340.000,00	R\$ 340.000,00
7	Capacitação especializada da equipe com emissão de certificação.	Treinamento	1	R\$ 8.250,00	R\$8.250,00
8	Consultoria Política de Segurança	Serviço	1	R\$37.000,00	R\$ 37.000,00

27.784.894/0001-04
TRIN INFORMATICA EIRELI
R T 36, 3385 QD 146 L8E 1004
SETOR BUENO - 74.223-052
GOIÂNIA - GO

Goiânia 04/04/2025



4 mensagens

5 de março de 2025 às 16:06

Para: governo@camoa.com.br

Prezado(s),

Cumprimentando-o(s) cordialmente, solicitamos a apresentação de **COTAÇÃO** para a contratação de empresa especializada na prestação de serviços de **segurança cibernética com Inteligência Artificial Preditiva**, compreendendo o **fornecimento, em regime de comodato, instalação e configuração de Next Generation Firewall (NGFW) e SD-WAN**, bem como a disponibilização de **redundância de conectividade** por meio de links **primário e secundário** de ASN e rotas distintas.

A contratação abrangerá, ainda, a **manutenção contínua**, o **suporte técnico especializado**, a disponibilização de **software de gerenciamento**, a garantia de **conectividade segura** para **unidades externas e praças públicas**, além da **capacitação certificada da equipe técnica** e o **atendimento técnico especializado**. O objeto da contratação visa assegurar **alta disponibilidade, segurança, eficiência e sustentabilidade** na prestação dos serviços demandados pelo Município de Cáceres.

As condições e especificações encontram-se detalhadas na **planilha de cotação** anexa. Assim, solicitamos o envio da cotação conforme os requisitos estabelecidos.

—

At.te

Coordenação de Tecnologia da Informação

Município de Cáceres

Tel: +55 65 9948-4477



PLANILHA COTAÇÃO.docx

155K

17 de março de 2025 às 13:43

Para: CTI CÁCERES <cacerescti@gmail.com>, "governo@camoa.com.br"

<governo@camoa.com.br>

Segue Proposta Comercial contemplando a planilha de cotação enviada.

Atenciosamente,

Sandro Araújo
Inovasete Tecnologia

De: CTI CÁCERES <cacerescti@gmail.com>

Enviado: quarta-feira, 5 de março de 2025 17:06

Para: governo@camoa.com.br <governo@camoa.com.br>

Assunto: COTAÇÃO - SEGURANÇA CIBERNÉTICA

[Texto das mensagens anteriores oculto]



Proposta_Comercial_Caceres_assinado.pdf
98K

CTI CÁCERES <cacerescti@gmail.com>

4 de abril de 2025 às 08:10

Para: Sandro Araújo <sandro.araujo@camoa.com.br>

Prezado(a),

Considerando a identificação de equívoco no preenchimento da cotação, especificamente na coluna referente ao *Valor Unitário Mensal*, a qual foi indevidamente preenchida com o valor total mensal, solicitamos a gentileza de proceder com a devida retificação, inserindo corretamente o valor unitário correspondente.

Informamos que o prazo para envio da resposta com as devidas correções encerra-se em **07 de abril de 2025**.

Desde já, agradecemos pela atenção e colaboração, colocando-nos à disposição para eventuais esclarecimentos que se fizerem necessários.

[Texto das mensagens anteriores oculto]

—

At.te

Coordenação de Tecnologia de Informação

Tel: +55 65 9948-4477

Sandro Araújo <sandro.araujo@camoa.com.br>

4 de abril de 2025 às 10:01

Para: CTI CÁCERES <cacerescti@gmail.com>

Segue proposta atualizada.

Peco a gentileza de conferir e informar se agora está ok.

Grato,

Sandro Araújo

De: CTI CÁCERES <cacerescti@gmail.com>

Enviado: sexta-feira, 4 de abril de 2025 09:10

Para: Sandro Araújo <sandro.araujo@camoa.com.br>

Assunto: Re: COTAÇÃO - SEGURANÇA CIBERNÉTICA

[Texto das mensagens anteriores oculto]

 **Proposta_Comercial_Caceres_assinado.pdf**
108K



CTI CÁCERES <cacerescti@gmail.com>

COTAÇÃO - SEGURANÇA CIBERNÉTICA

4 mensagens

CTI CÁCERES <cacerescti@gmail.com>

5 de março de 2025 às 16:05

Para: diretoria@redeexs.com.br

Prezado(s),

Cumprimentando-o(s) cordialmente, solicitamos a apresentação de **COTAÇÃO** para a contratação de empresa especializada na prestação de serviços de **segurança cibernética** com **Inteligência Artificial Preditiva**, compreendendo o **fornecimento, em regime de comodato, instalação e configuração de Next Generation Firewall (NGFW) e SD-WAN**, bem como a disponibilização de **redundância de conectividade** por meio de links **primário e secundário** de ASN e rotas distintas.

A contratação abrangerá, ainda, a **manutenção contínua**, o **suporte técnico especializado**, a disponibilização de **software de gerenciamento**, a garantia de **conectividade segura** para **unidades externas e praças públicas**, além da **capacitação certificada da equipe técnica** e o **atendimento técnico especializado**. O objeto da contratação visa assegurar **alta disponibilidade, segurança, eficiência e sustentabilidade** na prestação dos serviços demandados pelo Município de Cáceres.

As condições e especificações encontram-se detalhadas na **planilha de cotação** anexa. Assim, solicitamos o envio da cotação conforme os requisitos estabelecidos.

--

At.te

Coordenação de Tecnologia da Informação

Município de Cáceres

Tel: +55 65 9948-4477

**PLANILHA COTAÇÃO.docx**
155K

Régis Daniel <regis.daniel@redeexs.com.br>

17 de março de 2025 às 23:41

Para: CTI CÁCERES <cacerescti@gmail.com>

Cc: diretoria@redeexs.com.br

À Coordenação de Tecnologia da Informação,

Espero encontrá-los bem!

Segue proposta comercial conforme solicitado.

At.te.,

Régis Daniel

[Texto das mensagens anteriores oculto]



18.03.2025.PropostaComercial.PrefCaceres.pdf
479K

CTI CÁCERES <cacerescti@gmail.com>
Para: Régis Daniel <regis.daniel@redeexs.com.br>

4 de abril de 2025 às 08:10

Prezado(a),

Considerando a identificação de equívoco no preenchimento da cotação, especificamente na coluna referente ao *Valor Unitário Mensal*, a qual foi indevidamente preenchida com o valor total mensal, solicitamos a gentileza de proceder com a devida retificação, inserindo corretamente o valor unitário correspondente.

Informamos que o prazo para envio da resposta com as devidas correções encerra-se em **07 de abril de 2025**.

Desde já, agradecemos pela atenção e colaboração, colocando-nos à disposição para eventuais esclarecimentos que se fizerem necessários.

[Texto das mensagens anteriores oculto]

--

At.te

Coordenação de Tecnologia de Informação

Tel: +55 65 9948-4477

Régis Daniel <regis.daniel@redeexs.com.br>
Para: CTI CÁCERES <cacerescti@gmail.com>
Cc: Roselane Gonzalez do Nascimento Almeida <roselane@redeexs.com.br>

7 de abril de 2025 às 00:21

Bom dia,

segue proposta comercial devidamente preenchida e corrigida.

At.te.,

Régis Daniel

[Texto das mensagens anteriores oculto]



07.04.2025 Proposta Pref Caceres.pdf

469K



CTI CÁCERES <cacerescti@gmail.com>

COTAÇÃO - SEGURANÇA CIBERNÉTICA

6 mensagens

CTI CÁCERES <cacerescti@gmail.com>

5 de março de 2025 às 16:07

Para: lucas.trin.informatica@gmail.com

Prezado(s),

Cumprimentando-o(s) cordialmente, solicitamos a apresentação de **COTAÇÃO** para a contratação de empresa especializada na prestação de serviços de **segurança cibernética** com **Inteligência Artificial Preditiva**, compreendendo o **fornecimento, em regime de comodato, instalação e configuração** de **Next Generation Firewall (NGFW) e SD-WAN**, bem como a disponibilização de **redundância de conectividade** por meio de links **primário e secundário** de ASN e rotas distintas.

A contratação abrangerá, ainda, a **manutenção contínua**, o **suporte técnico especializado**, a disponibilização de **software de gerenciamento**, a garantia de **conectividade segura para unidades externas e praças públicas**, além da **capacitação certificada da equipe técnica** e o **atendimento técnico especializado**. O objeto da contratação visa assegurar **alta disponibilidade, segurança, eficiência e sustentabilidade** na prestação dos serviços demandados pelo Município de Cáceres.

As condições e especificações encontram-se detalhadas na **planilha de cotação** anexa. Assim, solicitamos o envio da cotação conforme os requisitos estabelecidos.

--
At.te

Coordenação de Tecnologia da Informação

Município de Cáceres
Tel: +55 65 9948-4477



Lucas França <lucas.trin.informatica@gmail.com>

Para: CTI CÁCERES <cacerescti@gmail.com>

Prezados Senhores

Bom dia, conforme solicitado enviamos em anexo nossa melhor proposta para a contratação de empresa especializada na prestação **Artificial Preditiva**, compreendendo o **fornecimento, em regime de comodato, instalação e configuração de Next Generation Firewall de redundância de conectividade** por meio de links **primário e secundário** de ASN e rotas distintas..

Ficamos à inteira disposição para qualquer dúvida.

Lucas França
Consultor de Vendas
(62)3251-6464



[Texto das mensagens anteriores oculto]

 **Proposta 20250317 PM Cáceres.pdf**
484K

CTI CÁCERES <cacerescti@gmail.com>
Para: Lucas França <lucas.trin.informatica@gmail.com>

4 de abril de 2025 às 08:10

Prezado(a),

Considerando a identificação de equívoco no preenchimento da cotação, especificamente na coluna referente ao *Valor Unitário Mensal*, a qual foi indevidamente preenchida com o valor total mensal, solicitamos a gentileza de proceder com a devida retificação, inserindo corretamente o valor unitário correspondente.

Informamos que o prazo para envio da resposta com as devidas correções encerra-se em **07 de abril de 2025**.

Desde já, agradecemos pela atenção e colaboração, colocando-nos à disposição para eventuais esclarecimentos que se fizerem necessários.

[Texto das mensagens anteriores oculto]

--

At.te

Coordenação de Tecnologia de Informação

Tel: +55 65 9948-4477

Lucas França <lucas.trin.informatica@gmail.com>
Para: CTI CÁCERES <cacerescti@gmail.com>

Prezados Senhores

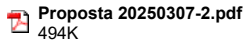
Bom dia, conforme solicitado enviamos em anexo nossa melhor proposta. já retificada, para a contratação de empresa especializada em **segurança cibernética com Inteligência Artificial Preditiva**, compreendendo o **fornecimento, em regime de comodato, instalação e configuração** bem como a disponibilização de **redundância de conectividade** por meio de links **primário e secundário** de ASN e rotas distintas..

Ficamos à inteira disposição para qualquer dúvida.

Lucas França
Consultor de Vendas
(62)3251-6464



[Texto das mensagens anteriores oculto]



CTI CÁCERES <cacerescti@gmail.com>
Para: Lucas França <lucas.trin.informatica@gmail.com>

4 de abril de 2025 às 09:28

Prezado(a),

Solicitamos a gentileza de proceder com a correção do valor unitário informado, observando que o valor final total da proposta **não deverá ser alterado**.

Caso não seja possível manter o montante originalmente apresentado, orientamos que a correção seja efetuada com valores unitários que se aproximem ao máximo do valor global anteriormente ofertado, a fim de preservar a compatibilidade e a razoabilidade da cotação.

Agradecemos, desde já, a atenção dispensada e colocamo-nos à disposição para quaisquer esclarecimentos que se fizerem necessários.

[Texto das mensagens anteriores oculto]

Lucas França <lucas.trin.informatica@gmail.com>
Para: CTI CÁCERES <cacerescti@gmail.com>

Prezados Senhores

Bom dia, conforme solicitado enviamos em anexo nossa melhor proposta, já retificada , para a contratação de empresa especializada: **cibernética com Inteligência Artificial Preditiva**, compreendendo o **fornecimento, em regime de comodato, instalação e configuração** bem como a disponibilização de **redundância de conectividade** por meio de links **primário e secundário** de ASN e rotas distintas..

Ficamos à inteira disposição para qualquer dúvida.

Lucas França
Consultor de Vendas
(62)3251-6464



[Texto das mensagens anteriores oculto]

 **Proposta 20250307-V3 Pm Cáceres.pdf**
494K

Proc. Administrativo Processo Licitatório - 1- 029/2025

De: Andressa C. - SMEAE - Compras

Para: SMEAE - Secretaria Municipal Especial de Assuntos Estratégicos

Data: 20/03/2025 às 09:25:53

Setores envolvidos:

SMEAE-CIS, SMEAE, SMEAE - Compras, SMEAE - CTI

Registro de Preço para futura e eventual aquisição de serviço de locação de firewall e segurança cibernética para atender à demanda do Município de Cáceres

Prezado Secretário,

Segue pesquisa de preço e justificativa da pesquisa de preço.

—

Atenciosamente,

Andressa Nair

Gerência de Compras

Anexos:

COTACAO_Inovasete_Tecnologia_Ltda.pdf

COTACAO_Rede_EXS.pdf

COTACAO_Trin_Informatica_Eireli.pdf

Modelo_de_justificativa_de_pesquisa_de_preco_final.pdf

Assinado por 2 pessoas: WELLINGTON DE BARROS MACIEL e GIRLANE VIEIRA PEREIRA
Para verificar a validade das assinaturas, acesse <https://caceres.1doc.com.br/verificacao/6467-BE37-0266-22F6> e informe o código 6467-BE37-0266-22F6

À
Prefeitura Municipal de Cáceres
Secretaria Municipal de Assuntos Estratégicos
Av. Brasil, nº 119, Jardim Celeste (COC), Cáceres/MT, CEP: 78210-906
CNPJ: 03.214.145/0001-83

PROPOSTA COMERCIAL

Identificação da Empresa: Inovasete Tecnologia Ltda
CNPJ: 10.365.200/0001-00
Endereço: SHN Quadra 1 Cj A Sl 1414 - Asa Norte - Brasília-DF - 70.701-000
Telefone: 61.3255.1253

Objeto: Contratação de empresa especializada na prestação de serviços de segurança cibernética com Inteligência Artificial Preditiva, compreendendo o fornecimento, em regime de comodato, instalação e configuração de Next Generation Firewall (NGFW) e SD-WAN, bem como a disponibilização de redundância de conectividade por meio de links primário e secundário de ASN e rotas distintas.

Item	Especificação	UNIDADE	Quantidade	Valor Unitário Mensal*	Valor Total Anual
1	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)	Serviço	173	R\$ 129.750,00 (R\$ 750,00)	R\$ 1.557.000,00
2	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	Serviço	2	R\$ 37.000,00 (R\$ 18.500,00)	R\$ 444.000,00
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)	Serviço	2	R\$ 7.000,00 (R\$ 3.500,00)	R\$ 84.000,00
4	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 150Mbps Sites Remotos (Fibra Óptica)	Serviço	171	R\$ 42.750,00 (R\$ 250,00)	R\$ 513.000,00
5	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G)	Serviço	171	R\$ 25.650,00 (R\$ 150,00)	R\$ 307.800,00
6	Implantação da Solução	Serviço	1	R\$ 350.000,00	R\$ 350.000,00
7	Capacitação especializada da equipe com emissão de certificação.	Treinamento	1	R\$ 8.500,00	R\$ 8.500,00
8	Consultoria Política de Segurança	Serviço	1	R\$ 35.000,00	R\$ 35.000,00

* Os valores entre parêntesis correspondem ao valor unitário. Sem parêntesis correspondem ao valor mensal do item.

Total da Proposta: R\$ 3.299.300,00 (Três milhões, duzentos e noventa e nove mil e trezentos reais).

Dados Bancários:
Banco de Brasília S.A. (BRB) - 070 - Agência 0164 - Conta 164009250-9

Declaramos ter pleno conhecimento das condições e peculiaridades inerentes à natureza dos trabalhos, assumindo total responsabilidade pela ocorrência de eventuais prejuízos em virtude de sua omissão na verificação das condições descritas neste termo, com vistas a proteger o interesse da Administração na fase de execução do contrato, nos termos do Acórdão 1.174/2008 – Plenário – TCU, em não havendo vistoria.

A contratação abrangerá, ainda, a manutenção contínua, o suporte técnico especializado, a disponibilização de software de gerenciamento, a garantia de conectividade segura para unidades externas e praças públicas, além da capacitação certificada da equipe técnica e o atendimento técnico especializado. O objeto da contratação visa assegurar alta disponibilidade, segurança, eficiência e sustentabilidade na prestação dos serviços demandados pelo Município de Cáceres.

Brasília, 17 de março de 2025.

Documento assinado digitalmente
 **ALAN MATHEUS TORRES DOS REIS**
Data: 17/03/2025 14:01:41-0300
Verifique em <https://validar.iti.gov.br>

Alan Matheus Torres dos Reis
Sócio-Administrador

À

Prefeitura Municipal de Cáceres

Secretaria Municipal de Assuntos Estratégicos

Av. Brasil, nº 119, Jardim Celeste (COC), Cáceres/MT, CEP: 78210-906

CNPJ: 03.214.145/0001-83

A/C, Gerente de TI da Prefeitura de Cáceres

Proposta Comercial

A EXS agradece a oportunidade de apresentar sua proposta para o fornecimento de Serviços de Cibersegurança para a Prefeitura de Cáceres.

Nos sentimos honrados em poder prestar nosso apoio e conhecimento na busca das soluções mais adequadas ao seu negócio, agregando tecnologia e serviços de qualidade às suas necessidades.

Estamos à disposição para esclarecer quaisquer dúvidas, com o objetivo de alinhar nossa proposta às suas necessidades.

Atenciosamente, Roselane Almeida
Administradora, *Rede EXS*

1. Apresentação

A EXS é uma empresa brasileira, sediada em Brasília, licenciada pela ANATEL como operadora SCM e SAC.

Nossos serviços contemplam Cibersegurança e conectividade para corporativo e governo.

2. Objetivo

Apresentar uma solução de conectividade à internet com base em tecnologia de última geração proporcionando alta qualidade na comunicação e uma melhor experiência.

3. Descrição do Serviço e Condições Comerciais

Fornecimento de serviços de Firewall de Nova Geração, Segurança Cibernética baseada em Inteligência Artificial, link de Internet e Transferência de Conhecimento.

Item	Especificação	UNIDADE	Quantidade	Valor Unitário Mensal	Valor Total Anual
1	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)	Serviço	173	R\$ 112.450,00	R\$ 1.349.400,00
2	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	Serviço	2	R\$ 33.000,00	R\$ 396.000,00
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)	Serviço	2	R\$ 8.000,00	R\$ 96.000,00
4	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 150Mbps Sites Remotos (Fibra Óptica)	Serviço	171	R\$ 39.330,00	R\$ 471.960,00
5	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G)	Serviço	171	R\$ 32.319,00	R\$ 387.828,00
6	Implantação da Solução	Serviço	1	R\$ 300.000,00	R\$ 300.000,00
7	Capacitação especializada da equipe com emissão de certificação.	Treinamento	1	R\$ 8.500,00	R\$ 8.500,00
8	Consultoria Política de Segurança	Serviço	1	R\$ 35.000,00	R\$ 35.000,00

4. Confidencialidade

Todas as informações obtidas por meio dessa negociação são confidenciais, as partes se obrigam a manter o mais absoluto sigilo com relação a toda e qualquer informação, dados, sistemas, dentre outros, que venha ter acesso, a partir do recebimento desta proposta comercial, exceto nos casos de compras governamentais.

5. Considerações finais

CNPJ: 23.935.457/0001-03

E-mails/contatos: roselane@redeexs.com.br / financeiro@redeexs.com.br / 21-991959540

Emissão da proposta: 18/03/2025

Validade da Proposta: 60(sessenta) dias.

ROSELANE GONZALEZ DO
NASCIMENTO
ALMEIDA:07894477702

Assinado de forma digital por
ROSELANE GONZALEZ DO NASCIMENTO
ALMEIDA:07894477702
Dados: 2025.03.18 00:00:26 -03'00'

Proposta

Conforme solicitado em vosso e-mail de 05 de março de 2025, estamos apresentando abaixo nossa proposta para contratação de empresa especializada na prestação de serviços de **segurança cibernética com Inteligência Artificial Preditiva**, compreendendo o **fornecimento, em regime de comodato, instalação e configuração de Next Generation Firewall (NGFW) e SD-WAN**, bem como a disponibilização de **redundância de conectividade** por meio de links **primário e secundário** de ASN e rotas distintas.

PRAZO - O prazo desta proposta é 90 dias.

FORMAS DE PAGAMENTO - Conforme condições do edital.

DADOS DO PROPONENTE Razão Social: Trin Informatica Eireli.

CNPJ: 27.784.894/0001-04

Endereço: Rua T 36, 3385 Qd 146 L8 - 1004

Goiânia / GO, Brasil / CEP 74223-052

Goiânia 17 de Março de 2025



PESQUISA DE PREÇO		
Nome Fantasia: PREFEITURA MUNICIPAL DE CÁCERES		
Endereço: <i>Av. Brasil, nº 119, Jardim Celeste (COC), Cáceres/MT, CEP: 78210-906</i>		
CNPJ: <i>03.214.145/0001-83</i>		
E-mail: <i>cacerescti@gmail.com</i>	Contato: <i>(65) 99948-4477</i>	
DADOS DA EMPRESA		
Nome Fantasia: <i>Trin Informática Eireli ME</i>		
Razão Social <i>trin Informática</i>		
CNPJ: <i>27.784.894/0001-04</i>	Optante pelo simples: (X) Sim () Não	
Insc. Est.:	Insc. Mun.: <i>4427963</i>	
Endereço: <i>Rua T-36 3385 Qd 146 Lt 8 1004</i>	Bairro: <i>Setor Bueno</i>	
Cidade: <i>Goiânia</i>	CEP: <i>74223-052</i>	
E-mail: <i>lucas.trin.informatica@gmail.com</i>	Telefone: <i>(62) 98338-9022</i>	
Banco: <i>Banco do Brasil</i>	Nº Agência: <i>367-0</i>	Conta Bancária nº: <i>110161-7</i>

ITEM	ESPECIFICAÇÃO	UNIDADE	QUANTIDADE	VALOR UNITÁRIO MENSAL	VALOR TOTAL ANUAL
1	Serviço de provimento de solução de Firewall de Nova Geração e SD-WAN (Alta Disponibilidade)	Serviço	173	R\$132.000,00	R\$1.584.000,00
2	Serviço de Segurança cibernética, baseado em Inteligência Artificial Preditiva	Serviço	2	R\$50.000,00	R\$600.000,00
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)	Serviço	2	R\$7.250,00	R\$ 87.000,00
4	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 150Mbps Sites Remotos (Fibra Óptica)	Serviço	171	R\$44.000,00	R\$528.000,00
5	Serviço de Link de acesso à Internet Banda Mínima de Acesso Garantida de 35Mbps Sites Remotos (Fibra Óptica e 4/5G)	Serviço	171	R\$26.500,00	R\$ 318.000,00
6	Implantação da Solução	Serviço	1	R\$ 340.000,00	R\$ 340.000,00
7	Capacitação especializada da equipe com emissão de certificação.	Treinamento	1	R\$ 8.250,00	R\$8.250,00
8	Consultoria Política de Segurança	Serviço	1	R\$37.000,00	R\$ 37.000,00




Goiânia 17/03/2025

JUSTIFICATIVA PESQUISA DE PREÇOS

1. DA PESQUISA DE PREÇOS Certifico que as pesquisas de preços foram realizadas conforme as normas estabelecidas pelo decreto municipal nº 240/2023, que dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral, no âmbito da Administração Pública. Ainda de acordo com o Art. 5º desse decreto, segue informações mínimas necessárias sobre a Pesquisa de Preços que integra esse Processo:

I - A pesquisa de preço foi realizada considerando os parâmetros dispostos no Art. 5º decreto municipal nº 240/2023, empregados de forma combinada: prioritariamente, foram consultados os preços através do sítio “banco de preços”(RADAR E PAINEL DE PREÇO), uma ferramenta informatizada, cuja pesquisa baseia-se em resultados de licitações adjudicadas e/ou homologadas realizadas pela administração pública o que contempla os parâmetros do Art. 5º decreto municipal nº 240/2023, Contudo, não obtivemos êxito, pois cada órgão público descreve o serviço de maneira distinta, o que impossibilitou a localização da pesquisa de preços tanto no painel quanto no radar. Foi realizada a pesquisa com fornecedor e obtivemos êxito.

III - Os comprovantes das pesquisas de preços coletadas integram este processo como documento anexo, em formato PDF. Estas informações subsidiaram a elaboração do Mapa de Preços no qual constam a média saneada de preços para o estabelecimento dos valores unitários máximos dos itens a serem licitados. O Mapa de Preços também é um anexo em formato PDF que compõe este processo;

IV - Considerando o Art. 6º decreto municipal nº 240/2023 foi utilizado, como método para obtenção do preço estimado por item, justifica-se que a metodologia de tratamento de dados utilizada foi a **média** dos valores obtidos na pesquisa de preços, sobre um conjunto preços, sendo este com valor economicamente viável para este órgão.

2.1 DA ANÁLISE CRÍTICA DOS PREÇOS PESQUISADOS

Declaramos que foi feita análise crítica dos preços coletados, observou-se que os valores das propostas não apresentaram muita variação. Assim, buscou-se, dentro do



conhecimento do material a ser adquirido/contratado, estabelecer um preço de referência condizente com o praticado no mercado. O Mapa de preço foi composto por no mínimo 3 preços.

Justificativa da escolha dos fornecedores

Introdução Primeiramente, de acordo com o Art. 5º decreto municipal nº 240/2023, as pesquisas de preço foram obtidas de acordo com o Artigo 5º, inciso IV § 2º, “pesquisa direta com fornecedores, mediante solicitação formal de cotação.

Da Pesquisa de Preço Optou-se pela pesquisa direta junto aos fornecedores locais e que os estão cadastrados no nosso sistema ou que já participaram dos nossos pregões.

Do prazo de resposta conferida ao fornecedor compatível com a complexidade do objeto a ser licitado: Após a compatibilização dos serviços em planilha, a mesma foi remetida aos fornecedores no intuito de adquirir a cotação em prazo estipulado e considerado razoável devido a especificação o objeto e quantidade de itens informada. A solicitação das propostas aos fornecedores foi feita via e-mail na data de 5 de março de 2025, estipulamos a data de entrega das propostas até a data de 17 de março de 2025, ou seja, aproximadamente 12 dias após a solicitação feita.

Obtenção de propostas formais, contendo, no mínimo

- a) descrição do objeto, valor unitário e total;
- b) número do Cadastro de Pessoa Física - CPF ou do Cadastro Nacional de Pessoa Jurídica - CNPJ do proponente;
- c) endereços físico e eletrônico e telefone de contato;
- d) data de emissão; e
- e) nome completo e identificação do responsável.

III - registro, nos autos da contratação correspondente, da relação de fornecedores que foram consultados e não enviaram propostas como resposta à solicitação de que trata o inciso IV do caput. Após o prazo estipulado para entrega das propostas, observou-se que 3 empresas deixaram de encaminhar suas propostas.



LISTA DE FORNECEDORES CONSULTADOS

FORNECEDOR	E-MAIL	DATA QUE ENVIOU O EMAIL	DATA QUE REINTER OU O PEDIDO NO E-MAIL	RECEBEM OS A PESQUISA (SIM/NÃO)	OBSERVAÇÃO
REDE EXS	diretoria@redeexs.com.br	qua., 5 de mar., 16:05	NÃO SE APLICA	SIM	
INOVASETE TECNOLOGIA LTDA	sandro.araujo@camoa.com.br governo@camoa.com.br	qua., 5 de mar., 16:06	NÃO SE APLICA	SIM	
TRIN INFORMÁTICA EIRELI	lucas.trin.informatica@gmail.com	qua., 5 de mar., 16:07	NÃO SE APLICA	SIM	
BRAVA INTERNET	central@bravainternet.com.br	qua., 5 de mar., 16:08	NÃO SE APLICA	NÃO	
DUNET FIBRAS	atendimento01@dunetfibras.com.br	qua., 5 de mar., 16:13	NÃO SE APLICA	NÃO	
SEEG FIBRAS	financeiro@seegfibras.com.br	qua., 5 de mar., 16:16	NÃO SE APLICA	NÃO	





VERIFICAÇÃO DAS ASSINATURAS



Código para verificação: 6467-BE37-0266-22F6

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



WELLYNGTON DE BARROS MACIEL (CPF 004.XXX.XXX-60) em 20/03/2025 08:37:19 GMT-04:00

Papel: Parte

Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)



GIRLANE VIEIRA PEREIRA (CPF 024.XXX.XXX-66) em 20/03/2025 09:13:39 GMT-04:00

Papel: Parte

Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

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

<https://caceres.1doc.com.br/verificacao/6467-BE37-0266-22F6>

De: Andressa C. - SMEAE - Compras

Para: SMA-CACBS - Coordenadoria de Aquisição e Controle de Bens e Serviços

Data: 21/03/2025 às 14:44:54

Segue para providências.

—

Atenciosamente,

Andressa Nair
Gerência de Compras

De: Aurelio O. - SMA-CACBS

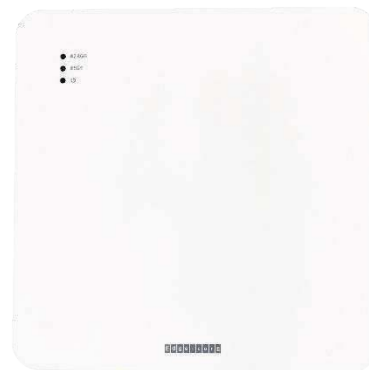
Para: SMEAE - Compras - Gerência de Compras

Data: 21/03/2025 às 16:14:25

Segue para inserir código do TCE nos itens no TR

—

Aurelio Ortiz

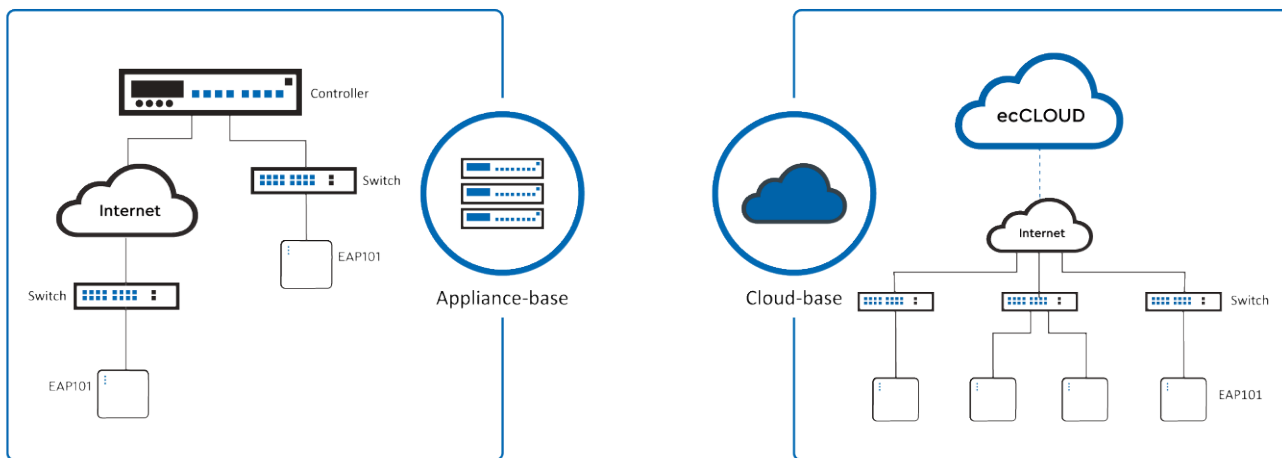


EAP101

Wi-Fi 6 屋内アクセスポイント

概要

EAP101は、エンタープライズグレードの同時デュアルバンドWi-Fi 6屋内アクセスポイントです。EAP101は、APと複数のクライアント間で2x2:2のアップリンクおよびダウンリンクMU-MIMOをサポートし、最大1.7Gbpsのアグリゲーション・データ・レートを実現します。EAP101はBluetooth Low Energy (BLE) 無線とZigBeeを搭載し、iBeaconなどの付加価値アプリケーションを実現します。スタンドアロン・モードで動作させ、EdgecoreのecCLOUDおよびEWSシリーズ・コントローラで管理することもできます。さらに、ecCLOUDで管理する場合、EAP101はAI対応のパフォーマンス検出をサポートし、管理者がネットワーク・パフォーマンスを監視・強化するのに役立ちます。



ハイライト

- 同時デュアルバンド2.4GHz & 5GHz
- 802.11ax 2x2:2 UL MU-MIMO、最大1.7Gbpsデータレートをサポート
- 最大32のESSIDをサポート
- エンタープライズグレードの無線セキュリティ
- Bluetooth Low Energy (BLE) 5.2
- ZigBee
- 802.3at power over ethernet (PoE)

性能

物理面	
電源	- DC入力： 12V/2.0A（電源アダプター付属） - PoE： 802.3at準拠（PoEインジェクターは含まれません）
寸法（長さ×幅×高さ）	19.5 cm x 19.5 cm x 3.9 cm (7.68 x 7.68 x 1.54 in)
重量	0.65 kg (1.44 lb)
インターフェース	- アップリンク 1 x 10/100/1000/2.5GBase-Tイーサネット、自動MDIX、802.3at PoE付きRJ-45 - LAN： 2 x 10/100/1000Base-Tイーサネット、自動MDIX、RJ-45 - コンソール 1 x RJ-45ポート - USB: 1 x USB 2.0ポート
LEDインジケーター	2.4G-WiFi / 5G-WiFi / Power
ボタン	リスタート/リセット
環境条件	- 動作温度 0° C (32° F) ～ 50° C (122° F) - 動作湿度： 5%～95%（結露なし）
電力消費	最大22.4 W
アンテナ	- タイプ 3 x 内蔵アンテナ（2 x 2.4 GHz & 5 GHz、1 x BLE） - ゲイン： 4.8 dBi（2.4 GHz）、6 dBi（5 GHz）、4.6 dBi（BLE）
マウンティング	壁/天井/Tバーマウント（マウントキット付属）
盗難防止対策	1 x Kensington lock slot
Wi-Fi	
標準	802.11ax (Wi-Fi 6) - コンカレント対応デュアルバンド2.4 & 5 GHz
対応データレート	802.11b: 1, 2, 5.5, 11 Mbps 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps 802.11n: 6.5 – 300 Mbps (20 / 40 MHz) 802.11ac: 6.5 – 867 Mbps (20 / 40 / 80 MHz) 802.11ax: 3.6 – 574 Mbps (2.4 GHz, 20 / 40 MHz) 802.11ax: 3.6 – 1200 Mbps (5 GHz, 20 / 40 / 80 MHz)
無線チェーン	2 x 2
空間ストリーム	2; MU-MIMO
合計伝導率 送信電力 ¹	2.4 GHz: 最大26 dBm² 5 GHz: 最大26 dBm²
チャンネル	2.4 GHz: 20 / 40 MHz 5 GHz: 20 / 40 / 80Mhz
周波数範囲	2.400 – 2.483 GHz 5.150 – 5.850 GHz
動作チャンネル	2.4 GHz: 1-11 (US), 1-13 (欧州), 1-13 (日本) 5 GHz³: 36-165 (US), 36-140 (欧州), 36-144 (日本)
ESSID	無線1つにつき最大16台（合計32台）
認証	FCC, CE, LVD, NCC, BSMI, VCCI, JATE, TELEC, IC, C-Tick

1: RF出力電力はMIMOチェーン全体で集約され、アンテナゲインは含まれません。

2: 最大出力は地域の規制要件に依存し、制限されることがあります。

3: 一部のチャンネルは、地域の規制および認証によって制限されています。

1Doc: Protocol 1.943/2025 Annex Item 34070680059 Data Sheet EAP101 Progress Administrative 02/9/2025so Alimto EAP101 2025 sheet JB.pdf (2/89) 1962/4726

Copyright © 2023 Edgecore Networks Corporation

パフォーマンス	
物理データレート	- 最大574 Mbps (2.4 GHz) - 最大1200 Mbps (5 GHz)
特徴	
無線	802.11 k/v/r - Orthogonal Frequency Division Multiple Access (OFDMA) - Client Isolation - Open Mesh - BSS Coloring - Band Steering - Wi-Fi Enhanced Open (OWE) - Wireless Site Survey
ネットワーク	- Spanning Tree Protocol (STP) - Dynamic Host Configuration Protocol (DHCP) - DHCP Relay 802.1q - Access Control List (ACL) - Network Address Translation (NAT) - Dynamic VLAN - Link Layer Discovery Protocol (LLDP) - Smart Isolation - IPv6 compatible - Proxy ARP
セキュリティ	- WPA-Personal (AES) - WPA-Enterprise (AES) - WPA2-Personal (AES) - WPA2-Enterprise (AES) - WPA3-Personal (AES) - WPA3-Personal Transition (AES) - WPA3-Enterprise (AES) - WPA3-Enterprise Transition (AES) - Multi Pre-Shared Key (MPSK) - Dynamic Pre-Shared Key (DPSK) - MAC Address Authentication - DHCP Snooping - ARP Inspection - L3 Firewall
メンテナンス	- Network Time Protocol (NTP) - Standalone - Management by ecCLOUD - Management by ecCLOUD-VPC - Management by EWS-Series Controller (Complete Tunnel/Split Tunnel) - SSH - QR Code Onboarding - SNMP v1/v2c/v3 - Remote Syslog - Discovery Tool - Zero Touch Provisioning (ZTP)

QoS

- RSSI Threshold (Optimal Client Filtering)
- Multicast-to-Unicast Conversion
- WME

その他

- Target Wake Time (TWT)
- iBeacon
- Hotspot Captive Portal
- Dynamic Authorization (DAE)

インターネット (WAN)

- Throughput (Up/Down)
- Packet Drops
- Roundtrip Latency
- Usage

Wi-Fi 接続

- DHCP Exchanges
- EAP Failures
- Slow Connectivity
- Connection Drops
- Poor Signal
- Beacon Miss
- Steering Efficiency
- AP Stability
- Wrong Key
- Inactivity
- Radio Congestion
- Wi-Fi Latency
- Hogging Airtime

Wi-Fi ローミング

- Poor AP Selection
- Poor Overlap
- AP Slow Response
- Sticky Client
- Slow Roaming

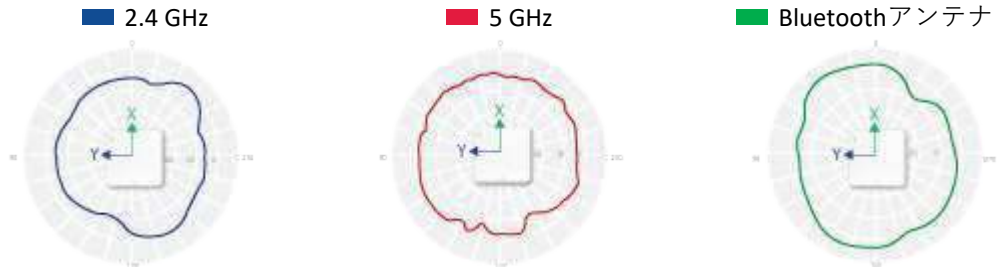
アプリケーション

- Reachability
- Upstream Health
- Downstream Health

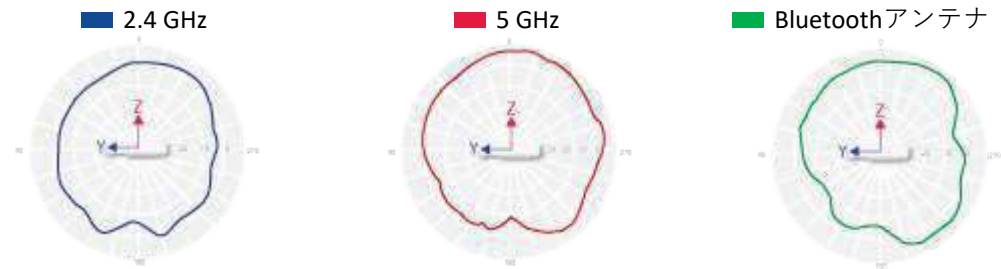
4：アプレコム[®]のAIソリューションVWE（Virtual Wireless Expert）を有効にしてecCLOUDで管理した場合。

シグナルカバレッジパターン

方位角



仰角



受信感度

動作モード	データレート	受信感度 (dBm)
802.11b	1 Mbps	-95
	11 Mbps	-87
802.11a	6 Mbps	-89
	54 Mbps	-72
802.11g	6 Mbps	-90
	54 Mbps	-73
802.11n (2.4 GHz/HT20)	MCS0	-90
	MCS7	-72
802.11n (2.4 GHz/HT40)	MCS0	-86
	MCS7	-70
802.11n (5 GHz/HT20)	MCS0	-89
	MCS7	-71
802.11n (5 GHz/HT40)	MCS0	-86
	MCS7	-70
802.11ac (VHT20)	MCS0	-90
	MCS8	-69
802.11ac (VHT40)	MCS0	-86
	MCS9	-64
802.11ac (VHT80)	MCS0	-84
	MCS9	-60
802.11ax (2.4 GHz/HE20)	MCS0	-90
	MCS11	-62
802.11ax (2.4 GHz/HE40)	MCS0	-86
	MCS11	-59
802.11ax (5 GHz/HE20)	MCS0	-89
	MCS11	-60
802.11ax (5 GHz/HE40)	MCS0	-86
	MCS11	-58
802.11ax (5 GHz/HE80)	MCS0	-84
	MCS11	-56

Package Contents



1. EAP101 access point

2. AC power adapter with international socket converters

3. Mounting bracket accessory

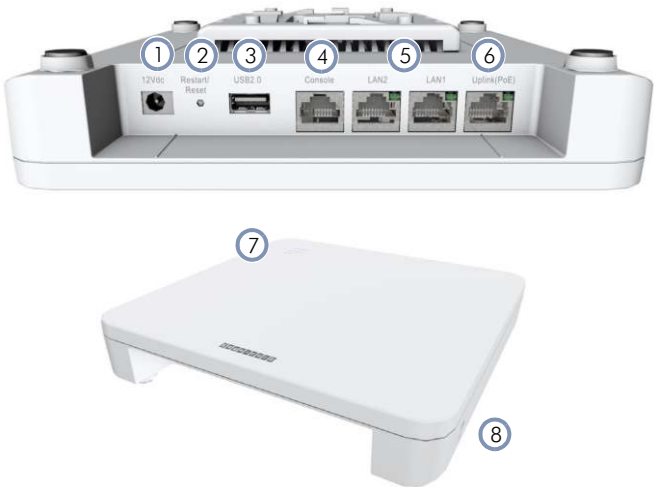
4. Mounting bracket security screw

5. Screw kit—4 screws and 4 plugs

6. Console cable—RJ-45 to DB-9 (TIP SKU only)

7. QR code card

Overview



1. 12 VDC power input

2. Restart/Reset button:
 - A quick press restarts the system.
 - Press and hold for 5 seconds resets to factory defaults.

3. USB 2.0 port (reserved for future use)

4. Console port (reserved for future use)

5. LAN1/LAN2 Ports: 1Gbps connection to LAN devices.
 - Port LED: On (link), Blinking (traffic)

6. Uplink(PoE) Port: 2.5Gbps connection to 802.3at PoE.
 - Port LED: On (link), Blinking (traffic)

7. System LED Indicators:
 - 2.4G: On (radio on), Blinking (traffic)
 - 5G: On (radio on), Blinking (traffic)
 - Power/Status: On (power OK), Blinking (boot up)

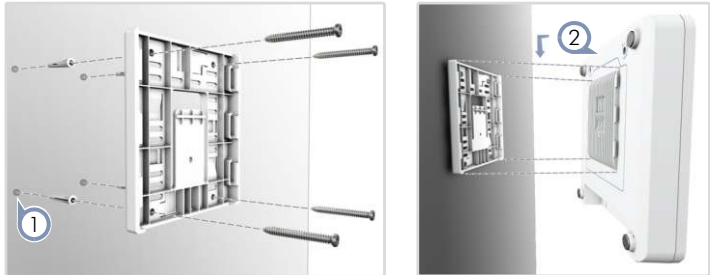
8. Kensington lock slot

Installation

**Warning:** For indoor use only. The access point, AC power adapter, and all connected cables are not for outdoor use.

1 Mount the AP

a. Mounting on a Wall



1. At the installation location on the wall, use the mounting bracket to mark four holes for the wall plugs and screws (included in the screw kit).

Drill four holes for the wall plugs, and then insert the plugs and tap them flush with the wall surface.

**Note:** Drill 2.5 mm (± 0.2 mm) holes for M3 self-tapping screws, or 4.5 mm (± 0.2 mm) holes for nylon wall plugs.

Use the four screws to secure the bracket to the wall.

2. With its ports facing down, place the AP over the bracket flanges and then slide it down until it snaps into its secured position.

b. Mounting on a Suspended Ceiling T-Bar



1. Slide the bracket accessory onto the base of the AP until it clicks into its locked position.

2. Use the included security screw to secure the bracket to the AP.

3. Position the ceiling-mount clip holders on either side of the T-bar, and then turn the AP until the two clips lock it to the T-bar.

**Note:** The AP mounting supports two different sizes of suspended ceiling T-bars. The position illustrated above is for 24.5 mm bars. Use the position at a 90 degrees angle for 15 mm bars.

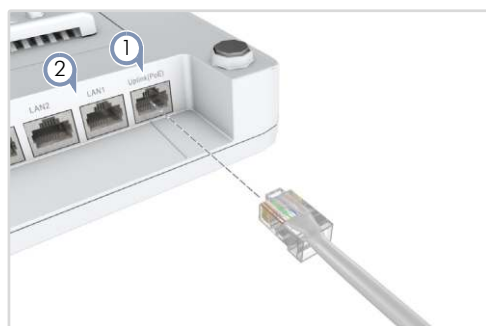
c. Mounting on a Ceiling Without T-Bars



1. At the installation location on the ceiling, use the mounting bracket to mark four holes for the plugs and screws (included in the screw kit).
Drill four holes for the plugs, and then insert the plugs and tap them flush with the ceiling surface.
Use the four screws to secure the bracket to the ceiling (screw torque must be less than 6 kgf.cm).
2. Place the AP over the bracket flanges and then slide it onto the bracket until it snaps into its secured position.

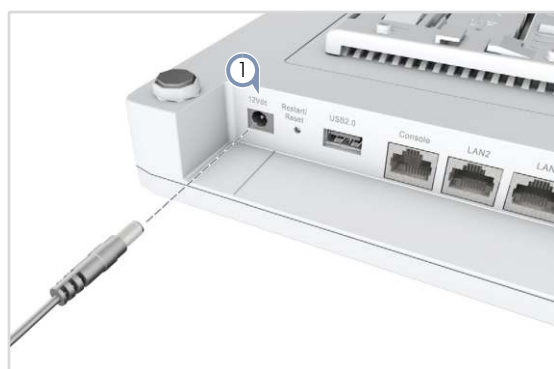
2 Connect Cables

g. Connect LAN Cables



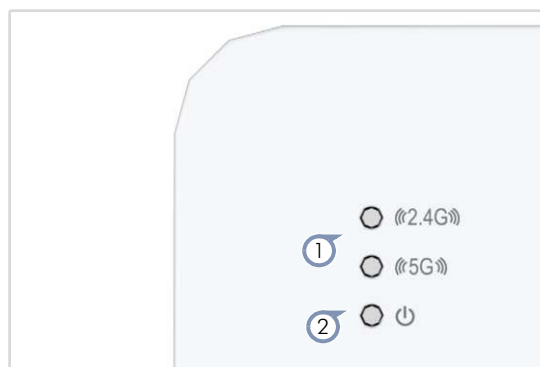
1. Connect Category 5e or better cable to the Uplink(PoE) 2.5G RJ-45 port. When connected to a PoE source, the Uplink(PoE) port connection provides power to the unit.
2. (Optional) Connect a local LAN switch or computer to the LAN1 or LAN2 1000BASE-T RJ-45 ports.

b. (Optional) Connect AC Power Adapter



1. When not connected to a PoE source, connect the AC power adapter to the DC power jack on the AP and then plug the adapter into a nearby AC power source.

3 Check AP LEDs



1. 2.4G and 5G LEDs — on green for radio enabled.
2. Power/Status LED — on green for normal operation.

4 Connect to the Web User Interface

1. Connect a PC directly to the AP's LAN1 or LAN2 port.
2. Set the PC IP address to be on the same subnet as the AP LAN port default IP address. (The PC address must start 192.168.2.x with subnet mask 255.255.255.0.)
3. Enter the AP's default IP address of 192.168.2.1 into the web browser address bar.

Note: To connect to the web interface using the Uplink(PoE) port, the IP address is automatically assigned through DHCP by default. If a DHCP server is unreachable, the Uplink(PoE) port reverts to a fallback IP address of 192.168.1.10.

4. On first-time log in to the web interface, the Setup Wizard starts and you must select how the AP will be managed, either using the ecCLOUD controller, an EWS-Series controller, or in stand-alone mode.

SETUP WIZARD

Will this device be managed?

☒ Yes, I will manage this device by ecCloud controller.

☐ Yes, I will manage this device by EWS-Series controller.

☐ No, I will be operating this device in stand-alone mode.

+ [Select Your Country](#)

Done

- Continue with the Setup Wizard to make other settings:
 - Cloud-Managed Mode:** Select the country of operation.
 - EWS-Series Controller Mode:** Complete the CAPWAP setup, use the default wireless network setting or customize the network name, then set a password (the default user name is “admin” with password “admin”), and select the country of operation.
 - Stand-Alone Mode:** Use the default wireless network setting or customize the network name, then set a password (the default user name is “admin” with password “admin”), and select the country of operation.
- Click “Done” to finish the setup wizard.

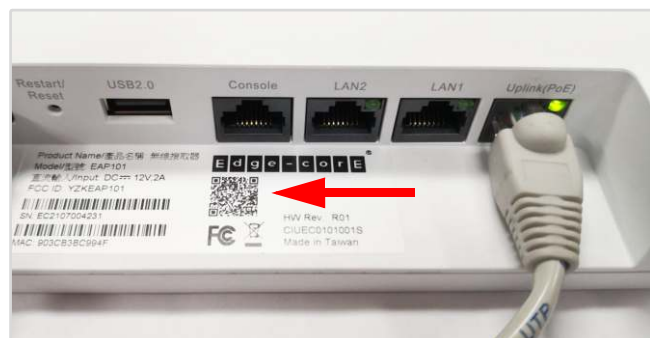
 **Note:** For more information on the Setup Wizard and AP configuration, refer to the *User Manual*.

5 (Optional) QR Code Onboarding

For quick set up and registration of your AP with the ecCLOUD controller, you can scan the QR code on the AP using a phone.

Follow these steps:

1. Make sure the AP is powered on and connected to the Internet.
2. Use the camera (iPhone) or a barcode app (Android) on your phone to scan the AP's QR code. The QR code is printed on a label next to the AP's ports.



3. When a message pops up, tap "yes" to join the Wi-Fi network (iPhone requires you to go to Settings > Wi-Fi or open the browser for the message to pop up).

The web browser should open and redirect to the Setup Wizard page.



Note: If the phone cannot connect to the Wi-Fi network, type the SSID (network name) and password manually. The SSID name is the AP serial number (for example, EC0123456789), and the password is the AP MAC address (for example, 903CB3BC1234).

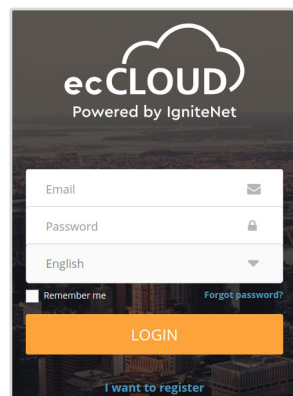
4. After setting a new password and the regulatory country, select to manage the AP using the ecCLOUD controller, an EWS-Series controller, or to manage the AP in stand-alone mode.

- a. Stand-Alone Mode:** Use the default wireless network setting or customize the network name and password. Tap "Done" to finish the Setup Wizard.

Wait about two minutes for the AP configuration to update, and then connect to the wireless network name configured in the setup wizard. The browser is then redirected to the login page of the AP.

- b. EWS-Series Controller Mode:** Complete the CAPWAP setup, then set a password and select the country of operation. Tap "Done" to finish the setup wizard.

- c. Cloud-Managed Mode:** Tap "Done" to finish the setup wizard and the browser is redirected to the ecCLOUD login page.



If you already have an ecCLOUD account, log in and select a site for the AP. The AP is automatically registered for cloud management. After you tap "Save," wait about two minutes for the cloud controller to configure the AP.

If you do not have an ecCLOUD account, tap "I want to register" and first set up an account. Create a cloud and site before confirming the regulatory country. After tapping "Next," the AP is then automatically registered for cloud management. After you tap "Save," wait about two minutes for the cloud controller to configure the AP.



Note: Refer to the Edgecore ecCLOUD Controller User Manual for more information on setting up and configuring APs through ecCLOUD.

Safety and Regulatory Information

FCC Class B

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

Professional Installation Instructions

1. Installation personnel

This product is designed for specific applications and should be installed by qualified personnel who have knowledge of RF and its related regulations. A general user shall not attempt to install or modify the equipment configuration.

2. Installation location

To meet regulatory RF exposure requirements, this product shall be installed at a location where, during normal operations, the radiating antenna is at least 23 cm away from any nearby persons.

3. External antenna

Use only the antennas which have been approved by the applicant. Using non-approved antenna(s) is prohibited and may produce unwanted spurious or excessive RF transmitting power which may lead to a violation of FCC limits.

4. Installation procedure

Please refer to this equipment's user manual for the procedure details.

5. Warning

The installation position must be carefully selected so that the final output power does not exceed the limit set forth in relevant regulations. Violation of output power regulations could lead to serious federal penalties.

Industry Canada

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

(1) This device may not cause interference.

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil contient des émetteurs / récepteurs exempts de licence qui sont conformes au (x) RSS (s) exemptés de licence d'Innovation, Sciences et Développement économique Canada. L'opération est soumise aux deux conditions suivantes:

(1) Cet appareil ne doit pas provoquer d'interférences.

(2) Cet appareil doit accepter toute interférence, y compris les interférences susceptibles de provoquer un fonctionnement indésirable de l'appareil.

The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

IMPORTANT NOTE:

IC Radiation Exposure Statement:

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 28 cm between the radiator & your body.

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 28 cm de distance entre la source de rayonnement et votre corps.

CE Statement

This equipment complies with EU radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 24 cm between the radiator and your body.

The device is restricted to indoor use only when operating in the 5150 to 5350 MHz frequency range.

All operational modes:

2.4 GHz: 802.11b, 802.11g, 802.11n (HT20), 802.11n (HT40), 802.11ac (VHT20), 802.11ac (VHT40), 802.11ax (HE20), 802.11ax (HE40)

5 GHz: 802.11a, 802.11n (HT20), 802.11n (HT40), 802.11ac (VHT20), 802.11ac (VHT40), 802.11ac (VHT80), 802.11ax (HE20), 802.11ax (HE40), 802.11ax (HE80)

BLE 2.4 GHz: 802.15.1

The frequency and maximum transmitted power limit in EU are listed as below:

2412-2472 MHz: 20 dBm

5150-5350 MHz: 23 dBm

5500-5700 MHz: 30 dBm

AT	BE	BG	CH	CY	CZ
DE	DK	EE	EL	ES	FI
FR	HR	HU	IE	IS	IT
LI	LT	LU	LV	MT	NL
NO	PL	PT	RO	SE	SI
SK	TR	UK			

CE



Hardware Specifications

AP Chassis

Size (WxDxH)	195 x 195 x 39 mm (7.68 x 7.68 x 1.54 in.)
Weight	0.65 kg (1.435 lb)
Temperature	Operating: 0° C to 50° C (32° F to 122° F) Storage: -20° C to 60° C (-4° F to 140° F)
Humidity	Operating: 5% to 95% (non-condensing)

Network Interfaces

Ports	Uplink(PoE) RJ-45 Port: 2.5G, PoE PD LAN1 RJ-45 Port: 1000BASE-T LAN2 RJ-45 Port: 1000BASE-T
2.4 GHz Radio	IEEE 802.11b/g/n/ax
5 GHz Radio	IEEE 802.11a/ac/n/ax
Bluetooth Radio	IEEE 802.15.1
Radio Frequencies	2.4–2.4835 GHz (US, Canada, ETSI, Japan, TW) 5.15–5.25 GHz (lower band) US/Canada, TW 5.725–5.825 GHz (upper band) US/Canada, TW Europe 5.15–5.25 GHz, 5.25–5.35, 5.47–5.725 GHz Japan 5.15–5.25 GHz, 5.25–5.35, 5.47–5.73 GHz

Power Specifications

PoE Input Power	22.4 W max, 48 VDC–55 VDC; 802.3at-compliant
AC Power Adapter	AC Input: 100–240 VAC, 50-60 Hz DC Output: 12 VDC, 2 A

Regulatory Compliances

Radio	EN300 328 V2.2.2 (2019-07) EN301 893 V2.1.1(2017-05) 47 CFR FCC Part 15.247 47 CFR FCC Part 15.407 IC RSS-247 Issue 2 and RSS-Gen Issue 5 NCC LP0002 Section 4.10.1 (2020-07-01) NCC LP0002 Section 5.7 (2020-07-01) MIC certification Rule, Article 2 Paragraph 1 Item 19 MIC certification Rule, Article 2 Paragraph 1 Item 19-3
Emissions	EN 301 489-1 V2.1.1 (2017-02) EN 301 489-17 V3.1.1 (2017-02) EN 55032:2015 AS/NZS CISPR 32:2015, Class B 47 CFR FCC Rules and Regulations Part 15 Subpart B, Class B Digital Device ICES-003, Issue 7 Class B CNS 13438 terminal equipment design certification, Article 3, Article 4, Article 6, Article 9 and Article 34 regulation
Safety	Low Voltage Directive IEC 62368-1:2014;and/or EN 62368-1:2014+A11:2017; and/or BS 62368-1:2014+A11:2017 CNS 14336-1 IEC/EN 62368-1, IEC/EN 60950-1
Taiwan RoHS	CNS 15663

Quick Start Guide

802.11ax Dual-Band Enterprise Access Point
EAP101 (P)

Package Contents



1. EAP101 (P) access point
2. AC power adapter with international socket converters
3. Mounting bracket accessory
4. Mounting bracket security screw
5. Screw kit—4 screws and 4 plugs
6. QR code card

Overview



1. 12 VDC power input
2. Restart/Reset button:
 - A quick press restarts the system.
 - Press and hold for 5 seconds resets to factory defaults.
3. USB 2.0 port (reserved for future use)
4. Console port (not functional)
5. LAN1/LAN2 Ports: 1 Gbps connection to LAN devices.
 - Port LED: On (link), Blinking (traffic)
6. Uplink(PoE) Port: 2.5Gbps connection to 802.3at PoE.
 - Port LED: On (link), Blinking (traffic)
7. System LED Indicators:
 - 2.4G: On (radio on), Blinking (traffic)
 - 5G: On (radio on), Blinking (traffic)
 - Power/Status: On (power OK), Blinking (boot up)
8. Kensington lock slot

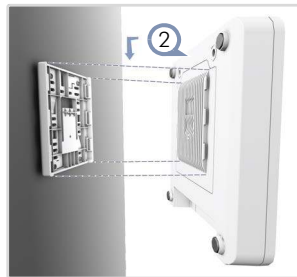
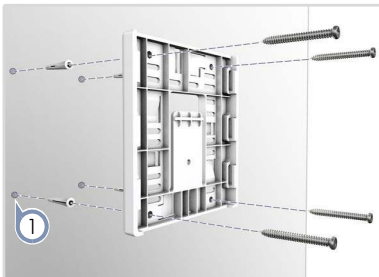
Installation



Warning: For indoor use only. The access point, AC power adapter, and all connected cables are not for outdoor use.

1 Mount the AP

a. Mounting on a Wall



1. At the installation location on the wall, use the mounting bracket to mark four holes for the wall plugs and screws (included in the screw kit).
Drill four holes for the wall plugs, and then insert the plugs and tap them flush with the wall surface.

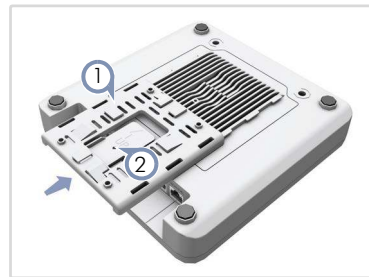


Note: Drill 2.5 mm (± 0.2 mm) holes for M3 self-tapping screws, or 4.5 mm (± 0.2 mm) holes for nylon wall plugs.

Use the four screws to secure the bracket to the wall.

2. With its ports facing down, place the AP over the bracket flanges and then slide it down until it snaps into its secured position.

b. Mounting on a Suspended Ceiling T-Bar

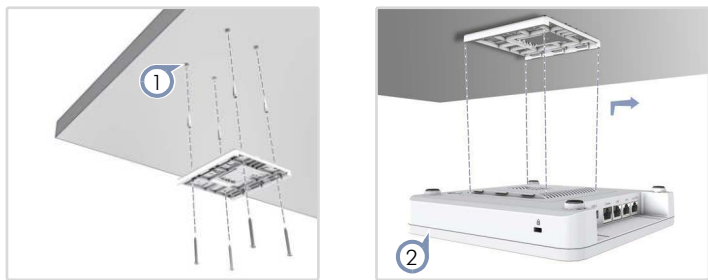


1. Slide the bracket accessory onto the base of the AP until it clicks into its locked position.
2. Use the included security screw to secure the bracket to the AP.
3. Position the ceiling-mount clip holders on either side of the T-bar, and then turn the AP until the two clips lock it to the T-bar.



Note: The AP mounting supports two different sizes of suspended ceiling T-bars. The position illustrated above is for 24.5 mm bars. Use the position at a 90 degrees angle for 15 mm bars.

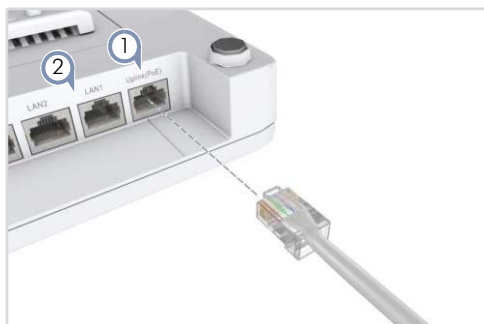
c. Mounting on a Ceiling Without T-Bars



1. At the installation location on the ceiling, use the mounting bracket to mark four holes for the plugs and screws (included in the screw kit).
Drill four holes for the plugs, and then insert the plugs and tap them flush with the ceiling surface.
Use the four screws to secure the bracket to the ceiling (screw torque must be less than 6 kgf.cm).
2. Place the AP over the bracket flanges and then slide it onto the bracket until it snaps into its secured position.

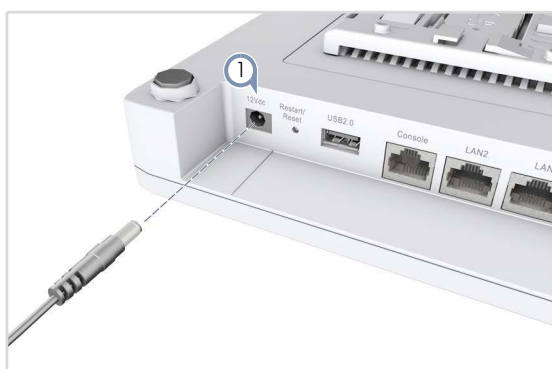
2 Connect Cables

g. Connect LAN Cables



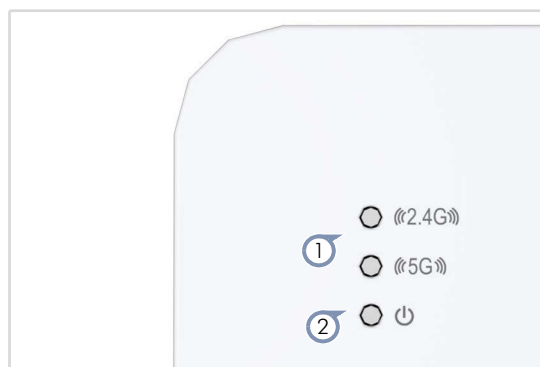
1. Connect Category 5e or better cable to the Uplink(PoE) 2.5G RJ-45 port. When connected to a PoE source, the Uplink(PoE) port connection provides power to the unit.
2. (Optional) Connect a local LAN switch or computer to the LAN1 or LAN2 1000BASE-T RJ-45 ports.

b. (Optional) Connect AC Power Adapter



1. When not connected to a PoE source, connect the AC power adapter to the DC power jack on the AP and then plug the adapter into a nearby AC power source.

3 Check AP LEDs



1. 2.4G and 5G LEDs — on green for radio enabled.
2. Power/Status LED — on green for normal operation.

4 Connect to Plume Cloud

The AP can be connected to Plume Cloud via the Plume mobile app and the EAP101 BLE function, or manually by adding the `NODE_ID` (the EAP101's serial number) into your Plume Cloud website when the AP is in the Plume Cloud inventory.

Safety and Regulatory Information

FCC Class B

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

Professional Installation Instructions

1. Installation personnel

This product is designed for specific applications and should be installed by qualified personnel who have knowledge of RF and its related regulations. A general user shall not attempt to install or modify the equipment configuration.

2. Installation location

To meet regulatory RF exposure requirements, this product shall be installed at a location where, during normal operations, the radiating antenna is at least 23 cm away from any nearby persons.

3. External antenna

Use only the antennas which have been approved by the applicant. Using non-approved antenna(s) is prohibited and may produce unwanted spurious or excessive RF transmitting power which may lead to a violation of FCC limits.

4. Installation procedure

Please refer to this equipment's user manual for the procedure details.

5. Warning

The installation position must be carefully selected so that the final output power does not exceed the limit set forth in relevant regulations. Violation of output power regulations could lead to serious federal penalties.

Industry Canada

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

(1) This device may not cause interference.

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Cet appareil contient des émetteurs / récepteurs exempts de licence qui sont conformes au (x) RSS (s) exemptés de licence d'Innovation, Sciences et Développement économique Canada. L'opération est soumise aux deux conditions suivantes:

(1) Cet appareil ne doit pas provoquer d'interférences.

(2) Cet appareil doit accepter toute interférence, y compris les interférences susceptibles de provoquer un fonctionnement indésirable de l'appareil.

The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

IMPORTANT NOTE:

IC Radiation Exposure Statement:

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 28 cm between the radiator & your body.

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 28 cm de distance entre la source de rayonnement et votre corps.

CE Statement

This equipment complies with EU radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 24 cm between the radiator and your body.

The device is restricted to indoor use only when operating in the 5150 to 5350 MHz frequency range.

All operational modes:

2.4 GHz: 802.11b, 802.11g, 802.11n (HT20), 802.11n (HT40), 802.11ac (VHT20), 802.11ac (VHT40), 802.11ax (HE20), 802.11ax (HE40)

5 GHz: 802.11a, 802.11n (HT20), 802.11n (HT40), 802.11ac (VHT20), 802.11ac (VHT40), 802.11ac (VHT80), 802.11ax (HE20), 802.11ax (HE40), 802.11ax (HE80)

BLE 2.4 GHz: 802.15.1

The frequency and maximum transmitted power limit in EU are listed as below:

2412-2472 MHz: 20 dBm

5150-5350 MHz: 23 dBm

5500-5700 MHz: 30 dBm



AT	BE	BG	CH	CY	CZ
DE	DK	EE	EL	ES	FI
FR	HR	HU	IE	IS	IT
LI	LT	LU	LV	MT	NL
NO	PL	PT	RO	SE	SI
SK	TR	UK			

The abbreviations of the countries, as prescribed in above table, where any restrictions on putting into service or any requirements for authorization of use exist.



CE Mark Declaration of Conformance for EMI and Safety (EEC)

This information technology equipment is in compliance with the Directive 2014/53/EU and Directive 2014/35/EU.

The Declaration of Conformity (DoC) can be obtained from www.edge-core.com -> support -> download.

Japan VCCI Statement

この装置は、クラスB機器です。この装置は、住宅環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。

VCCI — B

5 GHz band (W52, W53): Indoor use only

NCC Statement (Taiwan)

NCC 警語
取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前述合法通信，指依電信管理法規規定作業之無線電通信。低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

MPE
本產品電磁波曝露量 (MPE) 標準值 **1mW/cm2**，送測產品實測值為 **0.32982mW/cm2**，建議使用時至少距離人體 **24cm**。

Warnings and Cautionary Messages

Warning: This product does not contain any serviceable user parts.

Warning: Installation and removal of the unit must be carried out by qualified personnel only.

Caution: Wear an anti-static wrist strap or take other suitable measures to prevent electrostatic discharge when handling this equipment.

Caution: Do not plug a phone jack connector in the RJ-45 port. This may damage this device.

Caution: Use only twisted-pair cables with RJ-45 connectors that conform to FCC standards.

限用物質含有情況標示聲明書						
Declaration of the Presence Condition of the Restricted Substances Marking						
設備名稱：無線接收器			型號 (型式)：EAP101			
Equipment Name			Type Designation (Type)			
單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛 (Pb)	汞 (Hg)	鎘 (Cd)	六價鉻 (Cr ⁶⁺)	多溴聯苯 (PBB)	多溴二苯醚 (PBDE)
電路板組件 PCBA	—	○	○	○	○	○
機殼 Chassis	○	○	○	○	○	○
天線 Antenna	○	○	○	○	○	○
電源供應器 Power Supply	—	○	○	○	○	○
備 考 1. "超出 0.1 wt %" 及 "超出 0.01 wt %" 係指限用物質之百分比含量超出百分比含量基準值。						
Note 1: "Exceeding 0.1 wt %" and "exceeding 0.01 wt %" indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.						
備 考 2. "○" 係指該項限用物質之百分比含量未超出百分比含量基準值。						
Note 2: "○" indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.						
備 考 3. "—" 係指該項限用物質為排除項目。						
Note 3: The "—" indicates that the restricted substance corresponds to the exemption.						

Hardware Specifications

AP Chassis

Size (WxDxH)	195 x 195 x 39 mm (7.68 x 7.68 x 1.54 in.)
Weight	0.65 kg (1.435 lb)
Temperature	Operating: 0° C to 50° C (32° F to 122° F) Storage: -20° C to 60° C (-4° F to 140° F)
Humidity	Operating: 5% to 95% (non-condensing)

Network Interfaces

Ports	Uplink(PoE) RJ-45 Port: 2.5G, PoE PD LAN1 RJ-45 Port: 1000BASE-T LAN2 RJ-45 Port: 1000BASE-T
2.4 GHz Radio	IEEE 802.11b/g/n/ax
5 GHz Radio	IEEE 802.11a/c/n/ax
Bluetooth Radio	IEEE 802.15.1
Radio Frequencies	2.4–2.4835 GHz (US, Canada, ETSI, Japan, TW) 5.15–5.25 GHz (lower band) US/Canada, TW 5.725–5.825 GHz (upper band) US/Canada, TW Europe 5.15–5.25 GHz, 5.25–5.35, 5.47–5.725 GHz Japan 5.15–5.25 GHz, 5.25–5.35, 5.47–5.73 GHz

Power Specifications

PoE Input Power	22.4 W max, 48 VDC–55 VDC; 802.3at-compliant
AC Power Adapter	AC Input: 100–240 VAC, 50-60 Hz DC Output: 12 VDC, 2 A

Regulatory Compliances

Radio	EN300 328 V2.2.2 (2019-07) EN301 893 V2.1.1(2017-05) 47 CFR FCC Part 15.247 47 CFR FCC Part 15.407 IC RSS-247 Issue 2 and RSS-Gen Issue 5 NCC LP0002 Section 4.10.1 (2020-07-01) NCC LP0002 Section 5.7 (2020-07-01) MIC certification Rule, Article 2 Paragraph 1 Item 19 MIC certification Rule, Article 2 Paragraph 1 Item 19-3
Emissions	EN 301 489-1 V2.1.1 (2017-02) EN 301 489-17 V3.1.1 (2017-02) EN 55032:2015 AS/NZS CISPR 32:2015, Class B 47 CFR FCC Rules and Regulations Part 15 Subpart B, Class B Digital Device ICES-003, Issue 7 Class B CNS 13438 terminal equipment design certification, Article 3, Article 4, Article 6, Article 9 and Article 34 regulation
Safety	Low Voltage Directive IEC 62368-1:2014;and/or EN 62368-1:2014+A11:2017; and/or BS 62368-1:2014+A11:2017 CNS 14336-1 IEC/EN 62368-1, IEC/EN 60950-1
Taiwan RoHS	CNS 15663



FEATURES

MULTI-SITE & MULTI-CLOUD SUPPORT

- Multiple sites can be created within one cloud account
- Each site has its own distinct set of configurations, users, maps, and other properties
- Cloud users' logins can be associated with any number of clouds and can have different roles in each cloud

SECURE, ROBUST ARCHITECTURE

- Encrypted device-to-cloud communication
- Data is secure and always kept private
- Scalability: Register up to 500 sites per cloud and 500 devices per site

ADMINISTRATION PRIVILEGES

- Administrator/Owner Role: Full control of a cloud and its sites
- Manager: Full write access to specified sites
- Guest: Read-only access to specified sites

POWERFUL, FLEXIBLE CONFIGURATION

- Bulk (site-level) and individual (device-level) configuration options
- Fallback for upgrade reliability
- Two-way synchronization between local web GUI and cloud

DEVICE REGISTRATION & LICENSING

- Simple and intuitive registration
- All licenses are floating and not tied to specific devices

REMOTE FIRMWARE UPGRADE

- Upgrade multiple devices at one time
- Schedulable firmware upgrades
- Rolling upgrade option ensures most parts of the network are online at any given time
- Dual flash increases firmware upgrade reliability

WIRED & WIRELESS DEVICE INTEGRATION

- Automatically synchronize VLAN settings
- Port security on managed switches

BUILT-IN AAA SERVICE

- Built-in account database for authentication
- Time- and/or volume-based service plan for account creation
- Supports both UAM and 802.1X (WPA-EAP, WPA2-EAP) authentication
- Authenticated users can roam between APs
- SSID-based customizable captive portal
- Built-in captive portal editor

LIVE STATISTICS & INTERACTION

- Live data on the device dashboard comes directly from the device over a near real-time connection
- View data straight from the device:
 - Throughput rate per interface
 - Power consumption
 - CPU utilization & memory usage
 - System temperature
 - Client counts
 - Uptime
 - Load
 - Channel utilization
- Interact directly with your device:
 - Reboot the device with the click of a button
 - Blink LEDs for location-finding purposes
 - Initiate a remote packet capture

HISTORICAL STATISTICS

- Throughput rates per interface
- Client count per wireless interface (SSID) over time
- Channel utilization per wireless radio over time
- Current networking status and traffic details
- Client session information
- Historical data can be stored for two weeks or more, depending on the license type

ALERTS & MONITORING

- Email alerts are generated when devices go offline or require your attention

AUDIT TRAIL

- All changes made to the cloud are recorded in a system activity log

SUPPORTED DEVICES

WI-FI ACCESS POINTS

- EAP101*1
- EAP102*1
- EAP104*1
- EAP104 Lite
- EAP111
- EAP111e
- ECW5211-L*1
- ECW5410-L*1
- OAP100*1
- OAP100e
- OAP101
- SP-W2-AC1200(L)*1
- SS-W2-AC2600
- SP-W2M-AC1200
- SP-W2M-AC1200-POE
- SS-N300
- GW-AC1200
- SP-AC750

METROLINQ 60GHZ

- ML1-60 PTP
- ML2.5-60 PTP
- ML2.5-60 PTMP
- ML2.5-60-BF
- ML-60-LW
- ML-60-10G-360

TERRAGRAPH CERTIFIED PRODUCT

- MLTG-360
- MLTG-CN
- MLTG-CN LR

SD-WAN GATEWAY

- SDW-102

SWITCHES

- ECS1100-5P
- ECS1100-10HP
- ECS1100-28HP
- ECS2100-10T
- ECS2100-10P
- ECS2100-28T
- ECS2100-28P
- ECS2100-28PP
- ECS2100-52T
- ECS4100-12T
- ECS4100-12PH
- ECS4100-28T
- ECS4100-28P
- ECS4100-52T
- ECS4100-52P
- ECS4120-28T
- ECS4120-52T
- ECS4120-28Fv2
- ECS4120-28Fv2-I
- ECS4125-10P
- ECS4150-28P
- ECS4150-28T
- ECS4150-54P
- ECS4150-54T

NOTES:

*1: Support Built-in AAA Service



Private VLANs (traffic segmentation per port) isolate edge ports to ensure user privacy.

DAI (Dynamic ARP Inspection) is a security feature that validates Address Resolution Protocol (ARP) packets in a network. DAI allows a network administrator to intercept, log, and discard ARP packets with invalid MAC-to-IP address bindings.

Secure Shell (SSH) and Secure Sockets Layer (SSL/HTTPS) encrypt Telnet and web access to the switch, providing secure network management.

The ECS4125-10P also supports both RADIUS and TACACS+ authentication methods to secure your network.

Comprehensive QoS

The ECS4125-10P offers advanced QoS for marking, classification, and scheduling to deliver best-in-class performance for data, voice, and video traffic at wire speed. Eight egress queues per port enable differentiated management of up to eight traffic types through the switch.

Traffic is prioritized according to 802.1p and DSCP to provide optimal performance for real-time applications. Weighted Round Robin (WRR) and strict priority ensure differential prioritization of packet flows and avoid congestion of ingress and egress queues. Asymmetric bidirectional rate-limiting, per port or per traffic class, preserves network bandwidth and allows maximum control of network resources.

Robust Multicast Control

IGMP snooping prevents the flooding of multicast traffic by dynamically configuring switch ports so that multicast traffic is forwarded to only those ports associated with an IP multicast receiver. IGMP increases the performance of networks by reducing multicast traffic flooding.

IGMP groups allow you to create customer packages for IP-TV channels, making switch configuration easy. IGMP Filtering prevents subscribers seeing unsubscribed IP-TV channels. And, IGMP Throttling allows you to set how many IP-TV channels a subscriber can receive simultaneously.

Multicast VLANs are shared in the network, while subscribers remain in separate VLANs. This increases network security and saves bandwidth on core links. Multicast streams do not have to be routed in core L3 switches, which saves CPU power.

Multicast VLAN Registration (MVR) is designed for applications such as Media-on-Demand that send multicast traffic across an Ethernet network.

IPv6 Support

The switch supports a number of IPv6 features, including IPv6 Management, DHCPv6 Snooping with Option 37, IPv6 Source Guard, and MVR6.

Superior Management

An industry-standard command-line interface (CLI), accessed through the console port or Telnet/SSH, provides a familiar user interface and command set for users to manage the switch.

An embedded user-friendly web interface helps users to quickly and simply configure switches.

The ECS4125-10P supports SNMPv1,2c,3 and four-group RMON. The switch provides a complete private MIB for the configuration of most functions via the SNMP protocol.

Administrators can backup and restore firmware and configuration files via TFTP or FTP. The switch also provides the configuration of auto-provision for ease of use in large deployments.

AAA (Authentication, Authorization and Accounting) via RADIUS, TACACS+, enables centralized control of the switches. Access rights can be authorized per user and account for all actions performed by administrators.

Service Monitoring and Management

The ECS4125-10P supports IEEE 802.1ag and ITU-T Y.1731, allowing service providers to monitor end-to-end services, identify connectivity and performance issues, and isolate problems from a remote location without dispatching an engineer onsite.

The switch also provides the capability to monitor service availability, delay, jitter, and dropped packets for verifying SLA conformance (for billing purposes) and providing advance indication of performance degradation before a service outage occurs.

Virtual Private Networks

The ECS4125-10P supports Layer 2 VPNs by using Q-in-Q functions, where an 802.1Q tag from a customer VLAN (called CE-VLAN ID) is encapsulated in a second 802.1Q tag from a service-provider network (called an SP-VLAN ID). The switch supports rewriting the VLAN tag of egress traffic when the ingress traffic is tagged.

The switch also supports Layer 2 Protocol Tunneling for STP, CDP, VTP, PVST+, with Cisco-proprietary multicast address (01-00-0c-cd-cd-d0) replacement.

Reliability and Energy Efficiency

The design of the ECS4125-10P incorporates high energy efficiency in order to reduce the impact on the environment. The Green Ethernet power-saving features and fan-less design significantly reduce the power consumption.

Product Model		ECS4125-10P
Product Image		
Port	RJ-45 2.5G/1000M Ports	8
	100/1000 SFP Ports	0
	10/100/1000 Combo Ports	0
	SFP+ 10 Gigabit Uplink Ports	2
	RJ-45 Console Port	1
Performance	Switching Capacity	80 Gpbs
	Forwarding Rate	59.52 Mpps
	Flash Memory	64 MB
	DRAM	1 GB
	MAC Address Table Size	16 K
	Jumbo Frames	12 KB
	Auto-negotiation, Auto-MDI/MDIX	Yes
PoE	PoE ports	8
	PoE++ based on IEEE 802.3bt (60 W)	Yes
	PoE+ based on IEEE 802.3at/ 802.3af	Yes
	Auto disable after exceeding power budget	Yes
	Dynamic Power Allocation	Yes
	PoE Power Budget	240 W
Mechanical	Dimension (W x D x H) cm	33.0 x 20.8 x 4.4
	Weight	2.41 kg (5.31 lb)
Power Supply	100-240 VAC, 50-60 Hz	Yes
	Max System Power Consumption (Watts)	20 W (w/o PoE)
Environmental	Operating Temperature	0°C to 50°C
	Storage Temperature	-40°C to 70°C
	Operating Humidity (non-condensing)	10% to 90%
	Storage Humidity (non-condensing)	10% to 90%
	Environmental Regulation Compliance: WEEE	Yes
	Environmental Regulation Compliance: RoHS	Yes
Certification	FCC Class A	Yes
	CE	Yes
	Safety Compliance: CB	Yes
	Safety Compliance: UL	Yes
ecCLOUD Management		Supported

L2 Features

- 2.5G BASE-T copper interfaces
- Auto-negotiation for port speed and duplex mode
- Auto MDI/MDI-X
- Dual-speed (1G and 10G) fiber interfaces
- SFP+ Ports Support:
 - IEEE 802.3ae changeable (10GBASE-SR/LR)
 - IEEE 802.3z (1000BASE-SX/LX) transceivers, and 10G DAC/AOC
- Digital Diagnostic Monitoring (DDM) on 10G SFP+ port
- Flow Control:
 - IEEE 802.3x for full duplex mode
 - Back-Pressure for half duplex mode
- Jumbo frames 12KB
- Broadcast/Multicast/ Unknown Unicast Storm Control
- Spanning Tree Protocol:
 - IEEE 802.1D Spanning Tree Protocol (STP)
 - IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
 - IEEE 802.1s Multiple Spanning Tree Protocol (MSTP), 64 instances
 - BPDU Guard
 - BPDU filtering
 - Root Guard
 - BPDU transparent
 - Loopback detection
- Non-Spanning Tree Loopback detection
- ITU-T G.8032 Ethernet Ring Protection:
 - Sub 50 msec convergence
 - Revertive operation mode
 - Multiple-ring network
- VLANs:
 - Supports 4K VLAN
 - Port-based VLAN
 - IEEE 802.1Q VLAN
 - GVRP
 - IEEE 802.1v Protocol-based VLAN
 - IP Subnet-based VLAN
 - MAC-based VLAN
 - Traffic Segmentation
- L2 Virtual Private VLAN:
 - Q-in-Q
 - L2 Protocol tunneling (xSTP, CDP, VTP and PVST+, LLDP)
 - CDP/PVST+ Filtering
 - Selective Q-in-Q
- Link Aggregation:
 - Static Trunk
 - IEEE 802.3ad Link Aggregation Control Protocol
 - Trunk Groups: 16, up to 8 GE/4 10G ports per group
 - Load Balancing: SA+DA, SA, DA, SIP+DIP, SIP, DIP
- IGMP Snooping:
 - IGMP v1/v2/v3 snooping
 - IGMP Proxy reporting
 - IGMP Filtering
 - IGMP Throttling
 - IGMP Immediate Leave
 - IGMP Querier
- MVR (Multicast VLAN Registration): Supports 5 multicast VLANs
- Port mirroring
- Remote port mirror (RSPAN)

QoS Features

- Priority Queues: 8 hardware queues per port
- Traffic classification:
 - IEEE 802.1p CoS
 - IP Precedence
 - DSCP
 - MAC Access control list (Source/Destination MAC, Ether type, Priority ID/VLAN ID)
 - IP standard access control list (Source IP)
 - IP extended access control list (Source/Destination IP, Protocol, TCP/UDP port number)
- Traffic Scheduling:
 - Strict Priority
 - Weighted Round Robin
 - Strict + WRR
- Ingress policy map (police rate, remark CoS)
- Egress policy map (police rate, remark CoS/DSCP)
- Rate Limiting (Ingress and Egress, per port base)
 - GE: Resolution 64 Kbps ~ 1,000 Mbps
 - 10G: Resolution 64 Kbps ~ 10,000 Mbps
- Auto Traffic Control

Security

- Port security
- IEEE 802.1X port based and MAC based authentication
- Dynamic VLAN Assignment, Auto QoS
- MAC authentication
- Web authentication
- Voice VLAN
- Guest VLAN
- L2/L3/L4 Access Control List:
 - MAC Access control list (Source/Destination MAC, Ether type, Priority ID/VLAN ID)
 - IP standard access control list (Source IP)
 - IP extended access control list (Source/Destination IP, Protocol, TCP/UDP port number)
- IPv6 ACL
- DHCP Snooping
- DHCP Option 82
- DHCP Option 82 Relay
- IP Source Guard
- PPPoE IA
- Dynamic ARP Inspection
- Denial of Service
- Login Security
- RADIUS authentication
- RADIUS accounting
- TACACS + authentication
- TACACS + accounting
- TACACS + authorization
- Management Interface Access Filtering (SNMP, Web, Telnet)
- SSH (v1.5/v2.0) for secure Telnet
- SSL for HTTPS
- SNMPv3

Green Ethernet

- IEEE 802.3az Energy-Efficient Ethernet (EEE)

IPv6 Features

- IPv4/IPv6 Dual Protocol stack
- IPv6 Address Types Stack: Unicast
- IPv6 Neighbor Discovery:
 - Duplicate address
 - Address resolution
 - Unreachable neighbor detection
- Stateless auto-configuration
- Manual configuration
- Remote IPv6 ping
- IPv6 Telnet support
- HTTP over IPv6
- SNMP over IPv6
- IPv6 Syslog support
- IPv6 TFTP support
- MLD Snooping v1/v2
- IPv6 source guard
- DHCPv6 snooping
- MVR6

Management

- Switch Management:
 - CLI via console port or Telnet/SSH
 - Web management
 - SNMP v1, v2c, v3
- Firmware and Configuration:
 - Firmware upgrade via TFTP/HTTP/FTP/SFTP server
 - Multiple configuration files
 - Configuration file upload/download via TFTP/HTTP/FTP/SFTP server
- RMON (groups 1, 2, 3 and 9)
- BOOTP, DHCP client for IP address assignment
- DHCP dynamic provision option 66,67
- SNTP
- Syslog (local flash)
- Remotelog (RFC3164)
- SMTP (E-mail Notification)
- Support LLDP (802.1ab)
- sFlow v4, v5

Routing

- IPv4 Static Route/RIP

Safety

- UL (CSA 22.2. NO 60950-1 and UL60950-1)
- CB (IEC60950-1)

Power Supply

- Power input
100 to 240 VAC, 50/60 Hz, 1.0A

Electromagnetic Compatibility

- CE Mark
- FCC Class A
- CISPR Class A
- BSMI

Environmental Specifications

- Temperature:
 - 0°C to 50°C standard operation
 - 40°C to 70°C (Non-Operating)
- Humidity: 10% to 90% (Non-condensing)

Warranty

Please check www.edge-core.com for the warranty terms in your country.

For More Information

To find out more about Edgecore Networks Corporation products and solutions, visit www.edge-core.com.

About Edgecore Networks Corporation

Edgecore Networks Corporation is in the business of providing innovative network solutions. In the service provider network, in the data center or in the cloud, Edgecore Networks Corporation delivers the software and systems that transform the way the world connects. Edgecore Networks Corporation serves customers and partners worldwide. Additional information can be found at www.edge-core.com.

Edgecore Networks Corporation is a subsidiary of Accton Technology Corporation, the leading network ODM company. The Edgecore data center switches are developed and manufactured by Accton.

To purchase Edgecore Networks solutions, please contact your Edgecore Networks Corporation representatives at +886 3 563 8888 (HQ) or +1 (949)-336-6801 or authorized resellers.

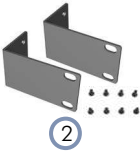
© Copyright 2022 Edgecore Networks Corporation. The information contained herein is subject to change without notice. This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered by Edgecore Networks Corporation. Edgecore Networks Corporation shall not be liable for technical or editorial errors or omissions contained herein.

Ordering Information

Optional Accessories	Product Description
ET4202-SX	1Gbps, (Distance: 500 m; Wavelength: 850 nm, DDM)
ET4202-LX	1Gbps, (Distance: 10 km; Wavelength: 1310 nm, DDM)
ET4202-EX	1Gbps, (Distance: 40 km; Wavelength: 1310 nm, DDM)
ET4202-ZX	1Gbps, (Distance: 80 km; Wavelength: 1550 nm, DDM)
ET4202-RJ45	1Gbps , (Distance:100 m)
ET5402-SR	10Gbps, (Distance: 3000 m; Wavelength: 850 nm, DDM)
ET5402-LR	10Gbps, (Distance: 10 km; Wavelength: 1310 nm, DDM)
ET5402-ER	10Gbps, (Distance: 40 km; Wavelength: 1550 nm, DDM)
ET5402-ZR	10Gbps, (Distance: 80 km; Wavelength: 1550 nm, DDM)
ET5402-DAC-xM	10G to 10G DAC cable,10G SFP+ DAC cable, 1-5 m
ET5402-AOC-xM	10G to 10G AOC cable,10G SFP+ AOC cable, 5-100 m
ecCLOUD Network Management Software	

• Note: More optics and detailed cabling information can be found at www.edge-core.com.

Package Contents

- 
1. ECS4125-10P or ECS4125-10T Switch

2. Rack mounting kit—2 brackets and 8 screws

3. Power cord

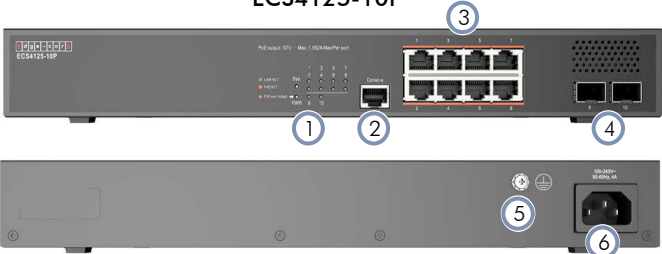
4. Four adhesive rubber feet

5. Console cable—RJ-45 to DE-9

6. QR code label (affixed to the top of the switch)

Overview

- ECS4125-10P



1. System LEDs

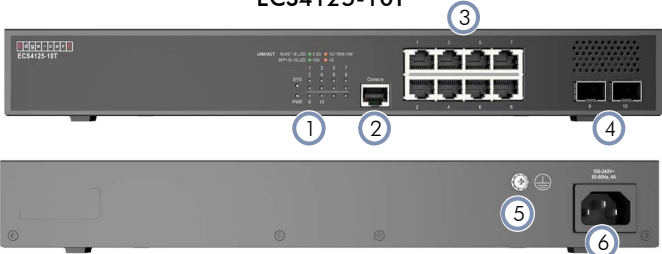
2. Console port

3. 8 x 10/100/1G/2.5G RJ-45 PoE ports

4. 2 x 1/10G SFP+ ports

5. Ground screw

6. AC power socket
- ECS4125-10T



1. System LEDs

2. Console port

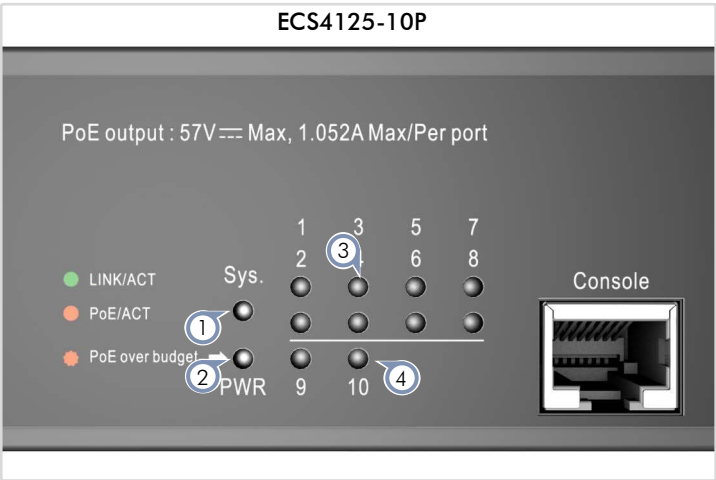
3. 8 x 10/100/1G/2.5G RJ-45 ports

4. 2 x 1/10G SFP+ ports

5. Ground screw

6. AC power socket

System/Port LEDs

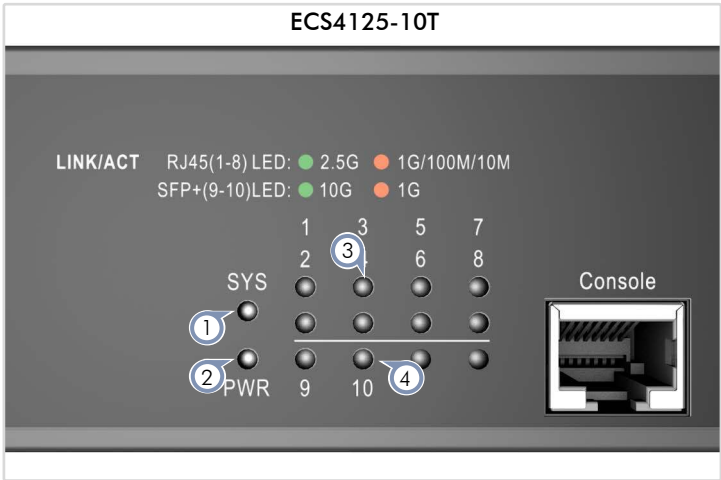


1. Sys: Green (OK), Blinking Green (booting), Orange (fault)

2. PWR: Green (OK), Orange (maximum PoE budget)

3. RJ-45 Ports: Green/Blinking (link/activity), Orange (PoE link)

4. SFP+ Ports: Green (10G), Orange (1G)



1. SYS: Green (OK), Blinking Green (booting), Orange (fault)

2. PWR: Green (OK)

3. RJ-45 Ports: Green (2.5G), Orange (1G/100M/10M)

4. SFP+ Ports: Green (10G), Orange (1G)



Installation



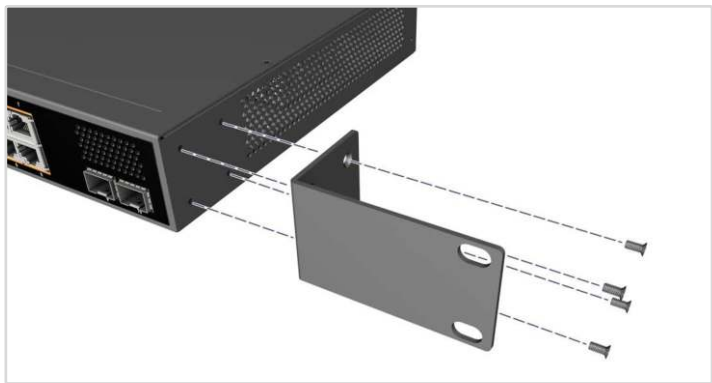
Warning: For a safe and reliable installation, use only the accessories and screws provided with the device. Use of other accessories and screws could result in damage to the unit. Any damages incurred by using unapproved accessories are not covered by the warranty.

Avertissement: Pour une installation sûre et fiable, utilisez uniquement les accessoires et les vis fournies avec l'appareil. L'utilisation d'autres accessoires et vis pourrait endommager l'appareil. Les dommages causés par l'utilisation d'accessoires non approuvés ne sont pas couverts par la garantie.



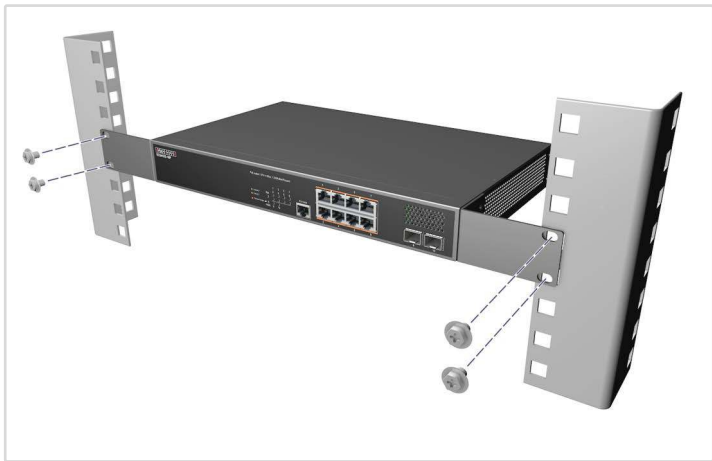
Note: The drawings in this document are for illustration only and may not match your particular model.

1 Mount the Device



1. Attach the Brackets

Use the included screws to attach the brackets.



2. Mount the Device

Mount the device in the rack and secure it with rack screws.



Note: The device can also be installed on a desktop or shelf using the included adhesive rubber feet.

2 Ground the Device



Attach a lug (not provided) to a #18 AWG minimum grounding wire (not provided), and connect it to the grounding point on the rear panel. Then connect the other end of the wire to rack ground.

3 Connect Power



Connect an AC power source to the device.

4 Make Network Connections



RJ-45 PoE Ports

Connect Cat. 5e or better twisted-pair cable.

SFP+ Ports

Install transceivers and then connect fiber optic cabling to the transceiver ports. The following transceivers are supported:

- 1000BASE-SX/LX/EX/ZX and 1000BASE-T (RJ-45)
- 10GBASE-SR/LR/ER/ZR

5 Make Management Connections



RJ-45 Console Port

Connect the included console cable and then configure the serial connection: 115200 bps, 8 characters, no parity, one stop bit, 8 data bits, and no flow control.

Hardware Specifications

Size (WxDxH)	330 x 207.9 x 47.3 mm (12.99 x 8.19 x 1.86 in.)
Weight	ECS4125-10P: 2.41 kg (5.31 lb) ECS4125-10T: 1.98 kg (4.36 lb)
Temperature	Operating: 0° C to 50° C (32° F to 122° F) Storage: -40° C to 70° C (-40° F to 158° F)
Humidity	Operating: 10% to 90% (non-condensing)
Power Consumption	ECS4125-10P: 370 Watts maximum ECS4125-10T: 36 Watts maximum
PoE Budget (ECS4125-10P)	240 Watts
Input Power Rating	ECS4125-10P: 100-240 VAC, 50-60Hz, 4 A ECS4125-10T: 100-240 VAC, 50-60Hz, 0.9 A

Regulatory Compliances

Emissions	EN 55032:2015/A1:2020 EN IEC 61000-3-2:2019/A1:2021 EN 61000-3-3:2013/A2:2021 FCC Class A VCCI-CISPR 32:2016 Class A BSMI (CNS 15936)
Immunity	IEC 61000-4-2/3/4/5/6/8/11 EN 55035:2017/A11:2020
Safety	UL (CSA 22.2 No 62368-1 & UL62368-1) CB (IEC/EN 62368-1) BSMI (CNS 15598-1)
Taiwan RoHS	CNS 15663

This unit cannot be powered from IT† supplies. If your supplies are of IT type, this unit must be powered by 230 V (2P+T) via an isolation transformer ratio 1:1, with the secondary connection point labeled Neutral, connected directly to earth (ground).

† Impédance à la terre

Important! Before making connections, make sure you have the correct cord set. Check it (read the label on the cable) against the following:

Power Cord Set	
U.S.A. and Canada	The cord set must be UL-approved and CSA certified. The minimum specifications for the flexible cord are: - Min. 1.5 m and Max. 4.5 m long, Type SJE, SJT, ST or SJTO, No. 18 AWG. - Min. 1.5 m and Max. 2.4 m long, Type SVT or SPT-2, No. 18 AWG - 3-conductor The cord set must have a rated current capacity of at least 10 A. The attachment plug must be an earth-grounding type with NEMA 5-15P (10 A, 125 V) configuration.
Denmark	The supply plug must comply with Section 107-2-D1, Standard DK2-1a or DK2-5a.
Switzerland	The supply plug must comply with SEV/ASE 1011.
U.K.	The supply plug must comply with BS1363 (3-pin 13 A) and be fitted with a 5 A fuse which complies with BS1362. The mains cord must comply with IEC 60227 (designation 60227 IEC 52).
Europe	The supply plug must comply with CEE7/7 ("SCHUKO"). The mains cord must comply with IEC 60227 (designation 60227 IEC 52). IEC-320 receptacle.

电源线安全

安装设备前，请仔细阅读以下安全信息。

警告：安装或拆卸本装置时，必须由合格的人员进行操作。

- 必须将本装置连接至接地插座，以符合国际安全标准。
- 切勿将本装置连接至未接地的 AC 插座（电源）。
- 电器耦合器（指的是插入装置的连接器，而非壁式插座）必须与 EN 60320/IEC 320 电器插座相匹配。
- 插座应位于装置附近易于连接的位置。只能透过从插座上断开电源线来断开装置电源。
- 本装置在 IEC 60950 的 SELV（安全特低电压）条件下进行运转。设备的连接方也必须在 SELV 条件下运转，否则无法保持该条件。

仅适用于法国和秘鲁

本装置无法透过 IT 供电系统进行供电。如使用 IT 供电系统，本装置必须使用绝缘变压器率为 1:1 的 230 V（2P+T）进行供电，且辅助连接点必须标记为中性并直接接地。

† Impédance à la terre

重要！ 连接前，请确保使用的缆线组件正确无误。检查（查看缆线的标签）是否符合以下项目：

电源线组件	
美國和加拿大	缆线组件必须经过 UL 认可和 CSA 认证。 软线的最低规格配置必须满足以下： - 最短 1.5 米，最长 4.5 米的 18 号 AWG 缆线，SJE, SJT, ST 或 SJTO 类型。 - 最短 1.5 米，最长 2.4 米的 18 号 AWG 缆线，SVT 或 SPT-2 类型。 - 3 导线。 缆线组件的额定电流容量不得低于 10 A。 附件插头必须是带有 NEMA 5-15P（10 A, 125 V）置的接地类型。
丹麦	电源插头必须符合 DK2-1a 或 DK2-5a 标准的第 107-2-D1 部分。
瑞士	电源插头必须符合 SEV/ASE 1011。
英国	电源插头必须符合 BS1363（3 针 13 A），且装有符合 BS1362 的 5 A 保险丝。 主缆线必须符合 IEC 60227（规定 60227 IEC 52）。
欧洲	电源插头必须符合 CEE7/7（"SCHUKO"）。 主缆线必须符合 IEC 60227（规定 60227 IEC 52）。 IEC-320 插座。

Veuillez lire à fond l'information de la sécurité suivante avant d'installer l'appareil:

Avertissement: L'installation et la dépose de ce groupe doivent être confiés à un personnel qualifié.

- Ne branchez pas votre appareil sur une prise secteur (alimentation électrique) lorsqu'il n'y a pas de connexion de mise à la terre (mise à la masse).
- Vous devez raccorder ce groupe à une sortie mise à la terre (mise à la masse) afin de respecter les normes internationales de sécurité.
- Le coupleur d'appareil (le connecteur du groupe et non pas la prise murale) doit respecter une configuration qui permet un branchement sur une entrée d'appareil EN 60320/IEC 320.
- La prise secteur doit se trouver à proximité de l'appareil et son accès doit être facile. Vous ne pouvez mettre l'appareil hors circuit qu'en débranchant son cordon électrique au niveau de cette prise.
- L'appareil fonctionne à une tension extrêmement basse de sécurité qui est conforme à la norme IEC 60950. Ces conditions ne sont maintenues que si l'équipement auquel il est raccordé fonctionne dans les mêmes conditions.

France et Pérou uniquement:

Ce groupe ne peut pas être alimenté par un dispositif à impédance à la terre. Si vos alimentations sont du type impédance à la terre, ce groupe doit être alimenté par une tension de 230 V (2 P+T) par le biais d'un transformateur d'isolement à rapport 1:1, avec un point secondaire de connexion portant l'appellation Neutre et avec raccordement direct à la terre (masse).

Cordon électrique - Il doit être agréé dans le pays d'utilisation

Etats-Unis et Canada:	Le cordon doit avoir reçu l'homologation des UL et un certificat de la CSA. Les spécifications minimales pour un câble flexible sont: - Câble No. 18 AWG, Min. 1,5 mètre et Max. 4,5 mètres de long, Type SJE, SJT, ST ou SJTO. - Câble No. 18 AWG, Min. 1,5 mètre et Max. 2,4 mètres de long, Type SVT ou SPT-2. - 3 conducteurs. Le cordon doit être en mesure d'acheminer un courant nominal d'au moins 10 A. La prise femelle de branchement doit être du type à mise à la terre (mise à la masse) et respecter la configuration NEMA 5-15P (10 A, 125 V).
Danemark:	La prise mâle d'alimentation doit respecter la section 107-2 D1 de la norme DK2 1a ou DK2 5a.
Suisse:	La prise mâle d'alimentation doit respecter la norme SEV/ASE 1011.
Europe	La prise secteur doit être conforme aux normes CEE 7/7 ("SCHUKO") Le cordon d'alimentation doit être conforme à la norme IEC 60227 (IEC 60227 désignation 52)

Warnings and Cautionary Messages

Warning: This product does not contain any serviceable user parts.

Warning: Installation and removal of the unit must be carried out by qualified personnel only.

Warning: When connecting this device to a power outlet, connect the field ground lead on the tri-pole power plug to a valid earth ground line to prevent electrical hazards.

Warning: This device uses lasers to transmit signals over fiber optic cable. The lasers are compliant with the requirements of a Class 1 Laser Product and are inherently eye safe in normal operation. However, you should never look directly at a transmit port when it is powered on.

Warning: When selecting a fiber SFP+ device, considering safety, please make sure that it can function at a temperature that is not less than the recommended maximum operational temperature of the product. You must also use an approved Laser Class 1 SFP+ transceiver.



Caution: Wear an anti-static wrist strap or take other suitable measures to prevent electrostatic discharge when handling this equipment.

Caution: Do not plug a phone jack connector in the RJ-45 port. This may damage this device.

Caution: Use only twisted-pair cables with RJ-45 connectors that conform to FCC standards.



Avertissement: Ce produit ne contient aucun composant susceptible d'être réparé par l'utilisateur.

Avertissement: L'installation et la dépose de l'unité ne doivent être réalisées que par du personnel qualifié.

Avertissement: Lorsque vous branchez cet appareil sur une prise électrique, la terre de la fiche à trois pôles doit être branchée sur une ligne mise à la terre pour écarter tout danger électrique.

Avertissement: Cet appareil utilise des lasers pour transmettre des signaux via un câble de fibre optique. Ces lasers répondent aux exigences des produits laser de classe 1 et sont sans danger intrinsèque pour les yeux, sous réserve de leur utilisation normale. Vous ne devez cependant jamais regarder directement un port de transmission lorsque ce dernier est sous tension.

Avertissement: Lorsque vous utilisez un dispositif fibre de type SFP+, en ce qui concerne la sécurité, assurez-vous qu'il puisse fonctionner à une température inférieure à la température maximale de fonctionnement recommandée du produit. Utilisez également un émetteur-récepteur laser SFP+ de classe 1 agréé.



Attention: La manipulation de cet équipement requiert le port d'un bracelet antistatique ou l'utilisation d'autres mesures pour éviter toute décharge électrostatique.

Attention: Ne branchez pas un connecteur téléphonique dans le port RJ-45. Vous risqueriez d'endommager l'appareil.

Attention: Ne branchez que des fils torsadés par paires conformes aux normes FCC sur les connecteurs RJ-45.

警告和警示消息

警告: 此产品不含任何用户可维修的部件。

警告: 本机的安装和拆卸必须由专业人士来完成。

警告: 在将此设备连接到电源插座时, 将三插片电源插头上的接地导线连接到有效的接地线路, 以防止电气危险。

警告: 此设备使用激光器通过光纤线缆发射信号。这些激光器符合 1 类激光产品的要求, 在正常使用情况下对眼睛无害。但是, 切勿在电源开启状态下直接注视发射端口。

警告: 在选择光纤 SFP+ 设备时, 为安全起见, 请确保其可以在不低于为产品建议的最大工作温度下工作。此外, 还必须使用经过认可的激光 1 类 SFP+ 收发器。



小心: 为防止静电释放, 在操作此设备时, 应戴上防静电腕带或采取其他必要措施。

小心: 请勿将电话插头插入 RJ-45 端口。否则, 可能损坏此设备。

小心: 只应使用符合 FCC 标准且带有 RJ-45 接头的双绞线。

CQC (China)

警告: 在居住环境中, 运行此设备可能会造成无线电干扰。

BSMI (Taiwan)

警告: 為避免電磁干擾, 本產品不應安裝或使用於住宅環境。

電氣方面的安全性

- 為避免可能的電擊造成嚴重損害, 在搬動產品之前, 請先將產品電源線暫時從電源插座中拔掉。
- 當您要加入硬體裝置到系統中或者要移除系統中的硬體裝置時, 請務必先連接該裝置的訊號線, 然後再連接電源線。可能的話, 在安裝硬體裝置之前先拔掉產品的電源供應器電源線。
- 當您要從主機板連接或拔除任何的訊號線之前, 請確定所有電源線已事先拔掉。
- 請確定電源供應器的電壓設定已調到本國 / 本區域所使用的電壓標準值。若您不確定您所屬區域的供應電壓值為何, 那麼請就近詢問當地的電力公司人員。
- 如果電源供應器已損壞, 請不要嘗試自行修復。請將之交給專業技術服務人員或經銷商來處理。

操作方面的安全性

- 在使用產品之前, 請確定所有的排線、電源線都已正確地連接好。若您發現有重大的瑕疵, 請盡速連絡您的經銷商。
- 為避免發生電氣短路情形, 請務必將所有沒用到的螺絲、迴紋針及其他零件收好, 不要遺留在主機板上或產品主機中。
- 灰塵、溼氣以及劇烈的溫度變化都會影響主機板的使用壽命, 因此請盡量避免放置在這些地方。
- 請勿將產品主機放置在容易搖晃的地方。
- 若在本產品的使用上有任何的技術性問題, 請和經過檢定或有經驗的技術人員聯絡。

使用注意事項

- 在您開始操作本系統之前, 請務必詳閱以下注意事項, 以避免因為人為的疏失造成系統損傷甚至人體本身的安全。
- 使用前, 請檢查產品各部份組件是否正常, 以及電源線是否有任破損, 或是連接不正確的情形發生。

- 如果有任何破損情形，請盡速與您的授權經銷商連絡，更換良好的線路。
- 產品放置的位置請遠離灰塵過多，溫度過高，太陽直射的地方。
- 保持機器在乾燥的環境下使用，雨水、溼氣、液體等含有礦物質將會腐蝕電子線路。
- 使用時，請務必保持周遭散熱空間，以利散熱。
- 使用前，請檢查各項周邊設備是否都已經連接妥當再開機。
- 避免邊吃東西邊使用，以免污染機件造成故障。
- 請避免讓紙張碎片、螺絲及線頭等小東西靠近產品之連接器、插槽、孔位等處，避免短路及接觸不良等情況發生。
- 請勿將任何物品塞入產品內，以避免引起機件短路或電路損毀。
- 產品開機一段時間之後，散熱片及部份IC表面可能會發熱、發燙，請勿用手觸摸，並請檢查系統是否散熱不良。
- 在安裝或移除周邊產品時請先關閉電源。
- 電源供應器如果發生損壞，切勿自行修理，請交由授權經銷商處理。
- 產品的機殼、鐵片大部份都經過防割傷處理，但是您仍必須注意避免被某些細部鐵片尖端及邊緣割傷，拆裝機殼時最好能夠戴上手套。

報驗義務人:

公司名稱: 鈺登科技股份有限公司

公司地址: 新竹市科學工業園區研新三路1號

電話: 886-3-5770270

产品内含危害物质揭露表 Products contain hazardous substances exposing table						
零部件名称 Component Name	危害物质项目 Hazardous Substances Project					
	铅 (Pb)	镉 (Cd)	汞 (Hg)	六价铬 (Cr ⁶⁺)	多溴联苯 (PBB)	多溴二苯乙醚 (PBDE)
电源供应器 Power Supply	×	○	○	○	○	○
风扇 Fan	×	○	○	○	○	○
散热片 Heat Sink	×	○	○	○	○	○
网络连接器 RJ45+X'FMR	×	○	○	○	○	○
突波吸收器 (静电保护) TVS Array	×	○	○	○	○	○
二极管 Diode	×	○	○	○	○	○
电阻 Resistor	×	○	○	○	○	○
本表格依据 SJ/T: 11364-2014 的规定编制。						
○: 表示此部件使用的所有同类材料中此种有毒或有害物质的含量均低于 GB/T 26572-2011 规定的限制要求。						
○: Indicates the toxic or hazardous substance content of the part (at the homogenous material level) is lower than the threshold defined by Requirements for Concentration Limits for Toxic or hazardous Substances in Electronic Information Products (GB/T 26572-2011) issued by Chinese Ministry of Information Industry ("Not Contained" toxic or hazardous substances).						
×: 表示此部件使用的至少一种同类材料中，此种有毒或有害物质的含量高于 GB/T 26572-2011 规定的限制要求。						
×: Indicates the toxic or hazardous substance content of the part (at the homogenous material level) is over the threshold defined by standard of GB/T 26572-2011 ("Contained" toxic or hazardous substances). Suppliers can explain the technical cause of "X" according to actual situation.						
除非另外特别的标注，此标志为针对所涉及产品的环保使用期标志，某些零部件会有一个不同的环保使用期（例如，电池单元模块）贴在其产品上。此环保使用期限只适用于产品是在产品手册中所规定的条件下工作。 The Environment- Friendly Use Period (EFUP) for all enclosed products and their parts are per the symbol shown here, unless otherwise marked. Certain parts may have a different EFUP (for example, battery modules) and so are marked to reflect such. The Environment- Friendly Use Period is valid only when the product is operated under the conditions defined in the product manual.						



限用物質含有情況標示聲明書						
Declaration of the Presence Condition of the Restricted Substances Marking						
設備名稱：2.5G L2 網管型 Ultra PoE++ 交換器			型號 (型式)：ECS4125-10P			
Equipment Name			Type Designation (Type)			
單元 Unit	限用物質及其化學符號		Restricted substances and its chemical symbols			
	鉛 (Pb)	汞 (Hg)	鎘 (Cd)	六價鉻 (Cr ⁶⁺)	多溴聯苯 (PBB)	多溴二苯醚 (PBDE)
電路板組件 PCBA	—	○	○	○	○	○
風扇 Fan	—	○	○	○	○	○
機殼 Chassis	○	○	○	○	○	○
組合線 Cable ass'y	○	○	○	○	○	○
電源供應器 Power Supply	—	○	○	○	○	○
備 考 1: "超出 0.1 wt %" 及 "超出 0.01 wt %" 係指限用物質之百分比含量超出百分比含量基準值。						
Note 1: "Exceeding 0.1 wt %" and "exceeding 0.01 wt %" indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.						
備 考 2: "○" 係指該項限用物質之百分比含量未超出百分比含量基準值。						
Note 2: "○" indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.						
備 考 3: "—" 係指該項限用物質為排除項目。						
Note 3: The "—" indicates that the restricted substance corresponds to the exemption.						

产品内含危害物质揭露表 Products contain hazardous substances exposing table						
零部件名称 Component Name	危害物质项目 Hazardous Substances Project					
	铅 (Pb)	镉 (Cd)	汞 (Hg)	六价铬 (Cr ⁶⁺)	多溴联苯 (PBB)	多溴二苯乙醚 (PBDE)
电源供应器 Power Supply	×	○	○	○	○	○
风扇 FAN	×	○	○	○	○	○
散热片 Heat Sink	×	○	○	○	○	○
网络连接器 RJ45+X'FMR	×	○	○	○	○	○
二极管 Diode	×	○	○	○	○	○
突波吸收器 (静电保护) TVS Array	×	○	○	○	○	○
电阻 Resistor	×	○	○	○	○	○
本表格依据 SJ/T: 11364-2014 的规定编制。						
○: 表示此部件使用的所有同类材料中此种有毒或有害物质的含量均低于 GB/T 26572-2011 规定的限制要求。						
○: Indicates the toxic or hazardous substance content of the part (at the homogenous material level) is lower than the threshold defined by Requirements for Concentration Limits for Toxic or hazardous Substances in Electronic Information Products (GB/T 26572-2011) issued by Chinese Ministry of Information Industry ("Not Contained" toxic or hazardous substances).						
×: 表示此部件使用的至少一种同类材料中，此种有毒或有害物质的含量高于 GB/T 26572-2011 规定的限制要求。						
×: Indicates the toxic or hazardous substance content of the part (at the homogenous material level) is over the threshold defined by standard of GB/T 26572-2011 ("Contained" toxic or hazardous substances). Suppliers can explain the technical cause of "X" according to actual situation.						
除非另外特别的标注，此标志为针对所涉及产品的环保使用期标志，某些零部件会有一个不同的环保使用期（例如，电池单元模块）贴在其产品上。此环保使用期限只适用于产品是在产品手册中所规定的条件下工作。 The Environment- Friendly Use Period (EFUP) for all enclosed products and their parts are per the symbol shown here, unless otherwise marked. Certain parts may have a different EFUP (for example, battery modules) and so are marked to reflect such. The Environment- Friendly Use Period is valid only when the product is operated under the conditions defined in the product manual.						



限用物質含有情況標示聲明書						
Declaration of the Presence Condition of the Restricted Substances Marking						
設備名稱：2.5G L2 網管型交換器			型號 (型式)：ECS4125-10T			
Equipment Name			Type Designation (Type)			
單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛 (Pb)	汞 (Hg)	鎘 (Cd)	六價鉻 (Cr ⁶⁺)	多溴聯苯 (PBB)	多溴二苯醚 (PBDE)
電路板組件 PCBA	—	○	○	○	○	○
電源供應器 Power Supply	—	○	○	○	○	○
風扇 FAN	—	○	○	○	○	○
機殼 Chassis	○	○	○	○	○	○
組合線 Cable ass'y	○	○	○	○	○	○
備 考 1: "超出 0.1 wt %" 及 "超出 0.01 wt %" 係指限用物質之百分比含量超出百分比含量基準值。						
Note 1: "Exceeding 0.1 wt %" and "exceeding 0.01 wt %" indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.						
備 考 2: "○" 係指該項限用物質之百分比含量未超出百分比含量基準值。						
Note 2: "○" indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.						
備 考 3: "—" 係指該項限用物質為排除項目。						
Note 3: The "—" indicates that the restricted substance corresponds to the exemption.						

Warranty Information and Technical Support

Registering your product enables you to receive a more efficient warranty service. Be sure to register at www.edge-core.com.

Anexo não disponível para exportação

ECS4125_Series_CLI_R02_0306.pdf

Consulte o documento digital na plataforma 1Doc para ter acesso a este arquivo:

Proc. Administrativo Processo Licitatório - 029/2025

Anexo não disponível para exportação

ECS4125_Series_WG_R02_0219.pdf

Consulte o documento digital na plataforma 1Doc para ter acesso a este arquivo:

Proc. Administrativo Processo Licitatório - 029/2025

EAP101

TIP OPEN INDOOR ACCESS POINT

INTRODUCTION

EAP101 is an enterprise-grade, concurrent dual-band Wi-Fi 6 indoor access point. EAP101 supports 2x2:2 uplink and downlink MU-MIMO between the AP and multiple clients, with up to 1.7Gbps aggregated data rate. EAP101 is equipped with Bluetooth Low Energy (BLE) radio enabling value-added applications such as iBeacon.

The TIP open EAP101 AP hardware is pre-installed with TIP's Open AP software, saving time and hassle from software installation, but at the same time reserve the flexibility for further changes. From SMB to MDUs to larger venues, the TIP open EAP101 is a flexible hardware platform for the different network use cases and requirements.



HIGHLIGHTS

- Concurrent Dual-Band 2.4 GHz & 5 GHz
- 802.11ax 2x2:2 UL MU-MIMO supporting up to 1.7 Gbps data rate
- Support up to 32 ESSIDs.
- Enterprise-Grade Wireless Security
- Bluetooth Low Energy (BLE)
- 802.3at Power over Ethernet (PoE)

SPECIFICATIONS

PHYSICAL	
CPU	IPQ6010
Flash	- NOR: 32MB - NAND: 256MB
Memory	1GB
Power	- DC Input: 12V / 2.0A (Power adapter included) - PoE: 802.3at compliant (PoE injector not included)
Dimensions	195 mm (L) x 195 mm (W) x 39 mm (H)
Weight	0.65 kg (1.44 lbs)
Interfaces	- Uplink: 1 x 10/100/1000/2.5GBase-T Ethernet, Auto MDIX, RJ-45 with 802.3at PoE - LAN: 2 x 10/100/1000Base-T Ethernet, Auto MDIX, RJ-45 - Console: 1 x RJ-45 Port - USB: 1 x USB 2.0 Port
LED Indicator	2.4G-WiFi / 5G-WiFi / Power
Buttons	Restart / Reset
Environmental Conditions	- Operating Temperature: 0°C (32°F) to 50°C (122°F) - Operating Humidity: 5% to 95% non-condensing
Power Consumption	22.4W max.
Antenna	- Type: 3 x Built-in antenna (2 x 2.4 GHz & 5 GHz, 1 x Bluetooth Low Energy) - Gain: 4.8 dBi (2.4 GHz), 6 dBi (5 GHz), 4.6 dBi (BLE)
Mounting	Wall/Ceiling/T-bar mount (Mounting kit included)
Anti-theft	1 x Kensington lock slot
WI-FI	
Standards	802.11ax (Wi-Fi 6) - Concurrent dual-band 2.4 & 5 GHz
Supported Data Rates	802.11b: 1, 2, 5.5, 11 Mbps 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps 802.11n: 6.5 – 300 Mbps (20 / 40 MHz) 802.11ac: 6.5 – 867 Mbps (20 / 40 / 80 MHz) 802.11ax: 3.6 – 574 Mbps (2.4 GHz, 20 / 40 MHz) 802.11ax: 3.6 – 1200 Mbps (5 GHz, 20 / 40 / 80 MHz)
Radio Chains	2 x 2
Spatial Streams	2; MU-MIMO support
Aggregate Conducted Transmit Power*1	2.4 GHz: 26dBm*2 5 GHz: 26dBm*2
Channelization	2.4 GHz: 20 / 40 MHz 5 GHz: 20 / 40 / 80MHz
Frequency Range	2.400 – 2.483 GHz 5.150 – 5.850 GHz
Operating Channels	5 GHz*3: 36 – 165 (US)
ESSIDs	Up to 16 per radio (32 total)
Certifications	FCC

*1: Aggregates across MIMO chains and doesn't contain antenna gain

*2: Maximum power is limited by local regulatory requirements

*3: Some channels are restricted by local regulatory requirements

- ◆ Up to 574 Mbps (2.4 GHz)
- ◆ Up to 1200 Mbps (5 GHz)

FIRMWARE

TIP Open WiFi Ready

PART NUMBER

EAP101_T

FIUEC0101002S-C (R0B)

Contact Us

For more information, please contact us: openwifi@edge-core.com

EC Open Wi-Fi Page

<https://wifi.edge-core.com/openwifi>

EC Open Wi-Fi User Forum

<https://openwifi.edge-core.com/>