EDITAL DE PREGÃO ELETRÔNICO Nº 02/2026

ORIGEM DA LICITAÇÃO:	**CÂMARA MUNICIPAL DE FORTALEZA – CMFOR**
MODALIDADE:	**PREGÃO ELETRÔNICO Nº 02/2026**
PROCESSO Nº	**03122025142900009544**
OBJETO:	**CONTRATAÇÃO, POR MEIO DE SISTEMA DE REGISTRO DE PREÇOS, DE EMPRESA ESPECIALIZADA PARA FORNECIMENTO DE SOLUÇÕES TECNOLÓGICAS DE SEGURANÇA, CONECTIVIDADE E REDE WI-FI CORPORATIVA, ABRANGENDO SERVIÇOS TÉCNICOS ESPECIALIZADOS, DESTINADOS À IMPLANTAÇÃO, MODERNIZAÇÃO, OPERAÇÃO E GESTÃO DA INFRAESTRUTURA DE REDE SEM FIO DA SEDE E DO PRÉDIO ANEXO DA CÂMARA MUNICIPAL DE FORTALEZA.**

A Autoridade Competente torna público torna público, para conhecimento dos interessados, que realizará licitação na modalidade **PREGÃO**, para **REGISTRO DE PREÇOS,** na forma **ELETRÔNICA**, a qual será conduzida pelo(a) Pregoeiro(a) designado(a) nos termos do **Lei Complementar nº 0370, de 27 de setembro de 2023 e Lei Complementar nº 0372, de 01 de fevereiro de 2023**, auxiliado(a) pela equipe de apoio também designada formalmente por ato publicado no **DOM** e juntado ao processo, para a escolha da proposta mais vantajosa, objetivando a contratação do objeto desta licitação, observadas as normas e condições do presente Edital e seus anexos, e as disposições contidas nos na **Lei Federal nº 14.133,** de 1º de abril de 2021, com suas alterações posteriores, no **Decreto Municipal nº 15.604**, de 28 de março de 2023, nas **Leis Municipais nº 10.350,** de 28 de maio de 2015, **nº 11.438,** de 04 de janeiro de 2024, na **Lei Complementar nº 123,** de 14 de dezembro de 2006, alterada pela **Lei Complementar nº 147,** de 07 de agosto de 2014, na **Lei Federal nº 13.709,** de 14 de agosto de 2018 (LGPD - Lei Geral de Proteção de Dados), bem como na Resolução nº 1.684, de 20 de dezembro de 2024, e no disposto no presente Edital e seus Anexos.

- **CRITÉRIO DE JULGAMENTO**: MENOR PREÇO GLOBAL
- **DO TIPO DE OBJETO:** SERVIÇOS COMUNS
- **MODO DE DISPUTA:** ABERTO E FECHADO
- **FORNECIMENTO:** PARCELADO
- **EXCLUSIVA ME/EPP/EQUIPARADAS**: NÃO

*__DO ACESSO AO EDITAL E DO LOCAL DE REALIZAÇÃO:__

1. O Edital e seus anexos estão disponíveis na íntegra, no Portal Nacional de Contratações Públicas – PNCP (https://www.gov.br/pncp/pt-br), bem como no sítio

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

https://portaltransparencia.cmfor.ce.gov.br/licitacoes/licitacoes e no site da Plataforma Licita Mais Brasil, acessível através do sítio www.licitamaisbrasil.com.br/editais**.**

2. O certame será realizado por meio da Plataforma de Licitações Eletrônicas Licita Mais Brasil, disponível no endereço eletrônico www.licitamaisbrasil.com.br**.**

3. As solicitações, informações ou dúvidas, bem como o acompanhamento de todo o trâmite ocorrerão através do sítio: www.licitamaisbrasil.com.br/editais, sendo necessário a licitante realizar **PRÉVIO CADASTRO SIMPLES NA PLATAFORMA.**

***DAS DATAS E HORÁRIOS DO CERTAME:**

4. **INÍCIO DO ACOLHIMENTO DAS PROPOSTAS**: 24/03/2026, às 15h00min.

5. DATA DE ABERTURA DAS PROPOSTAS: 14/04/2026, às 10h00min.

6. INÍCIO DA SESSÃO DE DISPUTA DE PREÇOS: 14/04/2026, às 10h00min.

7. REFERÊNCIA DE TEMPO: Para todas as referências de tempo utilizadas pelo Sistema será observado o horário de Brasília/DF.

8. Na hipótese de não haver expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data prevista, a sessão será remarcada, para no mínimo, 48h (quarenta e oito horas) a contar da respectiva data.

SUMÁRIO

1. DO OBJETO
2. DA PARTICIPAÇÃO NA LICITAÇÃO
3. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO
4. DO PREENCHIMENTO DA PROPOSTA
5. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES
6. DA FASE DE JULGAMENTO
7. DA FASE DE HABILITAÇÃO
8. DOS RECURSOS
9. DA ADJUDICAÇÃO E HOMOLOGAÇÃO
10. DA FORMALIZAÇÃO E ASSINATURA DA ATA DE REGISTRO DE PREÇOS
11. DA FORMAÇÃO DO CADASTRO DE RESERVA
12. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES
13. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO
14. DAS DISPOSIÇÕES GERAIS

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

1. DO OBJETO:

1.1 CONTRATAÇÃO, POR MEIO DE SISTEMA DE REGISTRO DE PREÇOS, DE EMPRESA ESPECIALIZADA PARA FORNECIMENTO DE SOLUÇÕES TECNOLÓGICAS DE SEGURANÇA, CONECTIVIDADE E REDE WI-FI CORPORATIVA, ABRANGENDO SERVIÇOS TÉCNICOS ESPECIALIZADOS, DESTINADOS À IMPLANTAÇÃO, MODERNIZAÇÃO, OPERAÇÃO E GESTÃO DA INFRAESTRUTURA DE REDE SEM FIO DA SEDE E DO PRÉDIO ANEXO DA CÂMARA MUNICIPAL DE FORTALEZA.

1.2 A licitação será em **LOTE ÚNICO**, conforme tabela constante do Termo de Referência, devendo oferecer proposta para todos os itens.

2. DA PARTICIPAÇÃO NA LICITAÇÃO:

2.1. Poderão participar deste Pregão Eletrônico os interessados que atenderem a todas as exigências de habilitação contidas neste Edital e seus anexos, cujo ramo de atividade seja compatível com o objeto desta licitação, e que estejam, obrigatoriamente, credenciados no sistema eletrônico utilizado neste processo.

2.2. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

2.3. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais nos Sistemas relacionados no item anterior e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

2.4. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

2.5. A participação implica a aceitação integral dos termos deste edital.

2.6. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 16, da Lei nº 14.133/2021, para o agricultor familiar, o produtor rural pessoa física e para o microempreendedor individual MEI, nos limites previstos da Lei Complementar nº 123, de 2006.

2.7. Será garantido às licitantes enquadradas como microempresas, empresas de pequeno porte, nos termos do art. 34, da Lei Federal n° 11.488/2007, como critério de desempate, preferência de contratação, de acordo com o previsto na Lei Complementar n° 123/2006, em seu Capítulo V – DO ACESSO AOS MERCADOS/Das Aquisições Públicas e Lei Municipal nº 10.350, 28 de maio de 2015; no Decreto nº 13.735, de 18 de janeiro de 2016 (atualizado).

2.8. Tratando-se de microempresas, empresas de pequeno porte que se enquadrem nos termos do art. 34, da Lei Federal n° 11.488/2007, e que não se encontram em qualquer das exclusões relacionadas no § 4º do artigo 3º, da Lei Complementar nº 123/2006, deverão declarar no Sistema o exercício do direito de preferência previsto em Lei.

2.9. Não poderão disputar esta licitação:

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

2.9.1. Aquele que não atenda às condições deste Edital e seus anexos;

2.9.2. Autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre serviços ou fornecimento de bens a ele relacionados;

2.9.3. Empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre serviços ou fornecimento de bens a ela necessários;

2.9.4. Pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

2.9.5. Aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

2.9.6. Empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

2.9.7. Pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

2.9.8. Agente público do órgão ou entidade licitante;

2.9.9. Pessoas jurídicas reunidas em consórcio, conforme justificativa constante no ANEXO IV;

2.9.10. Organizações da Sociedade Civil de Interesse Público – OSCIP, atuando nessa condição;

2.10. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º, do art. 9º, da Lei nº 14.133, de 2021.

2.11. O impedimento de que trata o item 2.9.4 será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

2.12. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens 2.9.2 e 2.9.3 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

2.13. Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

2.14. O disposto nos itens 2.9.2 e 2.9.3 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

2.15. Em licitações e contratações realizadas no âmbito de projetos e programas parcialmente financiados por agência oficial de cooperação estrangeira ou por organismo financeiro internacional com recursos do financiamento ou da contrapartida nacional, não poderá participar pessoa física ou jurídica que integre o rol de pessoas sancionadas por essas entidades ou que seja declarada inidônea nos termos da Lei nº 14.133/2021.

2.16. A vedação de que trata o item 2.9.8 estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

3. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO:

3.1. Será exigida apresentação dos documentos de habilitação, apenas pelo licitante vencedor.

3.1.1. Durante a fase de julgamento/negociação, logo após a aprovação da proposta primeiro colocada, será aberto o prazo de 2 (duas) horas para que o fornecedor encaminhe através do sistema o arquivo da proposta ajustada ao valor final negociado.

3.1.2. Após o julgamento da proposta, durante a fase de habilitação, o licitante vencedor deverá enviar no prazo de 2 (duas) horas contado da convocação da Pregoeira, os documentos de habilitação.

3.1.3. A fase de habilitação está prevista no item 7 deste edital.

3.2. Na presente licitação, a fase de habilitação sucederá as fases de apresentação de propostas e lances e de julgamento.

3.3. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública.

3.4. Caso a fase de habilitação anteceda as fases de apresentação de propostas e lances, os licitantes encaminharão, na forma e no prazo estabelecidos no item anterior, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto nos itens 7.6 e 7.13.1 deste Edital.

3.5. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:

3.5.1. Está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infra legais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

3.5.2. Não emprega menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 (dezesseis) anos, salvo menor, a partir de 14 (catorze) anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição Federal.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

3.5.3. Não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

3.5.4. Cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

3.6. O licitante organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 1 de abril de 2021.

3.7. O licitante enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei nº 14.133, de 2021.

3.8. Em caso de falsidade das documentações apresentadas, sujeitará o licitante às sanções previstas na Lei nº 14.133/2021, e neste Edital.

3.9. A licitante deverá apresentar **DECLARAÇÃO DE CONDUTA ÉTICA E ANTICORRUPÇÃO – ANEXO III** e, inclusive, na qualidade de eventualmente contratado, observará e fará observar por seus fornecedores e subcontratados, se admitida subcontratação, o mais alto padrão de ética durante todo o processo de licitação, de contratação e de execução do objeto contratual.

3.10. Os licitantes poderão retirar ou substituir a proposta ou, na hipótese de a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, os documentos de habilitação anteriormente inseridos no sistema, até a abertura da sessão pública.

3.11. Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

3.12. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo quando do cadastramento da proposta e obedecerá às seguintes regras:

3.12.1. A aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e

3.12.2. Os lances serão de envio automático pelo sistema, respeitado o valor final mínimo estabelecido e o intervalo de que trata o subitem acima.

3.13. O valor final mínimo ou o percentual de desconto final máximo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

3.13.1. Valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço; e

3.13.2. Percentual de desconto inferior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por maior desconto.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

3.14. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 3.12 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

3.15. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

3.16. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

4. DO PREENCHIMENTO DA PROPOSTA

4.1 O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

4.1.1 Valor unitário dos itens e o valor total do lote;

4.1.2 Descrição do objeto, contendo as informações similares à especificação do Termo de Referência;

4.1.3 O licitante não poderá oferecer proposta em quantitativo inferior ao máximo previsto no Termo de Referência, obrigando-se nos limites dela;

4.2 Na elaboração da Proposta, o preço cotado poderá ultrapassar o valor de referência da presente licitação discriminado na **ESTIMATIVA DA CONTRATAÇÃO**, **que terá caráter sigiloso até o final da licitação e será disponibilizado exclusiva e permanentemente aos órgãos de controle externo e interno**. Entretanto, na disputa de lances, o lance final, deverá atingir preço inferior ou igual ao limite máximo constante da **ESTIMATIVA DE CONTRATAÇÃO**. Caso não seja realizada a disputa de lances, a licitante que cotou na proposta o menor preço deverá reduzi-lo a um valor inferior ou igual ao limite máximo acima especificado.

4.3 Todas as especificações do objeto contidas na proposta vinculam o licitante.

4.4 Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

4.5 Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

4.6 Se o regime tributário da empresa implicar no recolhimento de tributos em percentuais variáveis, no momento dos pagamentos, deverão ser retidos na fonte os percentuais estabelecidos na legislação vigente.

4.7 A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais,

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

4.8 O prazo de validade da proposta não será inferior a **60 (sessenta) dias**, a contar da data de sua apresentação.

4.9 O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização pelo Tribunal de Contas competente, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

5. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES:

5.1 A abertura da presente licitação dar-se-á em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

5.2 Os licitantes poderão retirar ou substituir a proposta ou os documentos de habilitação, quando for o caso, anteriormente inseridos no sistema, até a abertura da sessão pública.

5.2.1 Será vedada a identificação da licitante, por qualquer meio ou forma, antes da etapa de lance.

5.2.2 A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

5.2.3 A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.

5.3 O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

5.4 O sistema disponibilizará campo próprio para troca de mensagens entre o(a) Pregoeiro(a) e os licitantes.

5.5 Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

5.6 O lance deverá ser ofertado pelo **VALOR TOTAL DO LOTE**.

5.7 Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

5.8 O licitante somente poderá oferecer lance **de valor inferior** ao último por ele ofertado e registrado pelo sistema.

5.9 O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de 0,01 (um centavo).

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

5.10 O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

5.11 O procedimento seguirá de acordo com o modo de disputa adotado: **ABERTO E FECHADO**.

5.12 Será adotado para o envio de lances no pregão eletrônico o modo de disputa "**aberto e fechado",** os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

5.12.1 A etapa de lances da sessão pública terá duração inicial de quinze minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de tempo de até dez minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.
5.12.2 Encerrado o prazo previsto no subitem anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até 10% (dez por cento) superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

5.12.3 No procedimento de que trata o subitem supra, o licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance.

5.12.4 Não havendo pelo menos três ofertas nas condições definidas neste item, poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

5.13 Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

5.14 Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

5.15 Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

5.16 No caso de desconexão com o(a) Pregoeiro(a), no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

5.17 Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

5.18 Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45, da Lei Complementar nº 123/2006, regulamentada pelo Decreto nº 13.735/2016.

5.18.1 Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

5.18.2 A melhor classificada nos termos do subitem anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

5.18.3 Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

5.18.4 No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

5.19 Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

5.19.1 Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60, da Lei nº 14.133/2021, nesta ordem:

5.19.1.1 Disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

5.19.1.2 Avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos nesta Lei;

5.19.1.3 Desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;

5.19.1.4 Desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

5.19.2 Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

5.19.2.1 Empresas estabelecidas no território do Estado ou do Distrito Federal do órgão ou entidade da Administração Pública estadual ou distrital licitante ou, no caso de licitação realizada por órgão ou entidade de Município, no território do Estado em que este se localize;

5.19.2.2 Empresas brasileiras;

5.19.2.3 Empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

5.19.2.4 Empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de dezembro de 2009;

5.19.2.5 Exauridos os critérios de desempate e do resultado persistir o empate, o(a) Pregoeiro(a) procederá com sorteio público para definição da ordem sequencial de colocações no certame;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

5.19.2.6 As regras e práticas da sessão pública de sorteio serão previamente divulgadas pelo(a) Pregoeiro(a).

5.20 Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo ou inferior ao desconto definido para a contratação, o(a) Pregoeiro(a) poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

5.20.1 A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela Administração.

5.20.2 A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

5.20.3 O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório.

5.20.4 O(a) Pregoeiro(a) solicitará ao licitante mais bem classificado que, **no prazo de 2 (duas) horas**, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

5.20.5 É facultado ao(a) Pregoeiro(a) prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

5.20.6 Após a negociação do preço, o(a) Pregoeiro(a) iniciará a fase de aceitação e julgamento da proposta.

6. DA FASE DE JULGAMENTO

6.1 Encerrada a etapa de negociação, o(a) Pregoeiro(a) verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021.

6.2 Caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

6.3 Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPP's, o(a) Pregoeiro(a) verificará se faz jus ao benefício, em conformidade com o item 3.7 do Edital.

6.4 Verificadas as condições de participação e de utilização do tratamento favorecido, a Pregoeira examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no artigo 29 a 35, da IN SEGES nº 73, de 30 de setembro de 2022.

6.5 Será desclassificada a proposta vencedora que:

6.5.1 Contiver vícios insanáveis;

6.5.2 Não obedecer às especificações técnicas contidas no Termo de Referência;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

6.5.3 Apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

6.5.4 Não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

6.5.5 Apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

6.6 No caso de bens e serviços em geral, é indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

6.6.1 A inexequibilidade, na hipótese de que trata o caput, só será considerada após diligência da Pregoeira, que comprove:

6.6.1.1 Que o custo do licitante ultrapassa o valor da proposta; e

6.6.1.2 Inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

6.7 Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a exequibilidade da proposta.

6.8 Caso o custo global estimado do objeto licitado tenha sido decomposto em seus respectivos custos unitários por meio de Planilha de Custos e Formação de Preços elaborada pela Administração, o licitante classificado em primeiro lugar será convocado para apresentar Planilha por ele elaborada, com os respectivos valores adequados ao valor final da sua proposta, sob pena de não aceitação da proposta.

6.9 Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado no sistema, desde que não haja majoração do preço.

6.9.1 O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas;

6.9.2 Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

6.10 Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

7. DA FASE DE HABILITAÇÃO

7.1 Os documentos previstos no **ANEXO I – TERMO DE REFERÊNCIA**, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021.

7.2 Quando permitida a participação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

7.2.1 Na hipótese de o licitante vencedor ser empresa estrangeira que não funcione no País, para fins de assinatura do contrato, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

7.3 Os documentos exigidos para fins de habilitação poderão ser apresentados em original ou por cópia.

7.4 Será verificado se o licitante apresentou DECLARAÇÃO de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I, da Lei nº 14.133/2021).

7.5 Será verificado se o licitante apresentou no sistema, sob pena de inabilitação, a declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

7.6 O licitante deverá apresentar, sob pena de desclassificação, DECLARAÇÃO de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

7.7 A verificação pelo(a) Pregoeiro(a), em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

7.8 Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para (Lei 14.133/21, art. 64, e IN 73/2022, art. 39, §4º):

7.8.1 Complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

7.8.2 Atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;

7.9 Na análise dos documentos de habilitação, o(a) Pregoeiro(a) poderá sanar erros ou falhas, que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

7.10 Na hipótese do licitante não atender às exigências para habilitação, o(a) Pregoeiro(a) examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital.

7.11 Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.

7.12 A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte somente será exigida para efeito de contratação, e não como condição para participação na licitação (art. 4º do Decreto nº 8.538/2015).

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

8. DOS RECURSOS

8.1 A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021.

8.2 O prazo recursal é de **3 (três) dias úteis**, contados da data de intimação ou de lavratura da ata.

8.3 Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:

8.3.1 A intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão no prazo de 10 minutos, concedidos após a fase de julgamento e negociação e após a fase de habilitação do primeiro colocado.

8.4 Os recursos deverão ser encaminhados em campo próprio do sistema.

8.5 O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

8.6 Os recursos interpostos fora do prazo não serão conhecidos.

8.7 O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de 3 (três) dias úteis, contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.

8.8 O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

8.9 O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

9. DA ADJUDICAÇÃO E HOMOLOGAÇÃO:

9.1 Encerrada a fase recursal, a autoridade superior do órgão ou entidade adjudicará o objeto da licitação e homologará o procedimento licitatório.

10. DA FORMALIZAÇÃO E ASSINATURA DA ATA DE REGISTRO DE PREÇOS:

10.1. Homologado o resultado da licitação, o Órgão gerenciador da Ata de Registro de Preços, respeitada a ordem de classificação e a quantidade de fornecedores a serem registrados, convocará os interessados para, no prazo de 5 (cinco) dias, contados da data da convocação, proceder à assinatura da Ata de Registro de Preços, a qual, após cumpridos os requisitos de publicidade, terá efeito de compromisso de fornecimento, nas condições estabelecidas.

10.2. O prazo previsto poderá ser prorrogado uma vez, por igual período, quando, durante o seu transcurso, for solicitado pela licitante convocada, desde que ocorra motivo justificado e aceito pelo órgão gerenciador.

10.3. Os preços registrados na Ata de Registro de Preços serão aqueles ofertados nas propostas de preços do(s) licitante(s) vencedor(s), bem como será incluído na respectiva ata o registro do(s)

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

licitante(s) que aceitar(em) cotar o objeto com preços iguais ao do licitante vencedor, na sequência da classificação do certame, conforme permissivo legal do art. 16, inciso II do Decreto 15.608, de 31 de março de 2023, ou a informação expressa de que não houve licitante que aceitasse cotar o objeto com preços iguais à da licitante vencedora.

10.4. Quando o licitante vencedor for convocado para assinar a Ata de Registro de Preços não comparecer, recusar-se a assinar ou não comprovar as condições habilitatórias, sem prejuízo das cominações previstas neste Edital e seus Anexos, poderá o(a) Pregoeiro(a) convocar outro licitante registrado na Ata, desde que respeitada a ordem de classificação e mantidos os preços registrados iguais ao do adjudicatário, para assinatura da Ata de Registro de Preços.

10.5. As regras referentes ao registro de preço, aos órgãos gerenciador, participantes e não participantes, descumprimento, remanejamento, prazo de vigência, do fornecimento, e demais regras constam da minuta de **ATA DE REGISTRO DE PREÇOS – ANEXO VI** deste edital.

11. DA FORMAÇÃO DO CADASTRO DE RESERVA:

11.1. Após a homologação da licitação, será incluído na ata, na forma de anexo, o registro:

11.1.1. Dos licitantes que aceitarem cotar o objeto com preço igual ao do adjudicatário, observada a classificação na licitação; e

11.1.2. Dos licitantes que mantiverem sua proposta original;

11.2. Será respeitada, nas contratações, a ordem de classificação dos licitantes ou fornecedores registrados na ata.

11.2.1. A apresentação de novas propostas na forma deste item não prejudicará o resultado do certame em relação ao licitante mais bem classificado.

11.2.2. Para fins da ordem de classificação, os licitantes ou fornecedores que aceitarem cotar o objeto com preço igual ao do adjudicatário antecederão aqueles que mantiverem sua proposta original.

11.3. A habilitação dos licitantes que comporão o cadastro de reserva será efetuada quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:

11.3.1. Quando o licitante vencedor não assinar a ata de registro de preços no prazo e nas condições estabelecidos no edital; ou

11.3.2. Quando houver o cancelamento do registro do fornecedor ou do registro de preços, nas hipóteses previstas nos art. 28 e art. 29 do Decreto nº 11.462/23.

11.4. Na hipótese de nenhum dos licitantes que aceitaram cotar o objeto com preço igual ao do adjudicatário concordar com a contratação nos termos em igual prazo e nas condições propostas pelo primeiro classificado, a Administração, observados o valor estimado e a sua eventual atualização na forma prevista no edital, poderá:

11.4.1. Convocar os licitantes que mantiveram sua proposta original para negociação, na ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário; ou

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

11.4.2. Adjudicar e firmar o contrato nas condições ofertadas pelos licitantes remanescentes, observada a ordem de classificação, quando frustrada a negociação de melhor condição.

12. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES:

12.1. Comete infração administrativa, nos termos da lei, o licitante que praticar ato ilícito na forma do art. 155 da Lei Federal nº 14.133, de 1º de abril de 2021, e especialmente quando:

12.1.1. deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a pregoeiro/a durante o certame;

12.1.2. salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:

12.1.2.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;

12.1.2.2. recusar-se a enviar o detalhamento da proposta quando exigível;

12.1.2.3. pedir para ser desclassificado quando encerrada a etapa competitiva; ou

12.1.2.4. deixar de apresentar amostra;

12.1.2.5. apresentar proposta ou amostra em desacordo com as especificações do edital;

12.1.2.6. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

12.1.2.7. recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

12.1.2.8. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação;

12.1.2.9. fraudar a licitação;

12.1.2.10. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

12.1.2.11. agir em conluio ou em desconformidade com a lei;

12.1.2.12. induzir deliberadamente a erro no julgamento;

12.1.2.13. apresentar amostra falsificada ou deteriorada;

12.1.2.14. praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

12.1.2.15. praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 2013.

12.2. Com fulcro na Lei nº 14.133, de 2021, a Administração poderá, garantido o devido processo legal, assegurado o prévio contraditório e a ampla defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

12.2.1. advertência;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

12.2.2. multa;

12.2.3. impedimento de licitar e contratar e

12.2.4. declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

12.2.5. A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor do contrato licitado, recolhida no prazo máximo de 30 (trinta) dias úteis, a contar da comunicação oficial.

12.2.6. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

12.2.7. Na aplicação da sanção de multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

12.2.8. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos termos do §4º do art. 156 da Lei nº 14.133, de 1º de abril de 2021 e do art. 15 do Decreto Municipal nº 15.604, de 28 de março de 2023, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

12.2.9. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos termos do § 5º do art. 156 da Lei nº 14.133, de 1º de abril de 2021, e do art. 16 do Decreto Municipal nº 15.604, de 28 de março de 2023, que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos.

12.2.10. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 10.1, caracteriza o descumprimento total da obrigação assumida e o sujeitará às penalidades e à decadência do direito à garantia de proposta em favor do órgão ou entidade promotora da licitação, nos termos do art. 18 do Decreto Municipal nº 15.604, de 28 de março de 2023.

12.2.11. A apuração de responsabilidades relacionadas às sanções descritas seguirá os procedimentos descritos na Lei 14.133, de 1º de abril de 2023, bem como o Decreto Municipal nº 15.604, de 28 de março de 2023.

12.2.12. O pagamento das multas não eximirá a contratada de ser acionada judicialmente pela responsabilidade civil derivada de perdas e danos junto à contratante, decorrentes das infrações porventura cometidas, inclusive pela inobservância do disposto na Lei 13.709/2018 (LGPD), na forma abaixo estipuladas:

12.2.12.1. Multa de 20% (vinte por cento) sobre o valor total do CONTRATO, na hipótese de tratamento de dados pessoais sensíveis com o objetivo de obter vantagem econômica, ou outra irregularidade havida no cumprimento do CONTRATO, por culpa da CONTRATADA.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

12.2.12.2. Multa de 10% (dez por cento) sobre o valor total do CONTRATO, na hipótese de descumprimento da obrigação de zelo no tratamento dos dados pessoais da pessoa natural vinculada à CONTRATANTE, ou em caso de tratamento de dados sem o consentimento específico e destacado por termo de compromisso, ou outra irregularidade havida no cumprimento do CONTRATO, por culpa da CONTRATADA.

13. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO:

13.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da Lei nº 14.133, de 2021, devendo protocolar o pedido **até 3 (três) dias úteis antes da data da abertura do certame,** no endereço eletrônico citado no item 13.3 abaixo.

13.2. A resposta à impugnação ou ao pedido de esclarecimento será divulgado em sítio eletrônico oficial no prazo de **até 3 (três) dias úteis**, limitado ao último dia útil anterior à data da abertura do certame.

13.2.1 As decisões do(a) Pregoeiro(a), se darão com embasamento nos pareceres e laudos emitidos pelas áreas técnicas e jurídicas da CMFOR.

13.2.2 Na impossibilidade de resposta à impugnação no prazo citado no item 13.2, o(a) Pregoeiro(a) poderá adiar a abertura da sessão pública, mediante aviso no sistema utilizado na realização do certame.

13.3. A impugnação e o pedido de esclarecimento deverão ser realizados exclusivamente por meio eletrônico, diretamente no site da Plataforma Licita Mais Brasil (https://licitamaisbrasil.com.br/). O fornecedor interessado em solicitar esclarecimentos ou impugnar o processo, deverão fazê-lo através de um cadastro simples na plataforma, que é totalmente gratuito ao usuário.

13.3.1 As impugnações apresentadas deverão ser subscritas por representante legal mediante comprovação, sob pena do seu não conhecimento.

13.4. O (a) Pregoeiro (a) poderá solicitar manifestação técnica da assessoria jurídica ou de outros setores do órgão ou da entidade, a fim de subsidiar sua decisão.

13.5. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

13.5.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo agente de contratação, nos autos do processo de licitação.

13.6. Acolhida a impugnação, será definida e publicada nova data para a realização do certame, exceto quando a alteração não comprometer a formulação das propostas.

13.7. Qualquer modificação no Edital exige divulgação pelo mesmo instrumento de publicação em que se deu o texto original, reabrindo-se o prazo inicialmente estabelecido, exceto quando, inquestionavelmente, a alteração não afetar a formulação das Propostas de Preços.

14. DAS DISPOSIÇÕES GERAIS:

14.1. Será divulgada Termo de Julgamento no sistema eletrônico.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

14.2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo(a) Pregoeiro(a).

14.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília – DF.

14.4. A homologação do resultado desta licitação não implicará direito à contratação.

14.5. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

14.6. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

14.7. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

14.8. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

14.9. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

14.10. É facultada ao(à) Pregoeiro(a) e/ou equipe de apoio, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou a complementar a instrução do processo licitatório (vedada a inclusão posterior de documentos que deveriam constar originalmente na proposta de preços e na documentação de habilitação), bem como para averiguar a veracidade das informações fornecidas pela licitante e, se for o caso, a adequação da estrutura física e operacional da empresa às exigências do objeto licitado.

14.11. O descumprimento de prazos estabelecidos neste Edital e/ou pelo(a) Pregoeiro(a) junto ao Sistema, ou o não atendimento às solicitações/determinações, ensejará DESCLASSIFICAÇÃO ou INABILITAÇÃO.

14.12. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) https://www.gov.br/pncp/pt-br e endereço eletrônico **http://transparencia.cmfor.ce.gov.br/#licitacoes** e no site da Plataforma Licita Mais Brasil, acessível através do sítio **www.licitamaisbrasil.com.br/editais**.

14.13. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:
ANEXO I – TERMO DE REFERÊNCIA
ANEXO II – MODELO DE PROPOSTA DE PREÇOS
ANEXO III – MODELO MERAMENTE SUGESTIVO DE DECLARAÇÃO DE CONDUTA ÉTICA E ANTICORRUPÇÃO
ANEXO IV – JUSTIFICATIVA DA ESCOLHA DO ORÇAMENTO SIGILOSO

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

ANEXO V - JUSTIFICATIVA DA NÃO PARTICIPAÇÃO DE EMPRESA NA FORMA DE CONSÓRCIO
ANEXO VI – MINUTA DA ATA DE REGISTRO DE PREÇOS
ANEXO VII – MINUTA DO CONTRATO

Fortaleza - CE, 20 de março de 2026.

EMANUEL ÂNGELO PINHEIRO DO VALE
Diretor Geral

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

ANEXO I
TERMO DE REFERÊNCIA

Conforme exigido pela Lei nº 14.133/2021, o Termo de Referência anexo a este Edital foi elaborado e assinado pelo setor técnico competente, responsável pela definição do objeto da contratação.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

ANEXO I - TERMO DE REFERÊNCIA

PROCESSO: 03122025142900009544

1. IDENTIFICAÇÃO

1.1. Órgão/Entidade Demandante:

CÂMARA MUNICIPAL DE FORTALEZA – CMFor

1.2. Unidade Administrativa Responsável:

Coordenação de Informação e Dados (COID)

2. IDENTIFICAÇÃO DA DEMANDA/OBJETO:

2.1. Constitui objeto da presente licitação a **contratação, por meio de sistema de registro de preços, de empresa especializada para fornecimento de soluções tecnológicas de segurança, conectividade e rede wi-fi corporativa, abrangendo serviços técnicos especializados, destinados à implantação, modernização, operação e gestão da infraestrutura de rede sem fio da sede e do prédio anexo da Câmara Municipal de Fortaleza.**

2.2. Este objeto será realizado mediante licitação, na modalidade PREGÃO, na forma ELETRÔNICA, do tipo MENOR PREÇO, com fornecimento EM LOTE ÚNICO.

2.3. O objeto compreende: Soluções de software e licenciamento: Plataformas de gerenciamento centralizado, monitoramento, segurança e controle de acesso à rede, incluindo soluções de firewall de nova geração, controle de acesso à rede (NAC), segurança de aplicações, segurança de e-mail, proteção de dispositivos e plataforma de monitoramento e observabilidade; Equipamentos e infraestrutura: Equipamentos de conectividade de rede, incluindo switches de acesso e de núcleo (core), solução Wi-Fi corporativa e demais componentes necessários à plena operação da infraestrutura de rede segura; Serviços técnicos especializados: Serviços de instalação, configuração, parametrização, integração, testes, homologação, treinamento, suporte técnico contínuo, manutenção preventiva e corretiva, bem como atualização de softwares, firmwares e assinaturas, durante toda a vigência contratual.

▪ **LOTE ÚNICO:** Fornecimento, implantação e suporte técnico de solução integrada de infraestrutura de rede e segurança da informação, incluindo equipamentos de conectividade, licenças de software, serviços de configuração, manutenção e suporte.

3. FUNDAMENTAÇÃO E JUSTIFICATIVA DA CONTRATAÇÃO

3.1. A contratação aqui pretendida fundamenta-se no estudo técnico preliminar, na Lei 14.133 de 01 de abril de 2021 e as demais normas vigentes aplicáveis às contratações públicas

3.2. A Câmara Municipal de Fortaleza (CMFOR), enquanto órgão do Poder Legislativo responsável pela produção normativa, fiscalização e controle externo da Administração Pública Municipal, depende de infraestrutura de tecnologia da informação estável, segura e alinhada às melhores práticas de gestão de redes e segurança cibernética. O ambiente atual, administrado pela Diretoria do Departamento de Processamento de Dados (DEPROD), por meio da Divisão de Administração de Rede (DIAR) e Divisão de Informática (DINFO), apresenta limitações estruturais que impactam diretamente a operação diária dos serviços legislativos e administrativos.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

3.3. A rede corporativa da CMFOR foi expandida ao longo dos últimos anos sem adoção de uma arquitetura padronizada de conectividade segura, possuindo switches com diferentes capacidades, modelos antigos sem suporte oficial, inexistência de camada de acesso padronizada, ausência de gerenciamento centralizado, lacunas no controle de acesso à rede (NAC) e falta de automatização na gestão de dispositivos conectados. Além disso, não há solução unificada de segurança de e-mail, proteção de aplicações web, monitoramento de tráfego, análise de comportamento, correlação de eventos ou visibilidade centralizada do ambiente de rede.

3.4. Essas fragilidades representam risco concreto à continuidade das atividades institucionais, expondo a CMFOR a indisponibilidades, falhas de comunicação interna, lentidão de serviços, pontos de falha únicos e vulnerabilidades que podem ser exploradas por ameaças externas, especialmente em um cenário de crescente sofisticação de ataques cibernéticos como ransomware, spear phishing, sequestro de sessões, exploração de APIs e ataques direcionados a aplicações web.

3.5. Adicionalmente, a instituição ainda não dispõe de solução robusta de conectividade Wi-Fi corporativa com gerenciamento em nuvem, autenticação segura e políticas centralizadas. A ausência desse componente limita iniciativas de modernização interna, dificulta o acesso móvel de servidores e vereadores, compromete a produtividade e não atende às necessidades atuais de mobilidade digital.

3.6. O ambiente de segurança também carece de uma solução padronizada de proteção de dispositivos de acesso à rede, filtros de navegação, mecanismos de prevenção de ameaças e estrutura de firewall de aplicações. A ausência dessas ferramentas dificulta a mitigação de riscos avançados, não atende às diretrizes da LGPD, compromete a confidencialidade das informações legislativas e afeta diretamente a integridade dos sistemas corporativos.

3.7. Diante dessas limitações e visando a modernização tecnológica da Casa Legislativa, a presente contratação se torna essencial para reestruturar a arquitetura de conectividade e segurança da CMFOR, abrangendo soluções de:

- segurança de rede (firewalls e proteção avançada contra ameaças);
- switches de acesso e core gerenciáveis;
- solução NAC para controle de acesso seguro;
- Wi-Fi corporativo de alto desempenho com gerenciamento unificado;
- segurança de e-mail;
- segurança das aplicações e firewall de aplicação;
- proteção dos dispositivos que acessam a rede;
- monitoramento centralizado;
- serviços de instalação, parametrização, suporte e operação assistida.

3.8. A adoção de uma solução integrada e padronizada permitirá à CMFOR elevar o nível de disponibilidade, confiabilidade, resiliência e segurança do ambiente tecnológico, garantindo continuidade dos serviços legislativos, proteção das informações críticas, redução de riscos operacionais e alinhamento às boas práticas contemporâneas de gestão de redes e segurança cibernética, conforme demandado pelo interesse público

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

4.1 A solução pretendida consiste na implementação de um conjunto integrado de tecnologias

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

capazes de modernizar de forma abrangente a infraestrutura de rede e segurança da Câmara Municipal de Fortaleza (CMFOR), contemplando elementos de conectividade, controle de acesso, segurança de perímetro, proteção de aplicações, segurança de e-mail, proteção de dispositivos, monitoramento contínuo e serviços técnicos especializados. Trata-se de uma arquitetura completa, unificada e padronizada, cujo objetivo é assegurar altos níveis de disponibilidade, desempenho, governança e segurança cibernética, atendendo às demandas operacionais da Casa Legislativa e mitigando riscos associados ao uso crescente de serviços digitais.

4.2 A solução será composta por dispositivos de segurança de rede (firewalls de nova geração) com recursos avançados de inspeção profunda de tráfego, prevenção contra intrusões, controle de aplicações, mitigação de ataques, filtragem de conteúdo e mecanismos integrados de proteção contra ameaças conhecidas e desconhecidas. Esses equipamentos deverão operar em alta disponibilidade, possuir capacidade para suportar o volume de tráfego atual e projetado, e integrar-se a uma plataforma centralizada de gerenciamento, capaz de consolidar logs, aplicar políticas, gerar alertas e fornecer relatórios detalhados sobre eventos de segurança.

4.3 No domínio da conectividade, a solução abrangerá switches de acesso e core de última geração, com suporte a funcionalidades avançadas de camada 2 e camada 3, incluindo VLANs, agregação de enlaces, protocolos de redundância, ACLs, QoS, IGMP, MLD, PoE/PoE+ e empilhamento. Esses equipamentos irão estruturar a espinha dorsal da rede da CMFOR, permitindo segmentação adequada, aumento de capacidade, maior estabilidade e expansão futura. Os switches operarão de forma integrada a uma plataforma de gerenciamento baseada em nuvem, possibilitando provisionamento automatizado, atualização centralizada, conformidade de software, definição de políticas por grupos e administração simplificada.

4.4 A solução compreenderá, ainda, a implantação de rede Wi-Fi corporativa com pontos de acesso de alto desempenho, gerenciados em ambiente de nuvem, oferecendo mobilidade, autenticação segura, controle de banda, gerenciamento centralizado e visibilidade detalhada dos usuários e dispositivos conectados. O ambiente wireless será integrado à política geral da rede, garantindo segurança, desempenho e fácil escalabilidade.

4.5 A camada de controle de acesso à rede (NAC) será responsável por autenticar usuários e dispositivos conectados tanto via cabo quanto via Wi-Fi, aplicando políticas de conformidade, bloqueando acessos irregulares, isolando dispositivos não autorizados e provendo visibilidade completa dos recursos conectados. A solução deverá suportar métodos de autenticação como 802.1X, MAC e portal cativo, integrando-se ao Active Directory e às demais plataformas de segurança.

4.6 Para proteção das aplicações expostas à internet, será incluída solução de firewall de aplicação (WAF), com capacidade de inspecionar tráfego HTTP/HTTPS, bloquear ataques direcionados a aplicações web, analisar requisições maliciosas, identificar comportamentos automatizados (bots), proteger APIs e mitigar técnicas de exploração comuns. Essa camada protege sistemas críticos, como portais institucionais, plataformas eletrônicas e serviços disponibilizados à população.

4.7 A solução incorporará também mecanismo de segurança de e-mail corporativo, responsável pela filtragem de mensagens, bloqueio de campanhas maliciosas, análise de reputação, deteção de phishing, verificação de links suspeitos e sandboxing de anexos. Esse componente é essencial para mitigar riscos provenientes do principal vetor de ataque contra instituições públicas.

4.8 Adicionalmente, será incluída solução de segurança dos dispositivos de acesso à rede, capaz de identificar comportamentos anômalos, aplicar políticas de quarentena, gerar alertas gerenciais e integrar-se ao NAC e às demais camadas de segurança. Essa funcionalidade amplia a proteção sobre notebooks, desktops e demais equipamentos corporativos.

4.9 Para garantir visibilidade plena, governança e suporte à tomada de decisão, a solução

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

incluirá plataforma integrada de monitoramento e observabilidade de rede, permitindo análise de tráfego, detecção de anomalias, acompanhamento de desempenho, geração de dashboards, emissão de alertas, consolidação de dados e diagnóstico avançado de incidentes. Essa ferramenta será crucial para suporte à operação diária e para a gestão da infraestrutura.

4.10 Todos os componentes da solução serão acompanhados de serviços de instalação, configuração, parametrização, testes, homologação e suporte técnico especializado, abrangendo atendimento remoto e presencial, manutenção preventiva e corretiva, atualização contínua de softwares, firmwares, assinaturas e licenciamento, garantindo operação ininterrupta ao longo de todo o período contratual. A solução deverá estar integralmente coberta por garantia e suporte oficial do fabricante, respeitando os níveis de serviço previstos, e deverá observar boas práticas de sustentabilidade, incluindo logística reversa, descarte ambiental adequado e eficiência energética dos equipamentos.

4.11 Consolidada em uma arquitetura integrada, padronizada e gerenciável, a solução atende às necessidades institucionais da CMFOR, elevando o nível de maturidade tecnológica, reduzindo riscos operacionais, fortalecendo a segurança cibernética e assegurando a continuidade das atividades legislativas, administrativas e de atendimento ao cidadão.

4.12 Para fins de precisão técnica e de atendimento integral às necessidades da CMFOR, todas as funcionalidades específicas, capacidades mínimas, parâmetros de desempenho, características de hardware e software, requisitos de segurança, critérios de gerenciamento, padrões de conectividade, políticas de autenticação, requisitos operacionais e demais especificações técnicas detalhadas encontram-se integralmente descritas na Especificações Técnicas, que acompanha este Termo de Referência e compõe, em conjunto, a base técnica que orienta a contratação proposta.

5. QUANTITATIVOS

ITEM	DESCRIÇÃO	UNIDADE	QTD.
1	SOLUÇÃO DE SEGURANÇA DE REDE	FORNECIMENTO	2
2	SOLUÇÃO DE CONECTIVIDADE DE REDE SEGURA – ACESSO – TIPO 1	FORNECIMENTO	20
3	SOLUÇÃO DE CONECTIVIDADE DE REDE SEGURA – ACESSO – TIPO 2	FORNECIMENTO	20
4	SOLUÇÃO DE CONECTIVIDADE DE REDE SEGURA – ACESSO – TIPO 3	FORNECIMENTO	10
5	SOLUÇÃO DE CONECTIVIDADE DE REDE SEGURA – ACESSO – TIPO 4	FORNECIMENTO	20
6	SOLUÇÃO DE CONECTIVIDADE DE REDE SEGURA – CORE	FORNECIMENTO	2
7	SOLUÇÃO DE CONECTIVIDADE DE REDE SEGURA – WI-FI	FORNECIMENTO	100
8	SOLUÇÃO DE MONITORAMENTO DE REDE	FORNECIMENTO	20
9	SOLUÇÃO DE SEGURANÇA DE ACESSO A REDE	FORNECIMENTO	2
10	SOLUÇÃO DE SEGURANÇA DAS APLICAÇÕES	FORNECIMENTO	2

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

11	SOLUÇÃO DE SEGURANÇA DE E-MAIL	FORNECIMENTO	700
12	SOLUÇÃO DE SEGURANÇA DOS DISPOSITIVOS DE ACESSO A REDE	FORNECIMENTO	700
13	SERVIÇO DE INSTALAÇÃO E PARAMETRIZAÇÃO	SERVIÇO	1
14	SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO	SERVIÇO MENSAL	12

5.1 Havendo divergência entre o sistema e o disposto nas especificações do Edital e no Termo de Referência, prevalecerão as disposições do Edital e seu Termo de Referência.

5.2 Os bens objeto desta contratação são caracterizados como comuns nos termos do inciso XIII do art. 6º c/c o art. 20 ambos da Lei nº 14.133/2021.

5.3 O critério de aceitabilidade de preços é SIGILOSO, nos termos do art. 24 da Lei nº 14.133 de 1º de abril de 2021, art. 54 do Decreto Municipal nº 15.595/2023 e art. 12, da Instrução Normativa SEGES/ME Nº 73, de 30 de setembro de 2022, sendo que os preços estimados pela administração foram fixados com base no MENOR PREÇO.

6. VIGÊNCIA DO CONTRATO

6.1 O contrato decorrente desta contratação terá vigência de **12 (doze) meses**, contados a partir da data de sua assinatura ou da emissão da ordem de serviço, podendo ser prorrogado na forma da Lei nº 14.133/2021, desde que haja interesse da Administração, seja demonstrada a vantajosidade da prorrogação e sejam mantidas as condições de habilitação da CONTRATADA.

7. MODELO DE GESTÃO DO CONTRATO

7.1 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.

7.2 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.

7.3 O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

7.4 Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

7.5 A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput).

7.6 O fiscal do contrato acompanhará a execução do contrato, para que sejam cumpridas todas

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para o Órgão.

7.7 O fiscal do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º).

7.8 Identificada qualquer inexatidão ou irregularidade, o fiscal do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção.

7.9 O fiscal 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.

7.10 No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal do contrato comunicará o fato imediatamente ao gestor do contrato.

7.11 O fiscal 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.

7.12 O fiscal administrativo do contrato verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário.

7.13 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.

7.14 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.

8. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

8.1 Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o licitante/adjudicatário que, com dolo ou culpa:

8.1.1 deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a pregoeiro/a durante o certame;
8.1.2 Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:

a) não enviar a proposta adequada ao último lance ofertado ou após a negociação;
b) recusar-se a enviar o detalhamento da proposta quando exigível;
c) pedir para ser desclassificado quando encerrada a etapa competitiva; ou
d) apresentar proposta em desacordo com as especificações do edital;

e) apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação;

f) fraudar a licitação;
g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:
h) agir em conluio ou em desconformidade com a lei;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

i) induzir deliberadamente a erro no julgamento;
j) apresentar amostra falsificada ou deteriorada;
k) praticar atos ilícitos com vistas a frustrar os objetivos da licitação;
l) praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.
m) Serão aplicadas ao licitante/adjudicatário que incorrer nas infrações acima descritas, garantida a defesa prévia, sem prejuízo das responsabilidades civil e criminal, as seguintes sanções:
   i. advertência;
   ii. multa;
   iii. impedimento de licitar e contratar e
   iv. declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.
n) Na aplicação das sanções serão considerados:
   i. a natureza e a gravidade da infração cometida.
   ii. as peculiaridades do caso concretoas circunstâncias agravantes ou atenuantes
   iii. os danos que dela provierem para a Administração Pública
   iv. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.
o) Para fins de dosimetria e cálculo das penalidades acima impostas, estas tomarão como base os parâmetros delineados no tópico a seguir.

8.2 Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o contratado que, com dolo ou culpa:
a) der causa à inexecução parcial do contrato;
b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
c) der causa à inexecução total do contrato;
d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
f) praticar ato fraudulento na execução do contrato;
g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.
i) Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:
a) Advertência, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);
b) Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);
c) Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).
d) Multa:
d.1) A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor do contrato licitado, recolhida no prazo máximo de 5 (cinco) dias úteis, a contar da comunicação oficial.
e) A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, §9º, da Lei nº 14.133, de 2021).
f) Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).
f.1.) Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) DIAS úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133, de 2021).Se a multa

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156,§8º, da Lei nº 14.133, de 2021).

g) Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

h) A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

i) Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133, de 2021):

I. a natureza e a gravidade da infração cometida;

II. as peculiaridades do caso concreto;

III. as circunstâncias agravantes ou atenuantes;

IV. os danos que dela provierem para o Contratante;

V. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

j) Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159).

k) A personalidade jurídica da contratada poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160, da Lei nº 14.133, de 2021).

l) O Contratante deverá, no prazo máximo 05 (CINCO) DIAS úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e no Cadastro Nacional de Empresas Punidas (CNEP). (Art. 161, da Lei nº 14.133, de 2021).

m) As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.

n) Os débitos da contratada para com a Administração contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o contratado possua com o mesmo órgão ora contratante.

9. REQUISITOS GERAIS DA SOLUÇÃO

9.1 Disponibilização de tecnologia atualizada, aderente às normas técnicas nacionais (incluindo homologação Anatel, quando aplicável) e internacionais, com suporte oficial do fabricante durante toda a vigência contratual.

9.2 Garantia de compatibilidade, interoperabilidade e integração nativa entre todos os módulos da solução, assegurando funcionamento coeso em arquitetura unificada.

9.3 Suporte técnico especializado 24x7 para atendimento remoto e 8x5 para atendimento

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

presencial, com níveis de serviço (SLA) definidos conforme gravidade do incidente (ex.: até 2 horas para falhas críticas).

9.4 Repasse de conhecimento à equipe técnica da CMFOR após a implantação, incluindo demonstração de funcionamento, políticas aplicadas, painéis de monitoramento e procedimentos operacionais essenciais.

9.5 Escalabilidade para ampliação futura da infraestrutura sem perda de desempenho, garantindo expansão de capacidade, cobertura e funcionalidades dentro da mesma arquitetura padronizada.Atendimento à Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018).

9.6 Critérios de Seleção e Julgamento

9.7 Tipo de Licitação: Pregão Eletrônico.

9.8 Critério de Julgamento: Menor preço global por lote.

9.9 Habilitação: Conforme Lei nº 14.133/2021, incluindo comprovação de capacidade técnica, idoneidade fiscal e trabalhista, além de atestado de execução similar.

10. REQUISITOS GERAIS DA CONTRATAÇÃO

10.1 Sustentabilidade:

10.1.1 A solução contratada deverá observar práticas de sustentabilidade, em especial:

- Fornecimento de equipamentos com eficiência energética comprovada;
- Adoção de medidas para descarte ambientalmente adequado de resíduos eletrônicos e insumos, conforme a Lei nº 12.305/2010;
- Utilização de embalagens recicláveis ou retornáveis**;**
- Disponibilização de suporte remoto sempre que possível, reduzindo deslocamentos e emissões de carbono;
- Garantia de que os serviços prestados estejam em conformidade com as normas trabalhistas, de saúde e segurança ocupacional.

10.2 Indicação de marcas ou modelo:

10.2.1 Não se aplica.

11.0 CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

11.1. Tipo de Julgamento

11.1.1 O julgamento será realizado pelo critério de MENOR PREÇO GLOBAL POR LOTE, conforme art. 33, inciso I, da Lei nº 14.133/2021, considerando todos os equipamentos, softwares e serviços descritos neste Termo de Referência.

12. DA HABILITAÇÃO

12.1. Os documentos previstos neste Termo de Referência, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021.

12.2. Os documentos de habilitação deverão ser apresentados da seguinte forma:

12.2.1. Obrigatoriamente, da mesma sede e igualdade de CNPJ, ou seja, se da matriz, todos da matriz, se de alguma filial, todos da mesma filial, com exceção dos documentos que são

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

válidos tanto para matriz como para todas as filiais. O contrato será celebrado com a sede que apresentou a documentação.

12.2.2. O documento obtido através de sítios oficiais, que esteja condicionado à aceitação via Internet, terá sua autenticidade verificada pelo(a) Pregoeiro(a).

12.2.3. Caso haja documento redigido em idioma estrangeiro, o mesmo somente será considerado se acompanhado da versão em português, firmada por tradutor juramentado.

12.2.4. O documento apresentado deverá estar dentro do prazo de validade. Na hipótese de no documento não constar expressamente o prazo de validade, este deverá ser acompanhado de declaração ou regulamentação do órgão emissor que disponha sobre sua validade. **Na ausência de tal declaração ou regulamentação, o documento será considerado válido pelo prazo de até 90 (noventa) dias, contados a partir da data de sua emissão**, quando se tratar de documentos referentes à habilitação fiscal e econômico-financeira.

12.3 HABILITAÇÃO JURÍDICA

12.3.1 A documentação relativa à habilitação jurídica consistirá em:

a) Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

b) 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;

c) Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.

d) Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

e) 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;

f) 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 5.764/1971;

12.4 QUALIFICAÇÃO TÉCNICA

12.4.1 Atestados de Capacidade Técnica

a) Para fins de habilitação, a licitante deverá apresentar 01 (um) ou mais Atestado(s) de Capacidade Técnica, emitido(s) por pessoa jurídica de direito público ou privado, que comprove(m) a execução satisfatória de fornecimento e/ou implantação de soluções, bem como a prestação de serviços compatíveis com o objeto licitado, contendo, no mínimo, a comprovação de experiência em um ou mais dos seguintes itens considerados essenciais à execução contratual:

- fornecimento de equipamentos e/ou licenças de conectividade;
- fornecimento de equipamentos de conectividade sem fio;
- fornecimento de equipamentos de segurança de perímetro;
- fornecimento de licenciamento de segurança de e-mail.

b) A exigência de comprovação de experiência nos elementos acima descritos justifica-se pela complexidade técnica e criticidade operacional do objeto, sendo indispensável para assegurar que a licitante possua capacidade técnica compatível com o porte e a natureza da contratação, mitigando riscos de indisponibilidade, falhas de integração e comprometimento da segurança do

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

ambiente, nos termos da Lei nº 14.133/2021, que autoriza a Administração a exigir qualificação técnica necessária e proporcional à adequada execução do contrato.

c) A licitante deverá disponibilizar todas as informações necessárias à verificação da legitimidade dos atestados, obrigando-se a apresentar, quando solicitada em diligência, cópia do contrato que deu suporte à contratação, notas fiscais, termos de recebimento, ordens de fornecimento/serviço ou outros documentos idôneos que comprovem a efetiva execução do objeto, conforme facultado pela Lei nº 14.133/2021.

12.4.2 Carta do Fabricante / Parceria Autorizada

a) Para fins de habilitação, a licitante deverá comprovar que é parceira, integradora, revendedora ou autorizada do(s) fabricante(s) das soluções de conectividade e segurança de acesso de e-mail ofertados, mediante apresentação de Carta do Fabricante ou documento equivalente, vigente, emitido em nome da licitante, que comprove a autorização para o fornecimento das soluções propostas.

b) A exigência da carta do fabricante fundamenta-se na necessidade de assegurar a regularidade da cadeia de fornecimento, a validade das licenças, a existência de suporte e garantia oficiais, bem como a continuidade e a segurança da execução contratual, estando em conformidade com a Lei nº 14.133/2021, por se tratar de requisito diretamente relacionado à capacidade da licitante de cumprir o objeto contratado.

12.4.3 Comprovação Técnica das Especificações

a) A licitante deverá apresentar comprovação técnica das especificações exigidas, mediante documentação oficial do fabricante e apresentação de tabela de atendimento ponto a ponto, demonstrando de forma objetiva o atendimento integral aos requisitos técnicos constantes do Termo de Referência.

b) A comprovação ponto a ponto visa assegurar o julgamento objetivo, a aderência da solução ofertada ao objeto e a seleção da proposta mais vantajosa, em observância aos princípios previstos na Lei nº 14.133/2021, especialmente os da vinculação ao instrumento convocatório e da eficiência administrativa.

12.4.4 Vistoria Técnica

a) Não será exigida a realização de avaliação ou vistoria prévia do local de execução dos serviços, por não se revelar indispensável à formulação das propostas.

12.5 HABILITAÇÕES FISCAL, SOCIAL E TRABALHISTA

12.5.1. As habilitações fiscal, social e trabalhista serão aferidas mediante a verificação dos seguintes requisitos:

a) A inscrição no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Nacional da Pessoa Jurídica (CNPJ);

b) A inscrição no cadastro de contribuintes estadual e/ou municipal, se houver, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

c) A regularidade perante a fazenda federal, estadual e/ou municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da lei;

d) A regularidade relativa à seguridade social e ao FGTS, que demonstre cumprimento dos encargos sociais instituídos por lei;

e) A regularidade 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 5.452/1943;

f) O cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal.

12.5.2. Caso o licitante seja considerado isento dos tributos estaduais e/ou municipais

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.
12.5.3. Para os Estados e Municípios que emitam prova de regularidade fiscal em separado, os proponentes deverão apresentar as respectivas certidões.
12.5.4. As microempresas e empresas de pequeno porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, § 1º da Lei Complementar nº 123, de 2006.
12.5.5. Havendo restrição quanto à regularidade fiscal e trabalhista da microempresa, da empresa de pequeno porte ou da cooperativa que se enquadre nos termos do art. 34, da Lei Federal nº 11.488/2007, será assegurado o prazo de 5 (cinco) dias úteis, contados a partir de declarado o vencedor, para a regularização do(s) documento(s), podendo tal prazo ser prorrogado por igual período, conforme dispõe a Lei Complementar nº 123/2006.
12.5.6. A não comprovação da regularidade fiscal e trabalhista, até o final do prazo estabelecido, implicará a decadência do direito, sem prejuízo das sanções cabíveis, sendo facultado ao pregoeiro convocar os licitantes remanescentes, por ordem de classificação.
12.5.7. Os documentos relativos à regularidade fiscal somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante melhor classificado.
12.5.8. Respeitada a exceção do subitem anterior, relativa à regularidade fiscal, quando a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, a verificação ou exigência do presente subitem ocorrerá em relação a todos os licitantes.

12.6 HABILITAÇÃO ECONÔMICO-FINANCEIRA

12.6.1. A habilitação econômico-financeira será aferida mediante a apresentação da seguinte documentação:

a) Certidão negativa de feitos sobre falência expedida pelo distribuidor da sede do licitante, exceto as sociedades cooperativas, conforme dispõe o art. 4º da Lei nº 5.764/1971. No caso de pessoa física ou de sociedade simples, certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante.

b) Na ausência da certidão negativa, o licitante em recuperação judicial deverá comprovar o acolhimento judicial do plano de recuperação judicial nos termos do art. 58 da Lei nº 11.101/2005. No caso do licitante em recuperação extrajudicial deverá apresentar a homologação judicial do plano de recuperação.

c) Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais que comprovem a boa situação financeira daempresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrados há mais de três meses da data da apresentação da proposta.

d) No caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos, a demonstração de resultado de exercício e demais demonstrações contábeis limitar-se-ão ao último exercício conforme dispõe o art. 69, § 6º da Lei nº 14.133/2021.

e) Tratando-se de pessoas jurídicas submetidas à Escrituração Contábil Digital (ECD) por meio do Sistema Público de Escrituração Digital (Sped), admite-se a apresentação da ECD, em observância à data limite definida nas Normas da Secretaria da Receita Federal.

f) A comprovação da boa situação financeira do licitante será atestada por documento assinado por profissional legalmente habilitado, demonstrando que a empresa apresenta índices de Liquidez Geral (LG), Liquidez Corrente (LC) e Solvência Geral (SG) superiores a 1 (um), índices calculados com base nas demonstrações contábeis dos 2 (dois) últimos exercícios sociais.

g) Caso o licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação patrimônio líquido mínimo de 10% (dez por cento) valor anual da proposta da licitante.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

g.1) 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 conforme dispõe o art. 65, §1º da Lei nº 14.133/2021.

12.7 OUTRAS EXIGÊNCIAS

a) Declarar que está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

b) Declarar que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do art. 7°, XXXIII, da Constituição;

c) Declarar que não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

d) Declarar que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da previdência social ou para aprendiz, bem como as reservas de cargo previstas em lei e em outras normas específicas.

13. CRITÉRIOS DE ACEITABILIDADE DE PREÇOS

13.1 O **orçamento estimado** para a contratação é **sigiloso**, nos termos do art. 24, § 1º, da Lei nº 14.133/2021, ficando acessível apenas aos órgãos de controle interno e externo.

13.2 Será considerada aceitável a proposta que:

a) Atenda integralmente às especificações do objeto;

b) Apresente valores compatíveis com os praticados no mercado, conforme pesquisas prévias realizadas pela Administração;

c) Não seja considerada inexequível, de acordo com o art. 59 da Lei nº 14.133/2021, presumindo-se inexequível o preço global que não seja suficiente para a cobertura dos custos diretos e indiretos necessários ao cumprimento das obrigações contratuais.

13.3 Serão desclassificadas as propostas que:

a) Contenham valores simbólicos, irrisórios ou de valor zero;
b) Apresentem preços manifestamente incompatíveis com os de mercado;
c) Não atendam às condições de execução mínima descritas neste Termo de Referência.

13.4 Estimativa do Valor da Contratação

13.4.1 A estimativa do valor da contratação foi realizada com base em:

a) **Pesquisa de preços de mercado**, mediante coleta de cotações junto a fornecedores especializados;

13.4.2 O valor estimado da contratação está registrado nos autos do processo, **mantido sob sigilo** nos termos do art. 24, §1º, da Lei nº 14.133/2021, sendo acessível apenas aos órgãos de controle interno e externo.

14. DOS RECURSOS ORÇAMENTÁRIOS

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

14.1. A despesa decorrente desta licitação correrá à conta da dotação consignada abaixo: Projeto/Atividade 01.031.0002.2783.0002 - MANUTENCAO DOS SERVICOS ADMINISTRATIVOS - Elemento de Despesa 33.90.40 – SERVICOS DE TECNOLOGIA DA INFORMACAO - Fonte de Recurso 103 do orçamento da Câmara Municipal de Fortaleza – despesas administrativas

15. DA PROVA DE CONCEITO

15.1 Não será necessária prova de conceito.

16. DA SUBCONTRATAÇÃO E PARTICIPAÇÃO EM CONSÓRCIO

16.1 Da subcontratação

16.1.1 Será admitida a subcontratação parcial do objeto, nos termos do art. 122 da Lei nº 14.133/2021, desde que previamente autorizada pela CONTRATANTE.
16.1.2 A subcontratação não poderá abranger a totalidade do objeto, nem as parcelas de maior relevância técnica e econômica, assim consideradas aquelas relacionadas ao fornecimento dos equipamentos principais e à responsabilidade técnica pela solução.

16.1.3 A CONTRATADA permanecerá integralmente responsável pela execução do contrato, inclusive quanto às obrigações assumidas por eventuais subcontratadas.

16.1.4 A subcontratação dependerá de autorização formal da fiscalização contratual, mediante apresentação da qualificação técnica da subcontratada compatível com a parcela a ser executada.

16.1.5 É vedada a subcontratação para mera intermediação de mão de obra ou transferência integral da execução contratual.

16.2. Da participação em Consórcio

16.2.1. É vedada participação em Consórcio
16.2.2 A participação de empresas reunidas em consórcio será vedada na presente contratação, tendo em vista a natureza e as características do objeto. A admissão de consórcios poderia comprometer a unidade do sistema, gerar dificuldades na integração tecnológica e aumentar os riscos de falhas operacionais.
16.2.3 Além disso, a vedação justifica-se pela necessidade de responsabilização direta e exclusiva da empresa contratada, o que se tornaria mais complexo em arranjos consorciados. Em tais casos, a fiscalização e o acompanhamento da execução ficariam sujeitos a eventuais conflitos internos entre consorciadas, fragilizando o controle da Administração sobre a execução contratual.

17. DAS CONDIÇÕES E PRAZOS DE EXECUÇÃO DO CONTRATO

Local de execução dos Serviços

17.1 Os serviços deverão ser executados nas dependências da Câmara Municipal de Fortaleza – CMFOR, bem como em seus anexos e áreas complementares, nos seguintes endereços:
17.1.1 Sede da Câmara Municipal de Fortaleza, situada na Rua Dr. Thompson Bulcão, nº 830, Bairro Luciano Cavalcante, Fortaleza – CE;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

17.1.2 Prédio anexo da Câmara Municipal de Fortaleza, localizado na Avenida Rogaciano Leite, nº 1040, Bairro Guararapes, Fortaleza – CE.
17.2. A CONTRATADA deverá assegurar que todos os serviços sejam prestados sem prejuízo das atividades institucionais da Câmara, observando os horários, normas internas de segurança e demais orientações fornecidas pela fiscalização contratual.

17.3. Da Entrega dos Equipamentos

17.3.1. Os equipamentos, objeto do contrato, deverão ser entregues pela CONTRATADA no prazo máximo de 45 (quarenta e cinco) dias corridos, contados a partir da emissão da **ORDEM DE SERVIÇO** ou do instrumento equivalente.

17.3.2. A entrega dos equipamentos deverá ocorrer nos endereços indicados no item 17.1 deste instrumento, em dias e horários previamente acordados com a fiscalização contratual, observadas as normas internas de acesso, segurança e funcionamento da CONTRATANTE.

17.3.3. Os equipamentos entregues deverão ser **novos, de primeiro uso**, originais do fabricante, acompanhados de manuais, licenças, garantias e demais documentos técnicos exigidos no Termo de Referência.

17.3.4. A entrega será formalizada mediante **recebimento provisório**, nos termos do art. 140 da Lei nº 14.133/2021, para fins de conferência quantitativa e verificação inicial de conformidade.

17.3.5. Constatada qualquer desconformidade, a CONTRATADA será notificada para promover a substituição, correção ou complementação dos equipamentos no prazo máximo de 10 (dez) dias, às suas expensas, sem prejuízo da aplicação das penalidades cabíveis.

17.3.6. O recebimento definitivo dos equipamentos ocorrerá após a verificação da conformidade técnica, funcional e documental, mediante emissão de termo próprio pela fiscalização contratual.

Forma de execução, acompanhamento e fiscalização da prestação dos serviços

17.4 A execução do objeto, compreendendo o fornecimento dos equipamentos e a prestação dos serviços, poderá ser feita de forma fracionada ou em sua totalidade, de acordo com a necessidade do órgão interessado durante o prazo de contratação, mediante a expedição de Ordens de Fornecimento (para os bens) e/ou Ordens de Serviço (para os serviços) pelo órgão demandante, constando a relação, quantidade e especificações dos itens a serem entregues ou executados.

17.5 A execução dos serviços será acompanhada e fiscalizada por servidor do órgão demandante, o qual deverá atestar os documentos da despesa, quando comprovada a fiel e correta entrega para fins de pagamento.

17.6 A presença da fiscalização do órgão demandante não elide nem diminui a responsabilidade da empresa contratada.

17.7 Caberá ao servidor designado rejeitar totalmente ou em parte, qualquer bem que não esteja de acordo com as exigências, bem como, determinar prazo para readequação de serviço eventualmente fora de especificação.

18. PRAZO PARA INÍCIO

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

18.1 Os serviços deverão ser iniciados no prazo de até **15 (quinze) dias corridos**, a contar da emissão da **ORDEM DE SERVIÇO**, **que será enviada à contratada através de e-mail** ou outro meio que comprove o seu recebimento.

18.2 A demanda correspondente a **ORDEM DE SERVIÇO** deverá ser entregue em remessa única.

18.3 Caso não seja possível o início da realização dos serviços na data assinalada, a empresa deverá comunicar as razões respectivas com pelo menos 03 (três) dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

19. DA FORMA DE EXECUÇÃO DO OBJETO E PAGAMENTO

Da forma de execução (provisório e definitivo)

19.1 O fornecimento dos bens e a execução dos serviços serão realizados conforme condições editalícias. Para o faturamento, será apresentada nota fiscal ou instrumento de cobrança equivalente, distingindo-se:

19.1.1 Para os Bens (Itens 1 a 12): A nota fiscal deverá acompanhar o termo de recebimento provisório e definitivo, conforme Item 17.3.

19.1.2 Para os Serviços (Itens 13 e 14): A nota fiscal deverá ser atestada pelo fiscal do contrato mediante medição mensal ou conforme cronograma de execução, verificando-se o cumprimento dos SLAs e metas estabelecidas.

19.2 Os serviços poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 02 (dois) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

19.3 O prazo para execução dos serviços poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

19.4 O prazo para a solução, pelo contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Órgão durante a análise prévia à liquidação de despesa, não será computado para os fins de execução do objeto.

19.5 A execução provisória ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

19.6 Pós conclusão dos procedimentos quanto a prestação dos serviços, serão realizados os atos correspondentes a liquidação e pagamento da despesa.

20. FORMA DE PAGAMENTO (art. 40, §2º, V)

20.1. O pagamento será efetuado até **30 (trinta) dias** contados da data da apresentação da nota fiscal/fatura devidamente atestada pelo fiscal da contratação, mediante crédito em conta corrente em nome da CONTRATADA.

20.1.1. A nota fiscal/fatura que apresente incorreções será devolvida à contratada para as devidas

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

correções. Nesse caso, o prazo de que trata o subitem anterior começará a fluir a partir da data de apresentação da nota fiscal/fatura corrigida.

20.2. Não será efetuado qualquer pagamento à contratada, em caso de descumprimento das condições de habilitação e qualificação exigidas na licitação.

20.3. É vedada a realização de pagamento antes da execução do objeto ou se o mesmo não estiver de acordo com as especificações deste instrumento.

20.4. Os pagamentos encontram-se ainda condicionados à apresentação dos seguintes comprovantes:

20.4.1. Documentação relativa à regularidade para com a Seguridade Social (INSS), Fundo de Garantia por Tempo de Serviço (FGTS), trabalhista e Fazendas Federal, Estadual e Municipal.

20.5. Toda a documentação exigida deverá ser apresentada em original ou por qualquer processo de reprografia, obrigatoriamente autenticada em cartório ou autenticação digital. Caso esta documentação tenha sido emitida pela Internet, só será aceita após a confirmação de sua autenticidade.

20.6. Caso o prazo exceda a 12 (doze) meses, os preços contratuais serão reajustados, contado da data do orçamento estimado, mediante aplicação do índice de Preços ao Consumidor Amplo – IPCA/IBGE, em conformidade com a legislação em vigor, tomando-se por base o índice vigente no mês de apresentação da proposta a que essa se referir.

20.7. Poderá haver revisão de preços na hipótese de ocorrência de fatos imprevisíveis ou previsíveis, porém de consequências incalculáveis durante a gestão contratual, bem como ocorra majoração legal de preços; devendo a Contratada se manifestar e, comprovadamente, demonstrar o desequilíbrio econômico-financeiro do contrato.

21. DAS OBRIGAÇÕES DA CONTRATADA

21.1. Prestar os serviços em conformidade com as condições deste contrato e do Termo de Referência.

21.2. Manter durante toda a execução do objeto, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

21.3. Aceitar, nas mesmas condições contratuais, os percentuais de acréscimos ou supressões limitadas ao estabelecido no art. 125, da Lei Federal nº 14.133/2021, tomando-se por base o valor inicial atualizado do contrato.

21.4. Responsabilizar-se pelos danos causados diretamente à contratante ou a terceiros, decorrentes da sua culpa ou dolo, quando da execução do objeto, não podendo ser arguido para efeito de exclusão ou redução de sua responsabilidade o fato de a contratante proceder à fiscalização ou acompanhar a execução contratual.

21.5. Responder por todas as despesas diretas e indiretas que incidam ou venham a incidir sobre a execução contratual, inclusive as obrigações relativas a salários, previdência social, impostos, encargos sociais e outras providências, respondendo obrigatoriamente pelo fiel cumprimento das leis trabalhistas e específicas de acidentes do trabalho e legislação correlata, aplicáveis ao pessoal empregado na execução contratual.

21.6. Prestar imediatamente as informações e os esclarecimentos que venham a ser solicitados pela contratante, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidas no prazo de 24 (vinte e quatro) horas.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

21.7. Reparar, corrigir, remover, reconstruir ou substituir, imediatamente, à suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados, ou em desconformidade com as especificações deste termo.

21.8. Cumprir, quando for o caso, as condições de garantia do objeto, responsabilizando-se pelo período oferecido em sua proposta comercial, observando o prazo mínimo exigido pela Administração.

21.9. Providenciar a substituição de qualquer profissional envolvido na execução do objeto contratual, cuja conduta seja considerada indesejável pela fiscalização da CONTRATANTE.

21.10. É de responsabilidade da CONTRATADA, estar em conformidade com os fundamentos da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), no que tratar-se da manipulação dos dados da CONTRATANTE e de terceiros, em sua criptografia, armazenamento e demais tratativas resguardando os dados utilizados, ficando vedado o tratamento de dados pessoais sensíveis por parte da CONTRATADA com objetivo de obter vantagem econômica de qualquer espécie, com exceção daquelas hipóteses previstas no parágrafo 4º do art. 11 da Lei nº 13.709, de 14 de agosto de 2018.

21.11**.** Cumprir as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

21.12**.** Assumir total responsabilidade pelo sigilo das informações, dados, nos termos da Lei Geral de Proteção de Dados - LGPD (Lei nº 13.709/2018), contidos em quaisquer mídias e documentos que seus empregados ou prepostos vierem a obter em função dos serviços prestados à CONTRATANTE, respondendo pelos danos que eventual vazamento de informações, decorrentes de ação danosa ou culposa, nas formas de negligência, imprudência ou imperícia, venha a ocasionar à CONTRATANTE.

21.13. Assumir total responsabilidade pelo sigilo das informações, dados, contidos em quaisquer mídias e documentos que seus empregados ou prepostos vierem a obter em função dos serviços prestados à CONTRATANTE, respondendo pelos danos que eventual vazamento de informações, decorrentes de ação danosa ou culposa, nas formas de negligência, imprudência ou imperícia, venha a ocasionar à CONTRATANTE.

21.14. A Contratada deverá disponibilizar, durante a vigência do contrato, mão de obra capacitada, idônea e experiente, de modo a reunir permanentemente em serviço equipe homogênea e suficiente de técnicos, que possa assegurar a prestação satisfatória dos serviços.

21.15. A CONTRATADA será responsável pela administração e manutenção do serviço em regime de 24x7x365 para atendimentos remotos e o regime 8x5 para atendimentos que possam ser necessários na forma presencial, durante todo o período do serviço contemplado nesse termo.

21.16. As tarefas atinentes ao transporte, deslocamento e remessa necessários, seja na implementação, substituição e/ ou remoção de equipamentos defeituosos será de responsabilidade da CONTRATADA.

21.17. Para garantir a qualidade e disponibilidade do serviço, deverá ser disponibilizado pela empresa CONTRATADA uma ferramenta de visibilidade e monitoramento com estrutura dedicada para a CONTRATANTE. A ferramenta deve ser acompanhada de todos os itens necessários para operacionalização, tais como: softwares de apoio (sistema operacional, etc) e licenças de softwares;

21.18. O serviço de monitoramento 24x7 deverá ser prestado OBRIGATÓRIA E INDISPENSAVELMENTE através de NOCs (Network Operation Center) redundantes da empresa CONTRATADA que já deverão estar em pleno funcionamento até a data da assinatura do contrato. Será o ponto único de contato com a equipe técnica da CONTRATANTE para abertura

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

de chamados, incidentes, problemas, dúvidas e requisições relacionadas aos serviços contratados, atuando como a primeira instância de atendimento à CONTRATANTE.

21.19. Os serviços prestados pelo NOC compreendem, entre outros, os seguintes procedimentos:

21.19.1. Suporte técnico para identificação e resolução de problemas em software e hardware;

21.19.2. Resolução de problemas quanto acesso à internet, sites remotos, serviços de rede oferecidos aos funcionários do CONTRATANTE;

21.19.3. Suporte em criação de políticas, configurações, parametrizações de quaisquer ordens relativos aos equipamentos ofertados;

21.19.4. Resolução de problemas referente a políticas, configurações, parametrizações de quaisquer ordens relativos aos equipamentos ofertados;

21.19.5. Suporte à criação, geração e parametrização de relatórios e eventos de segurança/rede de quaisquer naturezas detectados e prevenidos pelos equipamentos ofertados;

21.19.6. Encaminhar incidentes ao fabricante da solução;

21.19.7. Suporte em demais configurações de segurança, redundância e gerência;

21.19.8. Suporte, administração e monitoramento das políticas e tarefas de backup das configurações;

21.19.9. Apoio técnico para tarefas de auditoria e análise de logs.

21.20. A CONTRATADA deverá agir de forma reativa para incidentes, restabelecimento do serviço o mais rápido possível minimizando o impacto, seja por meio de uma solução de contorno ou definitiva. Ainda caberá a CONTRATADA agir de forma proativa aplicando medidas para a boa manutenção afim de garantir a regularidade da operação do serviço.

21.21. O atendimento e suporte técnico especializado de 1º (primeiro nível) será sempre telefônico e remoto em regime 24x7 e assim, responsável pelo acompanhamento e gestão dos chamados, controle dos indicadores de monitoramento, atuando como ponto único de contato entre a CONTRATANTE e profissionais da equipe da CONTRATADA.

21.22. O atendimento e suporte técnico especializado de 2º (segundo nível) poderá ser presencial ou remoto em regime 8x5 em Fortaleza/CE, caso o suporte remoto não seja suficiente para resolução do problema. Responsável pela prevenção e resolução de incidentes, problemas e requisições, identificando a causa raiz de eventual problema e buscando sua solução. Execução de atividades remotas e/ou presenciais em incidentes, solicitações de maior complexidade.

21.23. Os técnicos deverão ser capacitados e certificados para prestação dos serviços, resolução de incidentes, problemas e solicitações nos equipamentos ofertados. O comparecimento de um técnico ao local da necessidade será de no máximo 48 (quarenta e oito) horas para atendimentos na área que abrange e define a Região Metropolitana de Fortaleza devendo sempre atender aos critérios de SLA determinados nesse termo.

21.24. Para abertura dos chamados de suporte, a CONTRATADA deverá disponibilizar número telefônico 0800 (ou equivalente a ligação local), também serviço via portal WEB e/ou e-mail (em português). Na abertura do chamado, o órgão ao fazê-lo, receberá naquele momento, o número, data e hora de abertura do chamado. Este será considerado o início para contagem dos SLAs. O fechamento do chamado deverá ser comunicado pela CONTRATADA para fins de contagem do tempo de atendimento e resolução do chamado.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

21.26. A atualização de firmware quando disponibilizado exclusivamente pelo próprio fabricante dos equipamentos deverá ser executada pela CONTRATADA sem custo adicional, sempre que requisitado pela CONTRATANTE. Toda e qualquer atualização só poderá ser aplicada mediante autorização da CONTRATANTE. As atualizações deverão ocorrer em data e horário determinado pela CONTRATADA em comum acordo e autorização da CONTRATANTE visando manter em normal funcionamento a rede onde estiverem funcionando.

21.27. A CONTRATADA deverá fornecer informações de monitoramento on-line, via dashboard que permita o acompanhamento em tempo real do estado dos ativos. Deverá ainda apresentar relatórios mensais, por meio digital (DOCX, XLSX ou PDF), com o diagnóstico e controle dos equipamentos monitorados (dados, informações, descrição, indicadores e métricas que permitam quantificar o desempenho e a disponibilidade da operação do serviço).

21.28. A CONTRATADA deverá disponibilizar uma ferramenta de Service Desk comprovadamente aderente as boas práticas do ITIL e que contenha o detalhamento dos chamados com no mínimo as seguintes informações: o funcionário do órgão/entidade que realizou a abertura do chamado, data e hora de abertura, data e hora de atendimento, data e hora de solução, o funcionário do órgão/entidade que realizou o encerramento do chamado, descrição detalhada do problema e das ações tomadas para sua resolução e a relação dos equipamentos ou componentes substituídos, especificando marca, modelo, fabricante e número de série).

21.29. A CONTRATADA deverá comunicar ao CONTRATANTE, os casos de eminente falha operacional dos equipamentos ou de qualquer outra ação que possa vir a colocar em risco a operação da rede dela, mesmo que a falha não tenha sido consumada, mas que tenha sido detectada a existência do risco.

21.30. A CONTRATADA deverá respeitar os tempos máximos de ATENDIMENTOS e SLA (Nível de Acordo de Serviço) abaixo descritos, sob a pena de multa no caso de falhas em seu integral cumprimento:

21.30.1. Operação parada (incidente que gere parada total de algum serviço contemplado nesse contrato) o tempo de atendimento será de até 2 (duas) horas.

21.30.2. Operação impactada (incidente que gere parada parcial de algum serviço contemplado nesse contrato) o tempo de atendimento será de até 4 (quatro) horas.

21.30.3. Requisição de serviço (solicitações de mudanças nos equipamentos ou serviços do contrato) o tempo de atendimento será de até 8 (oito) horas.

21.30.4. Informações de contrato (solicitação de informação, parecer ou relatório de algum serviço contemplado no contrato) o tempo de atendimento será de até 12 (doze) horas.

21.31**.** Entregar o produto/prestar o serviço, onde o mesmo deverá obedecer às exigências contidas nas especificações deste Termo de Referência, bem como todas e quaisquer normas ou regulamentações intrínsecas ao tipo de fornecimento.

21.32. É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

21.33. Assumir inteira responsabilidade por qualquer extravio causado durante o transporte e demais serviços pertinentes ao fornecimento, devendo comunicar ao fiscal do Contrato, tempestivamente, a fim de que sejam adotadas as providências.

21.34. Não transferir a outrem, no todo ou em parte, a execução do objeto, sob pena de responsabilidade.

21.35. Manter, durante todo o período de vigência Contrato a ser firmado, um preposto aceito pela Contratante, para representação da Contratada sempre que for necessário e comunicando, por escrito, à Contratante qualquer mudança de endereço ou telefone de contato.

22. DAS OBRIGAÇÕES DA CONTRATANTE:

22.1 Solicitar a execução do objeto à CONTRATADA através da emissão de Ordem de Serviço, nota de empenho ou documento equivalente.

22.2. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, em conformidade com o Edital e seus anexos.

22.3. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

22.4. Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

22.5. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;

22.6. Comunicar a empresa para emissão de Nota Fiscal em relação à incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021;

22.7. Efetuar o pagamento ao Contratado do valor correspondente a execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência;

22.8. Aplicar ao Contratado as sanções previstas na Lei nº 14.133, de 2021 e neste Contrato;

22.9. Cientificar os órgãos responsáveis para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado;

22.10. Emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

22.11. Responder eventuais pedidos de restabelecimento do equilíbrio econômico-financeiro feitos.

22.12. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

22.13. A Administração não responderá por quaisquer compromissos assumidos pelo Contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do Contratado, de seus empregados, prepostos ou subordinados.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

22.14. A Contratante se compromete a zelar pelo tratamento dos dados pessoais dos titulares, pessoas naturais vinculadas à Contratada, sem prejuízo de qualquer responsabilidade, admitindo-se o tratamento nas hipóteses de consentimento específico e destacado por termo de compromisso e ou nas hipóteses previstas nos incisos II a X do art. 7º da Lei Federal nº 13709, de 14 de agosto de 2018, quando for o caso.

22.15. Fica vedado o tratamento de dados pessoais sensíveis por parte do CONTRATANTE com objetivo de obter vantagem econômica de qualquer espécie, com exceção daquelas hipóteses previstas no parágrafo 4º do art. 11 da Lei Federal nº 13.709, de 14 de agosto de 2018, quando for o caso.

22.16. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, em conformidade com o Edital e seus anexos.

22.17. Receber o objeto no prazo e condições estabelecidas no Termo de Referência.

22.18. A CONTRATANTE poderá solicitar qualquer relatório ou informação de qualquer parte da solução com uma frequência mensal o que deverá ser provido pela contratada num prazo de 5 dias úteis.

22.19. Os relatórios de chamados abertos poderão ser solicitados a qualquer instante pela CONTRATANTE dentro das condições estipuladas, respeitando, no entanto, um prazo de até 48 (quarenta e oito) horas uteis. Esses relatórios deverão ser retidos pelo tempo mínimo equivalente a vigência do contrato e após o seu encerramento inutilizados.

22.20. A CONTRATANTE deverá definir pessoas do seu Quadro de Funcionários que terão acesso de Administração nos equipamentos disponibilizados e essas pessoas deverão comunicar à empresa CONTRATADA qualquer alteração de configuração realizada nos equipamentos fornecidos nessa contratação e nessa situação respondendo por sua conta e risco pelas intervenções que possam ter efetuado.

23. DOS CASOS OMISSOS (art. 92, III)

23.1. Os casos omissos serão decididos pelo(s) órgão(s) demandante(s), segundo as disposições contidas na Lei nº 14.133, de 2021, nos regulamentos e normas locais específicas, nas normas federais aplicáveis e, subsidiariamente, pelas normas e princípios gerais em Direito Admitidas.

24. PROPRIEDADE, LICENCIAMENTO E CONFIDENCIALIDADE

24.1. Os equipamentos, sistemas e demais bens tecnológicos fornecidos no âmbito desta contratação serão entregues em regime de aquisição definitiva, com transferência de propriedade à CONTRATANTE após o recebimento definitivo, nos termos do art. 140 da Lei nº 14.133/2021, passando a integrar o patrimônio da Câmara Municipal de Fortaleza.

24.2. Os softwares embarcados nos equipamentos, bem como as respectivas licenças, assinaturas, subscrições e funcionalidades baseadas em nuvem associadas à solução, serão fornecidos na modalidade de cessão de direito de uso, observadas as condições estabelecidas pelo fabricante e as especificações técnicas constantes deste Termo de Referência.

Parágrafo único. As licenças, subscrições e garantias do fabricante deverão possuir validade mínima de 36 (trinta e seis) meses, independentemente da vigência contratual, conforme especificações técnicas da solução.

24.3. Todos os dados, imagens, informações, registros e relatórios captados, processados ou armazenados pelos equipamentos e sistemas durante a execução deste contrato são de propriedade exclusiva da CONTRATANTE, que poderá utilizá-los livremente para fins institucionais, de segurança, controle de acesso e gestão administrativa, nos termos da legislação aplicável.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

24.4. A CONTRATADA deverá assegurar a integridade, confidencialidade e inviolabilidade das informações tratadas no âmbito da execução contratual, sendo vedado o uso, cópia, compartilhamento, divulgação ou armazenamento fora do ambiente autorizado pela CONTRATANTE, salvo mediante autorização formal.

24.5. As licenças de software, assinaturas, subscrições e funcionalidades baseadas em nuvem associadas aos itens constantes da tabela de quantitativos deverão permanecer válidas **pelo prazo mínimo de 12 (doze) meses**, contado a partir da data de aceite definitivo da implantação, sendo de responsabilidade da CONTRATADA sua ativação, suporte e atualização durante a vigência contratual, sem ônus adicional para a CONTRATANTE.

24.6. Em caso de prorrogação contratual, esta abrangerá tanto o serviço continuado de monitoramento e suporte técnico quanto a renovação automática das licenças de software, assinaturas, subscrições e garantias do fabricante associadas aos equipamentos e soluções fornecidas, cujos termos e condições comerciais deverão ser mantidos, salvo manifestação em contrário da CONTRATANTE com antecedência mínima de 60 (sessenta) dias do término do período vigente.

24.7. Ao término do contrato, a CONTRATANTE permanecerá com a propriedade plena dos equipamentos físicos adquiridos, podendo optar pela contratação direta junto ao fabricante ou mediante nova licitação para renovação de licenças, garantias e suporte técnico, conforme sua conveniência administrativa.

25. DO SUPORTE TÉCNICO, DA MANUTENÇÃO E DA CAPACITAÇÃO

25.1. O suporte técnico prestado durante o período de garantia não incluirá evoluções tecnológicas, novas funcionalidades, atualizações de versão ou quaisquer melhorias que caracterizem desenvolvimento adicional do sistema, salvo se expressamente previstas neste Termo de Referência ou contratadas posteriormente por instrumento próprio.

25.2. Durante a vigência da garantia, a Contratada deverá, ainda, prestar treinamento inicial e operação assistida para os sistemas implantados, em formato presencial, remoto ou híbrido, conforme definido pela Administração, com o objetivo de capacitar a equipe interna e promover sua autonomia operacional.

25.3. Todas as obrigações previstas nesta cláusula deverão ser cumpridas sem ônus adicional para a Administração, observadas as condições e os limites estabelecidos neste Termo de Referência e na proposta comercial apresentada pela Contratada.

26. JUSTIFICATIVA DE CONTRATAÇÃO EM LOTE ÚNICO

A definição da contratação em lote único decorre da natureza integrada do objeto, que não se limita ao fornecimento isolado de bens ou à prestação pontual de serviços, mas consiste na implementação de uma solução tecnológica sistêmica destinada à modernização, padronização, operação e gestão da infraestrutura de rede, conectividade sem fio e segurança da informação da Câmara Municipal de Fortaleza. Trata-se de um ambiente concebido para funcionar de forma coordenada, cuja eficiência depende da integração plena entre equipamentos, softwares e serviços especializados.

Os itens previstos no Termo de Referência apresentam interdependência técnica e funcional, compondo uma única arquitetura lógica e operacional. As soluções de conectividade (acesso, core e Wi-Fi corporativo) articulam-se diretamente com as soluções de segurança de rede, segurança de acesso à rede, proteção de aplicações, segurança de e-mail e dispositivos, bem como com as plataformas de monitoramento e observabilidade, compartilhando políticas, dados, eventos e mecanismos de resposta a incidentes. Nesse contexto, a fragmentação do objeto

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

comprometeria a interoperabilidade das soluções, ampliaria o risco de incompatibilidades técnicas e prejudicaria a efetividade do conjunto contratado.

Além disso, a contratação por múltiplos lotes ou fornecedores distintos acarretaria complexidade excessiva na gestão contratual, com sobreposição de escopos, multiplicidade de interlocutores e dificuldade de atribuição de responsabilidades técnicas, sobretudo em situações de falha, degradação de desempenho ou incidentes de segurança. Em contrapartida, a contratação em lote único assegura centralização da gestão e da responsabilidade técnica, permitindo fiscalização mais eficiente, aplicação objetiva de níveis de serviço e maior segurança administrativa quanto à execução integral do objeto

Sob a perspectiva econômica, a adoção do lote único revela-se mais vantajosa à Administração, na medida em que promove a economicidade e a racionalidade do gasto público, ao reduzir custos indiretos de gestão contratual, evitar a duplicidade de licenças, integrações e ferramentas tecnológicas, bem como viabilizar ganhos de escala na formação do preço global. Ademais, a padronização tecnológica, na medida do tecnicamente viável, decorrente dessa opção, contribui para simplificar futuras expansões, manutenções e evoluções do ambiente, assegurando maior previsibilidade orçamentária, sustentabilidade do investimento e eficiência ao longo de todo o ciclo de vida da solução.

Do ponto de vista jurídico, a opção pelo lote único encontra respaldo na Lei nº 14.133/2021, que orienta as contratações públicas pelos princípios do planejamento, da eficiência e da governança, não impondo a divisão do objeto quando esta se revelar prejudicial à execução contratual ou ao interesse público. No caso concreto, a contratação integrada mostra-se medida necessária, proporcional e devidamente motivada, não configurando restrição indevida à competitividade, mas sim solução que melhor atende à segurança, à eficiência administrativa e à continuidade dos serviços institucionais da Câmara Municipal de Fortaleza.

27. JUSTIFICATIVA PARA A UTILIZAÇÃO DO SISTEMA DE REGISTRO DE PREÇOS

A contratação pretendida tem por objeto a seleção, por meio do Sistema de Registro de Preços, de empresa especializada para o fornecimento de soluções tecnológicas de segurança, conectividade e Rede Wi-Fi Corporativa, compreendendo tanto o fornecimento de equipamentos e demais itens de aquisição quanto a prestação de serviços técnicos especializados destinados à implantação, modernização, operação e gestão da infraestrutura de rede sem fio da Sede e do Prédio Anexo da Câmara Municipal de Fortaleza, razão pela qual a adoção do Sistema de Registro de Preços revela-se juridicamente adequada e tecnicamente recomendável diante das características do objeto e da natureza das necessidades institucionais envolvidas.

Nos termos do art. 82 da Lei nº 14.133/2021, o Sistema de Registro de Preços constitui instrumento legítimo para contratações em que a Administração Pública não consegue definir previamente, com exatidão, os quantitativos a serem demandados ao longo do período de vigência, ou quando a necessidade de contratação se apresenta de forma recorrente, variável ou condicionada a fatores supervenientes, circunstância que se verifica no presente caso, uma vez que as soluções de conectividade, segurança da informação e rede Wi-Fi corporativa envolvem elementos tecnológicos de elevado custo, cujo desembolso integral e imediato acarretaria significativo impacto orçamentário, sendo, portanto, mais vantajoso sob o aspecto econômico e mais compatível com o adequado planejamento administrativo e orçamentário realizar a contratação de forma parcelada, conforme a efetiva necessidade e a disponibilidade dos recursos públicos.

Com efeito, a natureza do objeto, que contempla majoritariamente itens de aquisição, recomenda a adoção da contratação de forma parcelada, uma vez que a contratação integral dos quantitativos não se mostra compatível com a dinâmica das necessidades institucionais,

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

revelando-se mais adequada a execução gradual das contratações ao longo da vigência da ata, em estrita observância à disponibilidade dos recursos orçamentários futuros, de modo a assegurar o adequado planejamento financeiro, evitar a assunção de compromissos orçamentários desnecessários e preservar a responsabilidade fiscal da Administração Pública.

Nesse contexto, o Sistema de Registro de Preços apresenta-se como solução adequada, na medida em que permite à Administração realizar contratações de forma parcelada e sob demanda, conforme a efetiva necessidade e a disponibilidade orçamentária, sem a imposição de aquisição imediata ou integral dos itens registrados, assegurando, assim, maior racionalidade no emprego dos recursos públicos e preservando a flexibilidade indispensável à gestão da infraestrutura tecnológica do órgão.

Sob a perspectiva da eficiência e da economicidade, a adoção do SRP contribui para a redução da repetição de procedimentos licitatórios voltados a objetos de natureza homogênea, ao mesmo tempo em que otimiza o planejamento das contratações e possibilita a obtenção de preços previamente registrados em ambiente competitivo, evitando aquisições antecipadas ou desnecessárias e garantindo que os recursos públicos sejam empregados apenas quando houver demanda concreta, em consonância com os princípios da boa governança e do interesse público.

Cumpre destacar, ademais, que as soluções objeto da contratação possuem caráter estratégico e essencial para o funcionamento regular das atividades legislativas, administrativas e institucionais da Câmara Municipal de Fortaleza, de sorte que eventual indisponibilidade ou fragilidade da infraestrutura de conectividade e segurança da informação pode comprometer a continuidade dos serviços públicos, a integridade das informações e o adequado suporte às atividades finalísticas do órgão, motivo pelo qual o Sistema de Registro de Preços, ao viabilizar respostas mais céleres às necessidades supervenientes, contribui para a mitigação de riscos operacionais e para o fortalecimento da continuidade e da confiabilidade dos serviços prestados.

Dessa forma, a opção pelo Sistema de Registro de Preços mostra-se plenamente alinhada aos princípios que regem as contratações públicas, notadamente os princípios do planejamento, da eficiência, da economicidade, da segurança jurídica e da supremacia do interesse público, todos expressamente consagrados na Lei nº 14.133/2021, encontrando a motivação administrativa respaldo tanto na legislação vigente quanto nas boas práticas de gestão pública, o que evidencia que o SRP constitui o instrumento mais adequado para atender às necessidades da Câmara Municipal de Fortaleza no que se refere à contratação de soluções tecnológicas de segurança, conectividade e rede Wi-Fi corporativa.

Diante de todo o exposto, resta devidamente justificada, sob os aspectos jurídico e técnico, a adoção do Sistema de Registro de Preços para a presente contratação, por se tratar de mecanismo apto a assegurar flexibilidade, eficiência, economicidade e continuidade dos serviços essenciais, em estrita consonância com a legislação aplicável e com as necessidades institucionais do órgão.

28. DOS ANEXOS:

- **ANEXO I – ESPECIFICAÇÕES TÉCNICAS DETALHADAS (LOTE ÚNICO)**
- **ANEXO A - PLATAFORMA DE MONITORAMENTO**

ELABORADO POR: Henrique Nogueira da Gama Mota - Coordenador Coid

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

ANEXO I

ESPECIFICAÇÕES TÉCNICAS DETALHADAS – LOTE ÚNICO

OBJETO: Constitui objeto da presente licitação a contratação, por meio de sistema de registro de preços, de empresa especializada para fornecimento de soluções tecnológicas de segurança, conectividade e rede wi-fi corporativa, abrangendo serviços técnicos especializados, destinados à implantação, modernização, operação e gestão da infraestrutura de rede sem fio da sede e do prédio anexo da Câmara Municipal de Fortaleza.

TABELA DE ITENS

ITEM	DESCRITIVO	UNIDADE DE FORNECIMENTO	QTD.
1	SOLUÇÃO DE SEGURANÇA DE REDE	FORNECIMENTO	2
2	SOLUÇÃO DE CONECTIVIDADE DE REDE SEGURA – ACESSO – TIPO 1	FORNECIMENTO	20
3	SOLUÇÃO DE CONECTIVIDADE DE REDE SEGURA – ACESSO – TIPO 2	FORNECIMENTO	20
4	SOLUÇÃO DE CONECTIVIDADE DE REDE SEGURA – ACESSO – TIPO 3	FORNECIMENTO	10
5	SOLUÇÃO DE CONECTIVIDADE DE REDE SEGURA – ACESSO – TIPO 4	FORNECIMENTO	20
6	SOLUÇÃO DE CONECTIVIDADE DE REDE SEGURA – CORE	FORNECIMENTO	2
7	SOLUÇÃO DE CONECTIVIDADE DE REDE SEGURA – WI-FI	FORNECIMENTO	100
8	SOLUÇÃO DE MONITORAMENTO DE REDE	FORNECIMENTO	20
9	SOLUÇÃO DE SEGURANÇA DE ACESSO À REDE	FORNECIMENTO	2
10	SOLUÇÃO DE SEGURANÇA DAS APLICAÇÕES	FORNECIMENTO	2
11	SOLUÇÃO DE SEGURANÇA DE E-MAIL	FORNECIMENTO	700
12	SOLUÇÃO DE SEGURANÇA DOS DISPOSITIVOS DE ACESSO À REDE	FORNECIMENTO	700
13	SERVIÇO DE INSTALAÇÃO E PARAMETRIZAÇÃO	SERVIÇO	1

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

14	SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO	SERVIÇO MENSAL	12

1. ESPECIFICAÇÕES TÉCNICAS

1.1 CONDIÇÕES COMUNS A TODOS OS ITENS

1.1.1 Todos os itens contemplados neste edital deverão ser fornecidos com licenciamento, assinaturas, subscrições, serviços contratados e/ou quaisquer mecanismos de habilitação necessários ao pleno funcionamento das soluções, pelo prazo mínimo de 36 (trinta e seis) meses, contados a partir da data de aceite definitivo da implantação pela CONTRATANTE, com previsão de renovação automática nas mesmas condições comerciais em caso de prorrogação contratual, salvo manifestação em contrário da CONTRATANTE com antecedência mínima de 60 (sessenta) dias do término do período vigente.

1.1.2 Durante todo o período da vigência contratual, a CONTRATADA deverá assegurar que todas as funcionalidades, módulos, características e capacidades técnicas previstas no edital permaneçam plenamente ativas, não sendo admitidas versões reduzidas, trial, limitadas ou com recursos descontinuados.

1.1.3 Todas as soluções ofertadas deverão contar com garantia oficial do fabricante, com cobertura mínima no regime 8x5 (oito horas por dia, cinco dias por semana), incluindo, no mínimo:

1.1.3.1 Suporte técnico do fabricante;

1.1.3.2 Acesso a atualizações, patches, hotfixes e correções de segurança;

1.1.3.3 Direito a substituição de hardware defeituoso quando aplicável, conforme política oficial do fabricante;

1.1.3.4 Acesso a releases, atualizações e melhorias de firmware e dos softwares embarcados ou vinculados às soluções fornecidas, disponibilizados pelo fabricante durante o período de garantia.

1.1.3.5 Acesso a toda a documentação disponível sobre a solução;

1.1.4 A garantia do fabricante deverá permanecer vigente, ativa e válida durante todo o período de 36 (trinta e seis) meses, sendo responsabilidade exclusiva da CONTRATADA a renovação, manutenção e operacionalização das eventuais assinaturas ou contratos necessários à sua continuidade.

1.1.5 É de inteira responsabilidade da CONTRATADA assegurar que todos os equipamentos, softwares, licenças, módulos, chaves de ativação, appliances virtuais ou físicos, plataformas em nuvem, agentes e serviços associados estejam devidamente elegíveis ao suporte do fabricante, não sendo admitidas ofertas que não atendam integralmente às políticas oficiais do fabricante.

1.1.6 A CONTRATADA deverá garantir que o nível de suporte contratado junto ao fabricante seja compatível com as necessidades técnicas da solução, incluindo o direito de abrir chamados diretamente ao fabricante quando assim previsto na política oficial do produto ou solicitado pela CONTRATANTE.

1.1.7 Em nenhuma hipótese será admitida a interrupção de licenciamento, garantia ou suporte durante o período de vigência, cabendo à CONTRATADA adotar as medidas necessárias para evitar qualquer descontinuidade, devendo comunicar à CONTRATANTE, com antecedência mínima de 30 (trinta) dias, sobre eventual expiração iminente ou renovação obrigatória de quaisquer componentes.

1.1.8 Todas as licenças, subscrições e garantias deverão ser fornecidas em conformidade com as boas práticas do fabricante, suas matrizes de licenciamento e respectivas metodologias de ativação, não sendo aceita a transferência de licenças entre contratos ou a utilização de mecanismos não reconhecidos oficialmente**.**

2. ITEM 1 – SOLUÇÃO DE SEGURANÇA DE REDE

2.1 CARACTERÍSTICAS GERAIS

2.1.1 A solução deverá ser composta de hardware e software licenciado, do mesmo fabricante;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

2.1.2 É permitido a composição da solução ofertada entre diversos fabricantes, desde que garantida a interoperabilidade, o suporte técnico oficial e a continuidade dos serviços durante toda a vigência contratual. Soluções baseadas em software livre serão aceitas desde que comprovadamente compatíveis com os requisitos de segurança e suporte exigidos neste Termo;
2.1.3 A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;
2.1.4 Na data da proposta, nenhum dos modelos ofertados poderá estar/ser listado no site do fabricante em listas de end-of-life, end-of-support e/ou end-of-sale;
2.1.5 Todos os componentes devem ser próprios para montagem em rack “19” e deverão ser fornecidos pela Contratada, incluindo kit tipo trilho para adaptação, cabos de alimentação, suportes, gavetas e braços, se necessário;
2.1.6 Os gateways de segurança, bem como a gerência centralizada, deverão suportar monitoramento através de SNMP v2 e v3;
2.1.7 Deve ser possível suportar arquitetura de armazenamento de logs redundante, permitindo a configuração de equipamentos distintos;

2.2 CAPACIDADE E QUANTIDADES
2.2.1 Throughput de, no mínimo, 10 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, filtro de URL, antivírus, anti-bot e prevenção de ameaças avançadas de dia zero;
2.2.2 Suporte a, no mínimo, 16.100.000 conexões ou sessões simultâneas;
2.2.3 Suporte a, no mínimo, 290.000 novas conexões por segundo;
2.2.4 Throughput de, no mínimo, 30 Gbps, no mínimo, para conexões VPN;
2.2.5 Fonte de alimentação redundante;
2.2.6 Throughput de no mínimo, 38 Gbps de IPS;
2.2.7 No mínimo, 08 (oito) interfaces de rede 10Gbps SFP+;
2.2.8 No mínimo, 08 (oito) interfaces de rede 10/100/1000 Base-T;
2.2.9 Possuir 1 (uma) interface de rede dedicada para sincronismo;
2.2.10 Possuir 1 (uma) interface de rede dedicada ao gerenciamento, não sendo permitido utilizar qualquer outra interface para exercer a função de gerenciamento do equipamento;
2.2.11 Possuir 1 (uma) interface do tipo console ou similar;
2.2.12 Possuir interface dedicada e física para gerenciamento do equipamento fora de banda. Essa interface deve ser um canal de gerenciamento que funcione mesmo quando o dispositivo não responde. Caso o equipamento não possua essa interface física/dedicada, deverá ser composta com outro equipamento de terceiro onde faça essa função. Não sendo permitido qualquer tipo de configuração via software ou uso da interface dedicada de gerenciamento.
2.2.13 Deve possuir SSD com, no mínimo, 480 GB de capacidade de armazenamento;
2.2.14 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
2.2.15 Suporte a RFC 4291 de arquitetura de endereçamento IPv6;
2.2.16 Solução deve suportar Dual Stack IPv4/IPv6 e NAT64;
2.2.17 Suportar configurar IPv6 em Dual Stack em uma interface Bond/Agregação;
2.2.18 Essa configuração também pode ser feita em uma sub-interface de bond/agregação;
2.2.19 Deve suportar NAT64 e NAT46;
2.2.20 Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
2.2.21 Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP v4 e v6 sem duplicação da base de objetos e regras;
2.2.22 Deve suportar operar em cluster ativo-passivo ou ativo-ativo sem a necessidade de licenças adicionais;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

2.2.23 O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces;
2.2.24 Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/transceptores.
2.2.25 Caso sejam fornecidas interfaces além das exigidas, todas as interfaces devem ser fornecidas com todos os transceivers/transceptores necessários para a plena utilização;
2.3 FUNCIONALIDADE DE FIREWALL
2.3.1 A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;
2.3.2 As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação técnica;
2.3.3 O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
2.3.4 A solução de segurança deve usar stateful inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede;
2.3.5 Realizar upgrade via SCP, SFTP e HTTPS via Interface WEB;
2.3.6 Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:
2.3.6.1 Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast, DHCP Relay, DHCP Server e Jumbo Frames;
2.3.6.2 Deverá suportar VXLAN;
2.3.7 Deve suportar os seguintes tipos de NAT:
2.3.7.1 Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;
2.3.8 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;
2.3.9 As regras de NAT devem suportar “hit count” para monitorar a quantidade de conexões que deram matches em cada regra;
2.3.10 Deverá permitir a criação de regras de firewall e NAT utilizando nos campos de origem e destino, objetos de serviços online atualizáveis de forma dinâmica, por exemplo: Office 365, AWS, Azure e outros. Objetos dinâmicos que não se caracterizam como FQDN.
2.3.11 Enviar logs para sistemas de monitoração externos, simultaneamente;
2.3.12 Prover mecanismo contra-ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;
2.3.13 Deve realizar roteamentos unicast e multicast simultaneamente em uma única instância(contexto) de firewall.
2.3.14 Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
2.3.15 Suportar OSPF graceful restart;
2.3.16 Deve suportar roteamento ECMP (equal cost multi-path);
2.3.17 Para o ECMP, a solução deve suportar o balanceamento do roteamento de forma simultânea usando os seguintes parâmetros: origem, destino, porta de origem, porta de destino e protocolo;
2.3.18 Autenticação integrada via Kerberos.
2.3.19 A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções/ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

mitigação de problema e aplicação de política para solução de problema. Entre as funções, deve suportar no mínimo: acesso SSH, FTP, acesso WEB, alterações de política, comunicação SNMP.
2.3.20 As regras de firewall devem suportar "hit count" para monitorar a quantidade de conexões que deram matches em cada regra;
2.3.21 Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas;
2.3.22 A solução deve ter a capacidade de operar através de uma única instancia de Firewall de forma simultânea mediante o uso das suas interfaces físicas nos seguintes modos: transparente, modo sniffer (monitoramento e análise o tráfego de rede), camada 2 (L2) e camada 3 (L3);
2.3.23 A solução deve permitir salvar as configurações das políticas para serem aplicadas em horários pré-definidos;
2.3.24 Deve possuir mecanismo de ativação de validada da regra com período customizado;
2.3.25 Deverá suportar redundância e balanceamento de links, tendo capacidade a no mínimo 3 links de internet.
2.3.26 Deverá suportar configurar um valor de threshold baseando-se em critérios mínimos como fator de decisão nas regras de balanceamento.
2.3.27 Deve permitir a configuração do tempo de checagem para cada um dos links.

2.4 FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB
2.4.1 Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;
2.4.2 Controle de políticas por usuários, grupos de usuários, IPs e redes;
2.4.3 Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2 e TLS 1.3
2.4.4 Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;
2.4.5 Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;
2.4.6 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:
2.4.6.1 Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;
2.4.6.2 Reconhecer pelo menos 5.200 (cinco mil e duzentas) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, *update* de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
2.4.7 A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não;
2.4.8 Para inspeção SSL, ou HTTPS Inspection, a solução deve oferecer suporte ao Perfect Forward Secrecy (conjuntos de cifras PFS, ECDHE)
2.4.9 Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;
2.4.9.1 Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;
2.4.10 Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo;
2.4.11 A fim de otimização de tempo operacional dos administradores, a solução deverá possuir pelo menos 90 categorias de aplicações WEB pré-definidas pelo fabricante;
2.4.12 Para solução de filtro de conteúdo e controle web, deve ser capaz de bloquear na mesma aplicação um conteúdo específico sem bloquear a aplicação principal (Ex.: Whatsapp

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

Web, Whatsapp voice e Whatsapp file transfer);
2.4.13 A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação;
2.4.14 Atualizar a base de assinaturas de aplicações automaticamente;
2.4.15 Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;
2.4.16 Os dispositivos de proteção de rede devem possuir a capacidade de identificar de forma transparente o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários. Assim, permitindo a criação de políticas de segurança baseadas nas informações coletadas entre elas usuários, IP, grupos de usuários do sistema do Active Directory;
2.4.17 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;
2.4.18 Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;
2.4.19 Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;
2.4.20 A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:
2.4.20.1 Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
2.4.20.2 Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;
2.4.20.3 Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via Active Directory e base de dados local;
2.4.20.4 Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
2.4.20.5 Suportar armazenamento, na própria solução, de URLs, evitando delay de comunicação/validação das URLs;
2.4.20.6 Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção “Safe Search” esteja desabilitada no navegador do usuário;
2.4.20.7 Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;
2.4.21 Suportar a criação de categorias de URLs customizadas;
2.4.22 Suportar a exclusão de URLs do bloqueio, por categoria; 2.4.20.10.Permitir a customização de página de bloqueio;
2.4.23 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, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;
2.4.24 Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou API’s ou Syslog, para a identificação de endereços IP e usuários;
2.4.25 Deve permitir o controle, sem instalação de cliente de software, em máquinas/computadores que solicitem saída à internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no Firewall (Captive Portal);

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

2.5 FUNCIONALIDADE DE FILTRO DE DADOS

2.5.1 A solução de controle de dados deve trazer de fábrica vários tipos de arquivos reconhecidos nativamente, permitindo a reconhecimento de pelo menos os seguintes tipos de arquivos:

2.5.1.1 PCI – Números de cartão de crédito;

2.5.1.2 International Bank Account Numbers - IBAN

2.5.1.3 Código-fonte: JAVA;

2.5.1.4 Arquivos PDF;

2.5.1.5 Arquivos executáveis;

2.5.1.6 Arquivo de banco de dados;

2.5.1.7 Arquivos de documentos;

2.5.1.8 Arquivos de apresentação;

2.5.1.9 Arquivos de planilhas;

2.5.2 A solução de controle de dados deve permitir que as direções do tráfego inspecionado sejam definidas no momento da criação da politica, tais como: "Upload", "Download" e "Download e Upload".

2.5.3 A solução de controle de dados deve permir que o usuário receba uma notificação, redirect de uma página web, sempre que um arquivo reconhecido por match em uma regra em uma das categorias acima, seja feito.

2.5.4 A solução de controle de dados deve permitir, inspecionar e prevenir vazamentos de arquivos mesmo quando estes sendo trafegados pela Web em páginas utilizando o protocolo HTTPS.

2.6 FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

2.6.1 Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento de firewall;

2.6.2 Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;

2.6.3 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/passivo;

2.6.4 Deve suportar granularidade nas políticas de Antivírus e Anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

2.6.5 A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo;

2.6.6 Deverá possuir os seguintes mecanismos de inspeção de IPS:

2.6.6.1 Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

2.6.7 Detectar e bloquear a origem de portscans;

2.6.8 Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

2.6.9 Possuir assinaturas para bloqueio de ataques de buffer overflow;

2.6.10 Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

2.6.11 Suportar bloqueio de arquivos por tipo;

2.6.12 Identificar e bloquear comunicação com botnets;

2.6.13 Deve suportar referência cruzada com CVE;

2.6.14 Em cada proteção de segurança, deve estar incluso informações como:

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

2.6.14.1 Código CVE (Common Vulnerabilities and Exposures), não sendo aceito outro código de referência;

2.6.14.2 Severidade;

2.6.14.3 Tipo de ação a ser executada.

2.6.15 O IPS deve fornecer um mecanismo automatizado para ativar ou gerenciar novas assinaturas vindas de atualizações.

2.6.16 O IPS deve suportar exceções de rede com base na origem, destino, serviço ou uma combinação dos três.

2.6.17 O IPS deve incluir um modo de solução de problemas que defina o perfil em uso para detectar apenas, sem modificar as proteções individuais.

2.6.18 O administrador deve poder ativar automaticamente novas proteções, com base em parâmetros configuráveis (impacto no desempenho, gravidade da ameaça, nível de confiança, proteção do cliente, proteção do servidor)

2.6.19 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

2.6.19.1 O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

2.6.20 Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;

2.6.21 Na própria interface de gerência, a solução de IPS deverá apresentar sumário de todos os equipamentos que estão sendo gerenciados, assim como, qual o tipo de perfil assinalado, de forma individual;

2.6.22 A solução de IPS, deve possuir mecanismo de análise baseado nas conexões realizadas para as aplicações, que aponta quais assinaturas que estão em modo detecção devem ser alterada para modo prevenção, assim evitando qualquer tipo de ataque para aplicações que estão expostas no ambiente.

2.6.23 O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados na funcionalidade de IPS;

2.6.24 A solução deverá possuir pelo menos dois perfis pré-configurados pelo fabricante que permitam sua utilização assim que o equipamento for configurado;

2.6.25 A solução deve permitir que o administrador possa configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados.

2.6.26 Deve incluir proteção contra vírus em conteúdo ActiveX e applets Java e worms;

2.6.27 Solução deve proteger contra os ataques do tipo DNS Cache Poisoning, e impedir que os usuários acessem endereços de domínios bloqueados;

2.6.28 O gerenciamento centralizado via interface gráfica, deve possibilitar a configuração de captura dos pacotes por regras individuais, visando aperfeiçoar o desempenho do equipamento;

2.6.29 A solução de IPS deve possuir mecanismo onde irá determinar de forma automática, onde qualquer nova assinatura que for baixada na base local deverá atuar em modo de prevenção ou detecção, assim evitará qualquer tipo de alteração na base de assinatura atual;

2.6.30 O antivírus deve oferecer suporte à verificação de links dentro de e-mails.

2.6.31 A solução de anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede quando usuário estiver conectado com ambiente externo malicioso

2.6.32 A solução deve permitir criar regras de exceção de acordo com a proteção, a partir do log visualizado na interface gráfica da gerência centralizada;

2.6.33 Para melhor administração a solução deve possuir a granularidade na classificação das proteções de IPS através de: severidade, nível de confiança da proteção, impacto da performance, referência de indústria terceira e status de download recente;

2.6.34 A solução deve permitir a criação de whitelist baseado no MD5 do arquivo;

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

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

2.6.36 A funcionalidade de IPS e anti-bot, deve possuir capacidade de correlacionar em seus logs a visibilidade de acordo com o framework ATT&CK Mitre Matrix, pontuando características de técnicas de acordo com a ameaça detectada/bloqueada pela solução. Caso a solução não possua determinada capacidade, poderá ser integrada com outra solução de mercado, não sendo ela soluções abertas;
2.6.37 Suportar rastreamento de vírus em arquivos pdf;
2.6.38 Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);
2.6.39 Possuir a capacidade de prevenção de ameaças não conhecidas;
2.6.40 Em caso de falha no mecanismo de inspeção do Antivírus, deve ser possível configurar se as conexões serão permitidas ou bloqueada
2.6.41 A solução de Antivírus e Anti-Malware deve funcionar de forma independente, ou seja, caso sejam desabilitadas, elas não podem causar a interrupção de outras funcionalidades de segurança como prevenção de ameaças avançadas (zero-day);
2.6.42 A solução Antivírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS/SMB, de forma a conter malwares se espalhando horizontalmente pela rede;
2.6.43 Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;
2.6.44 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
2.6.45 A solução deverá possuir mecanismo de “machine learning” para prevenção de ataques de DNS do tipo DGA (Domain Genaration Algorithm) não sendo aceito soluções que usem apenas mecanismo baseado em assinaturas.
2.6.46 A solução deverá possuir mecanismo de “machine learning” para prevenção de ataques de DNS Tunneling, não sendo aceito soluções que usem apenas mecanismo baseado em assinaturas.
2.6.47 Deverá possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos, sejam resolvidas pelo Firewall com endereços previamente definidos, para interceptar a comunicação e bloquear o acesso do usuário.
2.6.48 A solução de Anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede.
2.6.49 A solução deve possuir funcionalidade de identificação de bloqueio de tráfego malicioso comunicando com C&C (Command & Control);
2.6.50 A solução Antivírus deverá suportar a análise de links no corpo de e-mails;

2.7 FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO
2.7.1 Suportar a criação de políticas de QoS por:
2.7.2 Endereço de origem, endereço de destino e por porta;
2.7.3 O QoS deve possibilitar a definição de classes por:
2.7.4 Banda garantida, banda máxima e fila de prioridade;
2.7.5 Disponibilizar estatísticas em tempo real para classes de QoS;

2.8 FUNCIONALIDADES DE VPN
2.8.1 Suportar VPN Site-to-Site e Cliente-To-Site;
2.8.2 Suportar IPSec VPN;
2.8.3 A solução deve suportar Autoridade Certificadora Interna e Externa (de terceiros);
2.8.4 Suportar SSL VPN;
2.8.5 A VPN IPSEc deve suportar:
2.8.5.1 3DES, Autenticação MD5, SHA-1, SHA-384, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard), SHA-512 e Autenticação via certificado IKE PKI;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

2.8.6 A VPN SSL deve suportar:
2.8.6.1 Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
2.8.6.2 A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
2.8.6.3 Suportar configuração de conformidade para acesso do usuário via portal SSL ou cliente na máquina do usuário;
2.8.7 Atribuição de endereço IP nos clientes remotos de VPN;
2.8.8 Atribuição de DNS nos clientes remotos de VPN;
2.8.8.1 Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;
2.8.9 A solução deve possuir checagem de conformidade e verificar, no mínimo, as seguintes informações no cliente remoto: sistema operacional e patches instalados, antivírus, firewall no host, chaves de registros e processos ativos;
2.8.10 A solução deve permitir bloquear o acesso dos usuários aos recursos via VPN caso o usuário não esteja em conformidade com a verificação dos parâmetros configurados.
2.8.11 Suportar autenticação via AD/LDAP, certificado e base de usuários local;
2.8.12 A solução deve permitir a integração da ferramenta com provedores de identidade, através de SAML, para autenticação dos usuários remotos conectados via VPN;
2.8.13 Suportar leitura e verificação de CRL (certificate revocation list);
2.8.14 A tecnologia de VPN client-to-server deverá ser instalada na plataforma: iOS 10 ou superior e Android;
2.8.15 O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows 7, Windows 8 e MacOS X;

2.9 SOLUÇÃO PARA PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS – ZERO DAY
2.9.1 A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT;
2.9.2 A solução deverá ser composta por hardware e software específicos (appliance) com sistema operacional especializado em sua versão mais atualizada ou nuvem do próprio fabricante que possui o conceito de sandboxing para prevenção de ataques zero-day.
2.9.3 Não será aceito soluções que dependa da estrutura de hypervisors do contratante para a análise de ameaças de dia zero, como Vmware ESXi, Microsoft Hyper-V, entre outros;
2.9.4 A solução deverá operar em modo MTA (Mail Transfer Agent) para proteção de malware desconhecido de dia zero.
2.9.5 Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS), FTP e E-mail (SMTP/TLS) via MTA durante análise completa do arquivo no ambiente sandbox, sem que ele seja entregue parcialmente ao cliente.
2.9.6 A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;
2.9.7 Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URLs conhecidas;
2.9.8 A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows XP, Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 2016;
2.9.9 A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas antes de entregar este arquivo para o cliente;
2.9.10 O conteúdo enviado para a solução de sandboxing deverá ser feito automaticamente, sem a necessidade da interação do usuário/administrador para que o processo de análise seja

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

realizado;
2.9.11 Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização;
2.9.12 A análise dos arquivos deverá ser realizada em ambiente controlado (sandboxing), podendo ser em nuvem do fabricante ou appliance local, desde que garantida a isolamento do ambiente, a segurança dos dados e o suporte oficial. Não serão aceitas soluções que dependam de infraestrutura de hypervisors do contratante sem o devido suporte integrado;
2.9.13 A funcionalidade de prevenção de ameaças avançadas deve ser habilitada e funcionar de forma independente das outras funcionalidades de segurança;
2.9.14 Toda análise deverá ser realizada em ambiente seguro, preferencialmente em nuvem do fabricante ou appliance dedicado, não sendo aceitas soluções que necessitem de módulos e/ou servidores externos não suportados oficialmente para a implementação de máquinas virtuais.;
2.9.15 Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF acima de 10 Mb;
2.9.16 Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos executáveis, DLLs, ZIP e criptografados em SSL;
2.9.17 Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos java (.jar e class);
2.9.18 A solução deve suportar inspeção para o protocolo SMBv3;
2.9.19 O relatório das emulações deve conter print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;
2.9.20 Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;
2.9.21 Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;
2.9.22 Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, seven-z, exe rtf, csv, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, doc, docx, dot, docm, dotx, dotm e gz;
2.9.23 Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real e o bloqueio deve ser imediato, não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;
2.9.24 Possibilitar remoção de conteúdo ativo dinâmicos como macros, URL's, Java scripts e outros dos arquivos baixados, permitindo o download do arquivo original caso ele não seja malicioso;
2.9.25 A solução deve permitir a criação de whitelists baseado no MD5 do arquivo;
2.9.26 A solução deve possuir mecanismo para identificar sites conhecidos e desconhecidos como phishing, analisando em tempo real a URL acessada.
2.9.27 A solução deve permitir bloquear o acesso do usuário caso ele tente fazer o envio de suas informações em sites classificados como phishing;
2.9.28 O Mecanismo de classificação de anti-phising deve atuar sem a necessidade de instalação de agente na máquina do usuário;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

2.9.29 Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:

2.9.29.1 Número de arquivos emulados;

2.9.29.2 Número de arquivos com malware.

2.9.30 A solução de prevenção de ameaças avançada, deve possuir capacidade de apresentar em seus logs, visibilidade de acordo com o framework ATT&CK Mitre Matrix, pontuando características de táticas e técnicas de acordo com a ameaça detectada/bloqueada pela solução. Caso a solução não possua determinada capacidade, poderá ser integrada com outra solução de mercado, não sendo ela soluções abertas;

2.9.31 A solução deve prover informação, seja por meio de relatório ou log, sobre as seguintes situações:

2.9.31.1 O tamanho máximo do arquivo emulado seja excedido;

2.9.31.2 O tempo máximo de emulação seja excedido.

2.10 MÓDULO DE GERÊNCIA

2.10.1 A solução de gerência deverá ser separada dos gateways de segurança, que irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste item;

2.10.2 Caso a solução possua licenças relacionadas a capacidade de log indexados e armazenamento, deve ser ofertado a maior capacidade suportada ou ilimitada;

2.10.3 Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução;

2.10.4 Deve possuir solução de gerenciamento e administração centralizado, possibilitando o gerenciamento de diversos equipamentos de proteção de rede do mesmo fabricante desde que não sejam software livre;

2.10.5 O módulo de gerência deve ser capaz de gerenciar e administrar todas as soluções descritas neste item;

2.10.6 O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;

2.10.7 Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento;

2.10.8 O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS);

2.10.9 Todos os logs da solução devem ser indexados e seu licenciamento deve ser o de maior capacidade disponível ou de capacidade ilimitada, se houver.

2.10.10 O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores;

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

2.10.12 Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;

2.10.13 Suportar backup das configurações e rollback de configuração para a última configuração salva;

2.10.14 Suportar validação de regras antes da aplicação;

2.10.15 Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

2.10.16 Deve permitir a visualização dos logs de uma regra específica em tempo real e na mesma tela de configuração da regra selecionada;

2.10.17 Deve possibilitar a integração com outras soluções de SIEM de mercado desde que

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

não sejam software livre;

2.10.18 Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

2.10.19 Permitir a criação de certificados digitais para autenticação de usuários;

2.10.20 O relatório deve apresentar eventos em um único portal (dashboard) e geração de relatório de todas as funcionalidades de segurança que estão ativadas nos equipamentos de segurança, sendo que deve possuir relatório e telas de apresentação onde consta todo os principais eventos das funcionalidades de controle de aplicação web, filtro URL, prevenção de ameaças (IPS, Antivírus, Anti-Malware e sandboxing);

2.10.21 A solução deve permitir o login de múltiplos usuários administradores simultâneos com perfil de escrita, possibilitando agilidade e rapidez no gerenciamento pelo grupo de administradores da solução.

2.10.22 A solução deve permitir a integração da ferramenta com provedores de identidade para autenticação dos administradores da solução via SAML 2.0;

2.10.23 A solução deve permitir revisar e aprovar alterações de políticas de segurança feitas por outros administradores.

2.10.23.1 A solução deve permitir criar perfis de administradores para realizar revisão/alteração das políticas de segurança, com no mínimo, os perfis de aprovador e solicitante.

2.10.23.2 A solução deverá enviar a solicitação de aprovação de políticas de segurança por pelo menos uma das seguintes formas, Email, Requisição WEB ou Scripts.

2.10.24 A solução deve possuir logs, correlação de eventos e relatórios de auditoria dos administradores da solução;

2.10.25 Permitir criação de relatórios customizados via interface gráfica, sem necessidade de conhecer linguagens de banco de dados;

2.10.26 Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware), e URLs que passaram pela solução;

2.10.27 Deve ser possível exportar os logs em CSV ou TXT;

2.10.28 A solução deve ser capaz de aplicar proteções relacionadas a ameaças e regras de acesso separadamente;

2.10.29 A solução deve combinar configuração de políticas e análise de logs em um único painel, para evitar erros alcançando maior confiabilidade na alteração de políticas;

2.10.30 Deve possibilitar a geração de relatórios de eventos no formato PDF ou HTML;

2.10.31 Possibilitar rotação do log;

2.10.32 Suportar geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

2.10.32.1 Resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais hosts por número de ameaças identificadas, atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Malware), de rede vinculadas a este tráfego;

2.10.33 Deve permitir a criação de relatórios personalizados;

2.10.34 O gerenciamento centralizado deverá ser entregue como appliance virtual, no ambiente da CONTRATANTE, e dever ser compatível/homologado com/para VMWare ESX (vSphere 5.1, 5.5 ou 6);

2.10.35 A solução de gerenciamento deve possuir a capacidade de gerenciar outros firewalls de segurança do mesmo fabricante localizados em ambientes virtualizados, nuvens públicas (AWS e Azure) e nuvens privadas (VMWare NSX ou Cisco ACI);

2.10.36 Possuir capacidade de integração com soluções de terceiros via API e suportar configurações através de REST API.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

2.10.37 Deve consolidar logs e relatórios de todos os dispositivos administrados;
2.10.38 Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;
2.10.39 Deverá possuir mecanismo de drill-down para navegação e análise dos logs em tempo real;
2.10.40 Nas opções de drill-down, deve ser possível identificar o usuário que fez determinado acesso;
2.10.41 Permitir que os relatórios possam ser salvos, enviados e impressos;
2.10.42 Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc;
2.10.43 A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:
2.10.43.1 Visualizar quantidade de tráfego utilizado de aplicações e navegação;
2.10.43.2 Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;
2.10.44 A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares;
2.10.45 A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;
2.10.46 Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando, para tanto, gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos;
2.10.47 Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory via Radius;
2.10.48 Criar certificados digitais para acesso dos usuários VPN;
2.10.49 Criar certificados digitais para VPNs Site-to-Site;
2.10.50 Caso a solução possua licenciamento relacionado a capacidade de criação de certificados, deve ser contemplado a sua maior capacidade ou ilimitada;
2.10.51 Permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconheça os usuários de forma transparente;
2.10.52 Geração de painel e relatórios contendo mapas geográficos gerados em tempo real para a visualização das principais ameaças através de origens e destinos do tráfego gerado na Instituição.
2.10.53 A plataforma de gerência centralizada e monitoração deve possibilitar a visualização dos logs de firewall, navegação web, conteúdo de arquivos, prevenção de ameaças e sandbox, todos a partir de um único local centralizado possibilitando a procura correlacionada de logs em uma única tela, como por exemplo pesquisar logs de Antivírus e navegação web simultaneamente na mesma query de pesquisa.
2.10.54 O relatório das emulações (sandboxing) deve conter print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;
2.10.55 A plataforma de gerência centralizada e monitoração deve possibilitar a procura por IPs e redes, sendo que os resultados mostrem estes IPs e redes nos campos de origem e destino do logs na mesma tela de pesquisa.
2.10.56 Possuir mecanismo para que logs antigos sejam removidos automaticamente;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

2.10.57 Possuir a capacidade de personalização de gráficos como barra, linha e tabela;
2.10.58 Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;
2.10.59 Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU;
2.10.60 A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real;
2.10.61 A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria;
2.10.62 A solução deve ser capaz de personalizar e criar regras de correlação;
2.10.63 A solução deve fornecer uma interface gráfica para criação das regras citadas no item anterior;
2.10.64 A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências;

3. ITEM 2 – SOLUÇÃO DE CONECTIVIDADE DE REDE SEGURA – ACESSO – TIPO 1

3.1 CARACTERÍSTICAS DE CAPACIDADE

3.1.1 Deve possuir no mínimo 24 portas 10/100/1000BaseT Gigabit Ethernet BaseT
3.1.2 Deve possuir 4 portas adicionais com velocidade de 1/10G SFP+;
3.1.3 Deve implementar PoE e PoE+ (Power over Ethernet) de acordo com o padrão IEEE 803.3af e IEEE 802.3at;
3.1.4 Deve possuir no mínimo 350 watts destinados as portas com PoE+ ativo;
3.1.5 Deve possuir 1 interface RJ-45, USB-C ou serial para acesso console local
3.1.6 Deve possuir memória RAM de no mínimo 4GB;
3.1.7 Deve possuir buffer de pacotes de no mínimo 12MB;
3.1.8 Deve possuir capacidade de encaminhamento de no mínimo 95 Mpps;
3.1.9 Deve possuir capacidade de comutação de no mínimo 126 Gbps;
3.1.10 O switch deve ser do tipo empilhável, com altura máxima de 1RU e instalação em rack (19”). Deve acompanhar todos os componentes necessários para sua fixação no rack;
3.1.11 Deve possuir fonte de alimentação interna 100/240VAC;
3.1.12 Deve possuir Certificado de Homologação na Anatel, de acordo com a Resolução nº 242;

3.2 FUNCIONALIDADES DE CAMADA 2

3.2.1 Deve implementar VLAN 802.1Q;
3.2.2 Deve implementar BPDU;
3.2.3 Deve suportar Jumbo Packets de pelo menos 9000 bytes;
3.2.4 Port Mirroring com no mínimo 4 grupos de espelhamento;
3.2.5 Deve implementar funcionalidade que permita a detecção de links unidirecionais;
3.2.6 Deve implementar 4094 VALN Ids
3.2.7 Deve suportar 512 VLANS Comnfiguradas simultanmeamente
3.2.8 Deve implementar MVRP (Multiple VLAN Registration Protocol);
3.2.9 Deve implementar LLDP (IEEE 802.1ab);
3.2.10 Deve implementar LLDP-MED;
3.2.11 Deve implementar RPVST+ ou protocolo compatível;
3.2.12 Deve implementar MSTP (IEEE 802.1s);
3.2.13 MVRP
3.2.14 IGMP
3.2.15 Possuir tabela ARP de pelo menos 1024 entradas

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

3.2.16 Deve possuir capacidade mínima da tabela MAC de 8 mil entradas

3.3 FUNCIONALIDADES DE CAMADA 3

3.3.1 Deve implementar roteamento estático;

3.3.2 Deve suportar dual stack

3.3.3 Deve suportar DHCP Client para IPv4 e IPv6

3.3.4 Deve suportar no mínimo 512 rotas IPV4 e 512 rotas IPv6

3.4 MULTICAST

3.4.1 Deve implementar MLD snooping;

3.4.2 Deve implementar IGMP v2 e v3;

3.5 QOS E ACL

3.5.1 Deve implementar controle de Storm de broadcast e multicast;

3.5.2 Deve implementar rate limiting para pacotes ICMP;

3.5.3 Deve implementar Strict priority (SP) queuing

3.5.4 Deve implementar priorização de trafego em tempo real

3.5.5 Deve implementar priorização de tráfego com no mínimo os seguintes parâmetros: endereço IP, Tipo de Serviço, Numero da porta TCP/UDP, porta de origem e Diffserv.

3.5.6 Deve suporta no mínimo oito filas por porta

3.5.7 Deve suportar ACL para IPv4 e IPv6

3.5.8 Deve implementar Acl com base no IP de origem e destino, porta TCP e UDP de origem e destino baeanda em VLAN ou por Porta.

3.6 SEGURANÇA

3.6.1 Deve suportar controle de acesso baseado em perfis (Role Based Access Control);

3.6.2 Deve implementar 802.1x;

3.6.3 Deve implementar autenticação baseada em web;

3.6.4 Deve implementar autenticação baseada em endereço MAC;

3.6.5 Deve permitir a utilização simultânea de autenticação 802.1x, WEB e MAC em uma mesma porta, com suporte a até 32 sessões simultâneas;

3.6.6 Deve implementar protocolo padrão de AAA para autenticação, autorização e contabilização de acesso administrativo, como TACACS+ ou RADIUS, com suporte a criptografia de sessão e integração com diretórios corporativos;

3.6.7 Deve possuir proteção contra-ataques na CPU do switch para prevenção de desligamento do appliance

3.6.8 Deve suportar SSHv2;

3.7 GERENCIAMENTO

3.7.1 Deve implementar NTP;

3.7.2 Deve suportar duas imagens de software na flash;

3.7.3 Deve suportar múltiplos arquivos de configuração na flash;

3.7.4 Deve suportar detecção de falha e link entre switches;

3.7.5 Deve implementar sFlow;

3.7.6 Deve possuir interface web e via linha de comando para configuração;

3.7.7 Deve implementar Syslog;

3.7.8 Deve implementar Secure SFTP (SFTP);

3.7.9 Deve suportar RMON

3.7.10 Deve suportar Ping e Tracerout para IPv4 e IPv6

3.7.11 Deve implementar SNMP v1/v2/v3

3.7.12 Deve implementar compatibilidade com o protocolo CDP para provisionamento de telefones IP;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

3.8 CARACTERÍSTICAS DE GERENCIAMENTO CENTRALIZADO

3.8.1 A solução de gerenciamento deverá permitir acesso via plataforma centralizada, podendo ser oferecido em modelo SaaS (nuvem pública) ou on-premise (local), desde que garantida a disponibilidade, segurança e integração com os dispositivos gerenciados;

3.8.2 Caso a solução seja oferecida em modelo SaaS, todos os recursos de hardware, software, suporte, manutenção e segurança para funcionamento da solução deverão ser providos pelo fornecedor. Se on-premise, a CONTRATADA deverá fornecer as licenças e infraestrutura necessárias;

3.8.3 A solução de gerenciamento deverá ser acessível através de navegador WEB padrão, com criptografia de tráfego TLS 1.2 ou superior;

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

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

3.8.6 A solução de gerenciamento deverá permitir a gestão, monitoramento e ferramentas de diagnóstico para switches e pontos de acesso de rede sem fio, através de um único painel;

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

3.8.8 Os certificados digitais utilizados para estabelecimento desta comunicação segura deverão estar armazenados em hardware específicos (TPM - Trusted Platform Module) nos dispositivos a serem gerenciados;

3.8.9 As URLs de destino necessárias para estabelecimento da comunicação com os dispositivos a serem gerenciados deverão ser disponibilizadas;

3.8.10 A solução de gerenciamento deverá encaminhar por e-mail o convite para o usuário concluir seu cadastro, incluindo a definição de senha, para acesso a plataforma, assim que seu e-mail for incluído como novo usuário;

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

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

3.8.13 Deve disponibilizar aplicativo gratuito através das lojas oficiais (App Store e Google Play);

3.8.14 A utilização do aplicativo para ativação deverá ser controlada, permitindo definir, o usuário, localidade, data e hora em que poderá ser realizada;

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

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

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

3.8.18 Os equipamentos deverão permitir o acesso local, sem necessidade de abertura de chamado técnico com o fabricante, para realização das configurações iniciais para acesso a solução de gerenciamento, nos casos em que não houver serviço de configuração dinâmica de

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

endereços IPs para acesso à Internet;

3.8.19 Toda a solução de gerenciamento deverá estar disponível em Português, permitindo alternar para o Inglês conforme desejado pelo operador;

3.8.20 A solução de gerenciamento deve permitir a configuração baseada em grupos, permitindo que em um mesmo grupo possam ser definidas graficamente as configurações para switches e pontos de acesso de rede sem fio;

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

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

3.8.23 Os arquivos templates em linha de comando deverão permitir a criação de variáveis e condicionantes para definição de parâmetros da configuração

3.8.24 Deverá permitir a visualização das diferenças de configuração entre o arquivo template e a configuração vigente no equipamento;

3.8.25 Deverá permitir que os equipamentos sejam movimentados entre grupos diferentes, assumindo sempre a configuração do grupo de destino;

3.8.26 Deverá permitir que as configurações sejam salvas através de acesso direto aos equipamentos via FTP, SFTP e TFTP;

3.8.27 Deverá promover o ZTP (Zero Touch Provisioning) das configurações de equipamentos sem necessidade de acesso local;

3.8.28 Deverá permitir a configuração de política de conformidade de versão de software dos equipamentos por grupo de configuração;

3.8.29 Deverá executar a atualização de software automática quando o equipamento for associado ao grupo de destino, obedecendo a versão definida na política de conformidade;

3.8.30 Deverá permitir programar a atualização de software por localidade, definindo a data e horário para execução;

3.8.31 Deverá possuir API (Application Programming Interface) aberta que permita o acesso e integração a solução de gerenciamento, não só para monitoramento, mas também para configuração dos equipamentos e seus grupos;

3.8.32 Deverá possuir Streaming API, que permita o envio de informações a partir da solução de gerenciamento sem depender de requisições externas, entre elas:

3.8.32.1 Auditoria (conexão, configuração e firmware de equipamentos)

3.8.32.2 Monitoramento (status e estatísticas) de clientes

3.8.33 Deverá permitir o encaminhamento de alertas utilizando e-mail e WEBHOOK, considerando, no mínimo, os seguintes escopos de alertas para encaminhamento:

3.8.33.1 Alertas de Usuários

3.8.33.2 Alertas de Switches

3.8.33.3 Alertas de conectividade com a solução de gerência

3.8.33.4 Alertas de auditoria

3.8.33.5 Alertas de localidade

3.8.34 Deverá permitir a integração, através de API, com solução que permita validar a experiência dos usuários no acesso aos recursos de rede e aplicações internas, externas (SaaS) e customizadas, permitindo visibilidade do status verificado nos últimos 5 minutos através do dashboard por localidades.

3.8.35 Funcionalidade de relatórios:

3.8.35.1 Capacidade de geração de relatório para armazenagem de informações;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

3.8.35.2 Coleta de informações da rede por períodos de tempo pré-definidos;
3.8.35.3 Capacidade de geração e envio automático de relatórios por e-mail;
3.8.36 Caso seja utilizado soluções de terceiros para a geração de relatórios, estas devem ser homologadas pelo fornecedor dos equipamentos de rede.

4. ITEM 3 – SOLUÇÃO DE CONECTIVIDADE DE REDE SEGURA – ACESSO – TIPO 2

4.1 CARACTERÍSTICAS DE CAPACIDADE

4.1.1 Deve possuir no mínimo 24 portas 10/100/1000BaseT Gigabit Ethernet BaseT
4.1.2 Deve possuir 4 portas adicionais com velocidade de 1/10G SFP+;
4.1.3 Deve possuir 1 interface RJ-45, USB-C ou serial para acesso console local
4.1.4 Deve possuir memória RAM de no mínimo 4 Gbytes;
4.1.5 Deve possuir buffer de pacotes de no mínimo 12 MB;
4.1.6 Deve possuir capacidade de encaminhamento de no mínimo 95 Mpps;
4.1.7 Deve possuir capacidade de comutação de no mínimo 126 Gbps;
4.1.8 O switch deve ser do tipo empilhável, com altura máxima de 1RU e instalação em rack (19”). Deve acompanhar todos os componentes necessários para sua fixação no rack;
4.1.9 Deve possuir fonte de alimentação interna 100/240VAC
4.1.10 Deve possuir Certificado de Homologação na Anatel, de acordo com a Resolução nº 242;

4.2 FUNCIONALIDADES DE CAMADA 2

4.2.1 Deve implementar VLAN 802.1Q;
4.2.2 Deve implementar BPDU;
4.2.3 Deve suportar Jumbo Packets de pelo menos 9000 bytes;
4.2.4 Port Mirroring com no mínimo 4 grupos de espelhamento;
4.2.5 Deve implementar funcionalidade que permita a detecção de links unidirecionais;
4.2.6 Deve implementar 4094 VALN Ids
4.2.7 Deve suportar 512 VLANS Comnfiguradas simultanmeamente
4.2.8 Deve implementar MVRP (Multiple VLAN Registration Protocol);
4.2.9 Deve implementar LLDP (IEEE 802.1ab);
4.2.10 Deve implementar LLDP-MED;
4.2.11 Deve implementar RPVST+ ou protocolo compatível;
4.2.12 Deve implementar MSTP (IEEE 802.1s);
4.2.13 MVRP
4.2.14 IGMP
4.2.15 Possuir tabea ARP de pelo meno 1024 entradas
4.2.16 Deve possuir capacidade mínima da tabela MAC de 8 mil entradas

4.3 FUNCIONALIDADES DE CAMADA 3

4.3.1 Deve implementar roteamento estático;
4.3.2 Deve suportar dual stack
4.3.3 Deve suportar DHCP Client para IPv4 e IPv6
4.3.4 Deve suportar no mínimo 512 rotas IPV4 e 512 rotas IPv6

4.4 MULTICAST

4.4.1 Deve implementar MLD snooping;
4.4.2 Deve implementar IGMP v2 e v3;

4.5 QOS E ACL

4.5.1 Deve implementar controle de Storm de broadcast e multicast;
4.5.2 Deve implementar rate limiting para pacotes ICMP;
4.5.3 Deve implementar Strict priority (SP) queuing

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

4.5.4 Deve implementar priorização de tráfego em tempo real
4.5.5 Deve implementar priorização de tráfego com no mínimo os seguintes parâmetros: endereço IP, Tipo de Serviço, Número da porta TCP/UDP, porta de origem e Diffserv.
4.5.6 Deve suporta no mínimo oito filas por porta
4.5.7 Deve suportar ACL para IPv4 e IPv6
4.5.8 Deve implementar Acl com base no IP de origem e destino, porta TCP e UDP de origem e destino baseada em VLAN ou por Porta.

4.6 SEGURANÇA

4.6.1 Deve suportar controle de acesso baseado em perfis (Role Based Access Control);
4.6.2 Deve implementar 802.1x;
4.6.3 Deve implementar autenticação baseada em web;
4.6.4 Deve implementar autenticação baseada em endereço MAC;
4.6.5 Deve permitir a utilização simultânea de autenticação 802.1x, WEB e MAC em uma mesma porta, com suporte a até 32 sessões simultâneas;
4.6.6 Deve implementar protocolo padrão de AAA para autenticação, autorização e contabilização de acesso administrativo, como TACACS+ ou RADIUS, com suporte a criptografia de sessão e integração com diretórios corporativos;
4.6.7 Deve possuir proteção contra-ataques na CPU do switch para prevenção de desligamento do appliance
4.6.8 Deve suportar SSHv2;

4.7 GERENCIAMENTO

4.7.1 Deve implementar NTP;
4.7.2 Deve suportar duas imagens de software na flash;
4.7.3 Deve suportar múltiplos arquivos de configuração na flash;
4.7.4 Deve suportar detecção de falha e link entre switches;
4.7.5 Deve implementar sFlow;
4.7.6 Deve possuir interface web e via linha de comando para configuração;
4.7.7 Deve implementar Syslog;
4.7.8 Deve implementar Secure SFTP (SFTP);
4.7.9 Deve suportar RMON
4.7.10 Deve suportar Ping e Tracerout para IPv4 e IPv6
4.7.11 Deve implementar SNMP v1/v2/v3
4.7.12 Deve implementar compatibilidade com o protocolo CDP para provisionamento de telefones IP;

4.8 CARACTERÍSTICAS DE GERENCIAMENTO CENTRALIZADO

4.8.1 A solução de gerenciamento deverá permitir acesso via plataforma centralizada, podendo ser oferecido em modelo SaaS (nuvem pública) ou on-premise (local), desde que garantida a disponibilidade, segurança e integração com os dispositivos gerenciados;
4.8.2 Caso a solução seja oferecida em modelo SaaS, todos os recursos de hardware, software, suporte, manutenção e segurança para funcionamento da solução deverão ser providos pelo fornecedor. Se on-premise, a CONTRATADA deverá fornecer as licenças e infraestrutura necessárias;
4.8.3 A solução de gerenciamento deverá ser acessível através de navegador WEB padrão, com criptografia de tráfego TLS 1.2 ou superior;
4.8.4 Todo acesso deverá ser controlado com autenticação de usuário em base própria e

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

externa utilizando para isso Single Sign-on através do protocolo SAML;

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

4.8.6 A solução de gerenciamento deverá permitir a gestão, monitoramento e ferramentas de diagnóstico para switches e pontos de acesso de rede sem fio, através de um único painel;

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

4.8.8 Os certificados digitais utilizados para estabelecimento desta comunicação segura deverão estar armazenados em hardware específicos (TPM - Trusted Platform Module) nos dispositivos a serem gerenciados;

4.8.9 As URLs de destino necessárias para estabelecimento da comunicação com os dispositivos a serem gerenciados deverão ser disponibilizadas;

4.8.10 A solução de gerenciamento deverá encaminhar por e-mail o convite para o usuário concluir seu cadastro, incluindo a definição de senha, para acesso a plataforma, assim que seu e-mail for incluído como novo usuário;

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

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

4.8.13 Deve disponibilizar aplicativo gratuito através das lojas oficiais (App Store e Google Play);

4.8.14 A utilização do aplicativo para ativação deverá ser controlada, permitindo definir, o usuário, localidade, data e hora em que poderá ser realizada;

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

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

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

4.8.18 Os equipamentos deverão permitir o acesso local, sem necessidade de abertura de chamado técnico com o fabricante, para realização das configurações iniciais para acesso a solução de gerenciamento, nos casos em que não houver serviço de configuração dinâmica de endereços IPs para acesso à Internet;

4.8.19 Toda a solução de gerenciamento deverá estar disponível em Português, permitindo alternar para o Inglês conforme desejado pelo operador;

4.8.20 A solução de gerenciamento deve permitir a configuração baseada em grupos, permitindo que em um mesmo grupo possam ser definidas graficamente as configurações para switches e pontos de acesso de rede sem fio;

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

4.8.22 Os grupos devem permitir dois modos de configuração dos equipamentos, interface

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

gráfica e através de templates em arquivos de linha de comando;
4.8.23 Os arquivos templates em linha de comando deverão permitir a criação de variáveis e condicionantes para definição de parâmetros da configuração
4.8.24 Deverá permitir a visualização das diferenças de configuração entre o arquivo template e a configuração vigente no equipamento;
4.8.25 Deverá permitir que os equipamentos sejam movimentados entre grupos diferentes, assumindo sempre a configuração do grupo de destino;
4.8.26 Deverá permitir que as configurações sejam salvas através de acesso direto aos equipamentos via FTP, SFTP e TFTP;
4.8.27 Deverá promover o ZTP (Zero Touch Provisioning) das configurações de equipamentos sem necessidade de acesso local;
4.8.28 Deverá permitir a configuração de política de conformidade de versão de software dos equipamentos por grupo de configuração;
4.8.29 Deverá executar a atualização de software automática quando o equipamento for associado ao grupo de destino, obedecendo a versão definida na política de conformidade;
4.8.30 Deverá permitir programar a atualização de software por localidade, definindo a data e horário para execução;
4.8.31 Deverá possuir API (Application Programming Interface) aberta que permita o acesso e integração a solução de gerenciamento, não só para monitoramento, mas também para configuração dos equipamentos e seus grupos;
4.8.32 Deverá possuir Streaming API, que permita o envio de informações a partir da solução de gerenciamento sem depender de requisições externas, entre elas:
4.8.32.1 Auditoria (conexão, configuração e firmware de equipamentos)
4.8.32.2 Monitoramento (status e estatísticas) de clientes
4.8.33 Deverá permitir o encaminhamento de alertas utilizando e-mail e WEBHOOK, considerando, no mínimo, os seguintes escopos de alertas para encaminhamento:
4.8.33.1 Alertas de Usuários
4.8.33.2 Alertas de Switches
4.8.33.3 Alertas de conectividade com a solução de gerência
4.8.33.4 Alertas de auditoria
4.8.33.5 Alertas de localidade
4.8.34 Deverá permitir a integração, através de API, com solução que permita validar a experiência dos usuários no acesso aos recursos de rede e aplicações internas, externas (SaaS) e customizadas, permitindo visibilidade do status verificado nos últimos 5 minutos através do dashboard por localidades.
4.8.35 Funcionalidade de relatórios:
4.8.35.1 Capacidade de geração de relatório para armazenagem de informações;
4.8.35.2 Coleta de informações da rede por períodos pré-definidos;
4.8.35.3 Capacidade de geração e envio automático de relatórios por e-mail;
4.8.36 Caso seja utilizado soluções de terceiros para a geração de relatórios, estas devem ser homologadas pelo fornecedor dos equipamentos de rede.

5. ITEM 4 - SOLUÇÃO DE CONECTIVIDADE DE REDE SEGURA – ACESSO – TIPO 3

5.1 CARACTERÍSTICAS DE CAPACIDADE

5.1.1 Deve possuir no mínimo 48 portas 10/100/1000BaseT Gigabit Ethernet BaseT
5.1.2 Deve possuir 4 portas adicionais com velocidade de 1/10G SFP+;
5.1.3 Deve possuir 1 interface RJ-45, USB-C ou serial para acesso console local

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

5.1.4 Deve implementar PoE e PoE+ (Power over Ethernet) de acordo com o padrão IEEE 803.3af e IEEE 802.3at;
5.1.5 Deve possuir no mínimo 730 watts destinados as portas com PoE+ ativo;
5.1.6 Deve possuir memória RAM de no mínimo 4 Gbytes;
5.1.7 Deve possuir buffer de pacotes de no mínimo 12MB;
5.1.8 Deve possuir capacidade de encaminhamento de no mínimo 97 Mpps;
5.1.9 Deve possuir capacidade de comutação de no mínimo 174 Gbps;
5.1.10 O switch deve ser do tipo empilhável, com altura máxima de 1RU e instalação em rack (19”). Deve acompanhar todos os componentes necessários para sua fixação no rack;
5.1.11 Deve possuir fonte de alimentação interna 100/240VAC
5.1.12 Deve possuir Certificado de Homologação na Anatel, de acordo com a Resolução nº 242;

5.2 FUNCIONALIDADES DE CAMADA 2

5.2.1 Deve implementar VLAN 802.1Q;
5.2.2 Deve implementar BPDU;
5.2.3 Deve suportar Jumbo Packets de pelo menos 9000 bytes;
5.2.4 Port Mirroring com no mínimo 4 grupos de espelhamento;
5.2.5 Deve implementar funcionalidade que permita a detecção de links unidirecionais;
5.2.6 Deve implementar 4094 VALN Ids
5.2.7 Deve suportar 512 VLANS Comnfiguradas simultanmeamente
5.2.8 Deve implementar MVRP (Multiple VLAN Registration Protocol);
5.2.9 Deve implementar LLDP (IEEE 802.1ab);
5.2.10 Deve implementar LLDP-MED;
5.2.11 Deve implementar RPVST+ ou protocolo compatível;
5.2.12 Deve implementar MSTP (IEEE 802.1s);
5.2.13 MVRP
5.2.14 IGMP
5.2.15 Possuir tabela ARP de pelo menos 1024 entradas
5.2.16 Deve possuir capacidade mínima da tabela MAC de 8 mil entradas

5.3 FUNCIONALIDADES DE CAMADA 3

5.3.1 Deve implementar roteamento estático;
5.3.2 Deve suportar dual stack
5.3.3 Deve suportar DHCP Client para IPv4 e IPv6
5.3.4 Deve suportar no mínimo 512 rotas IPV4 e 512 rotas IPv6

5.4 MULTICAST

5.4.1 Deve implementar MLD snooping;
5.4.2 Deve implementar IGMP v2 e v3;

5.5 QOS E ACL

5.5.1 Deve implementar controle de Storm de broadcast e multicast;
5.5.2 Deve implementar rate limiting para pacotes ICMP;
5.5.3 Deve implementar Strict priority (SP) queuing
5.5.4 Deve implementar priorização de tráfego em tempo real
5.5.5 Deve implementar priorização de tráfego com no mínimo os seguintes parâmetros: endereço IP, Tipo de Serviço, Número da porta TCP/UDP, porta de origem e Diffserv.
5.5.6 Deve suporta no mínimo oito filas por porta
5.5.7 Deve suportar ACL para IPv4 e IPv6
5.5.8 Deve implementar Acl com base no IP de origem e destino, porta TCP e UDP de origem e destino baseada em VLAN ou por Porta.

5.6 SEGURANÇA

5.6.1 Deve suportar controle de acesso baseado em perfis (Role Based Access Control);
5.6.2 Deve implementar 802.1x;
5.6.3 Deve implementar autenticação baseada em web;
5.6.4 Deve implementar autenticação baseada em endereço MAC;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

5.6.5 Deve permitir a utilização simultânea de autenticação 802.1x, WEB e MAC em uma mesma porta, com suporte a até 32 sessões simultâneas;
5.6.6 Deve implementar protocolo padrão de AAA para autenticação, autorização e contabilização de acesso administrativo, como TACACS+ ou RADIUS, com suporte a criptografia de sessão e integração com diretórios corporativos;
5.6.7 Deve possuir proteção contra ataques na CPU do switch para prevenção de desligamento do appliance
5.6.8 Deve suportar SSHv2;

5.7 GERENCIAMENTO

5.7.1 Deve implementar NTP;
5.7.2 Deve suportar duas imagens de software no flash;
5.7.3 Deve suportar múltiplos arquivos de configuração no flash;
5.7.4 Deve suportar detecção de falha e link entre switches;
5.7.5 Deve implementar sFlow;
5.7.6 Deve possuir interface web e via linha de comando para configuração;
5.7.7 Deve implementar Syslog;
5.7.8 Deve implementar Secure SFTP (SFTP);
5.7.9 Deve suportar RMON
5.7.10 Deve suportar Ping e Tracerout para IPv4 e IPv6
5.7.11 Deve implementar SNMP v1/v2/v3
5.7.12 Deve implementar compatibilidade com o protocolo CDP para provisionamento de telefones IP;

5.8 CARACTERÍSTICAS DE GERENCIAMENTO CENTRALIZADO

5.8.1 A solução de gerenciamento deverá permitir acesso via plataforma centralizada, podendo ser oferecido em modelo SaaS (nuvem pública) ou on-premise (local), desde que garantida a disponibilidade, segurança e integração com os dispositivos gerenciados;
5.8.2 Caso a solução seja oferecida em modelo SaaS, todos os recursos de hardware, software, suporte, manutenção e segurança para funcionamento da solução deverão ser providos pelo fornecedor. Se on-premise, a CONTRATADA deverá fornecer as licenças e infraestrutura necessárias;
5.8.3 A solução de gerenciamento deverá ser acessível através de navegador WEB padrão, com criptografia de tráfego TLS 1.2 ou superior;
5.8.4 Todo acesso deverá ser controlado com autenticação de usuário em base própria e externa utilizando para isso Single Sign-on através do protocolo SAML;
5.8.5 Os privilégios de acesso deverão ser controlados através de RBAC (Role Base Access Control) permitindo derivar privilégios por usuário baseado em Roles para determinar quais níveis de acesso será permitido;
5.8.6 A solução de gerenciamento deverá permitir a gestão, monitoramento e ferramentas de diagnóstico para switches e pontos de acesso de rede sem fio, através de um único painel;
5.8.7 Toda a comunicação entre a solução de gerenciamento e os dispositivos gerenciados deverá ser feita através de conexão segura SSL v1.3, utilizando porta TCP 443;
5.8.8 Os certificados digitais utilizados para estabelecimento desta comunicação segura deverão estar armazenados em hardware específicos (TPM - Trusted Platform Module) nos dispositivos a serem gerenciados;
5.8.9 As URLs de destino necessárias para estabelecimento da comunicação com os dispositivos a serem gerenciados deverão ser disponibilizadas;
5.8.10 A solução de gerenciamento deverá encaminhar por e-mail o convite para o usuário concluir seu cadastro, incluindo a definição de senha, para acesso a plataforma, assim que seu e-mail for incluído como novo usuário;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

5.8.11 Deve permitir que as licenças sejam migradas entre equipamentos da mesma família, para o caso de substituição de equipamentos com defeito ou outros, sem depender de abertura de chamado técnico para isso;
5.8.12 Deve contemplar todas as atualizações disponibilizadas de maneira automática durante o período de vigência das licenças, sem depender de intervenção manual do operador;
5.8.13 Deve disponibilizar aplicativo gratuito através das lojas oficiais (App Store e Google Play);
5.8.14 A utilização do aplicativo para ativação deverá ser controlada, permitindo definir, o usuário, localidade, data e hora em que poderá ser realizada;
5.8.15 O aplicativo para ativação deverá permitir o envio de foto para comprovar o término da implantação pelo usuário, além de permitir o envio de instruções básicas para o instalador através do painel de acompanhamento e gestão da implantação;
5.8.16 Após marcada como concluída, ou finalizado o período para implantação, o usuário do aplicativo não terá mais acesso a referida rotina para implantação;
5.8.17 Toda a configuração, bem como a versão de software em que os equipamentos deverão utilizar, deverão ser automaticamente enviadas após a conclusão da implantação através do aplicativo;
5.8.18 Os equipamentos deverão permitir o acesso local, sem necessidade de abertura de chamado técnico com o fabricante, para realização das configurações iniciais para acesso a solução de gerenciamento, nos casos em que não houver serviço de configuração dinâmica de endereços IPs para acesso à Internet;
5.8.19 Toda a solução de gerenciamento deverá estar disponível em Português, permitindo alternar para o Inglês conforme desejado pelo operador;
5.8.20 A solução de gerenciamento deve permitir a configuração baseada em grupos, permitindo que em um mesmo grupo possam ser definidas graficamente as configurações para switches e pontos de acesso de rede sem fio;
5.8.21 As configurações do grupo ao qual o equipamento está associado deverão ser substituídas pelas configurações associadas ao equipamento específico (interfaces, VLAN, endereçamento IP, gateway, hostname);
5.8.22 Os grupos devem permitir dois modos de configuração dos equipamentos, interface gráfica e através de templates em arquivos de linha de comando;
5.8.23 Os arquivos templates em linha de comando deverão permitir a criação de variáveis e condicionantes para definição de parâmetros da configuração
5.8.24 Deverá permitir a visualização das diferenças de configuração entre o arquivo template e a configuração vigente no equipamento;
5.8.25 Deverá permitir que os equipamentos sejam movimentados entre grupos diferentes, assumindo sempre a configuração do grupo de destino;
5.8.26 Deverá permitir que as configurações sejam salvas através de acesso direto aos equipamentos via FTP, SFTP e TFTP;
5.8.27 Deverá promover o ZTP (Zero Touch Provisioning) das configurações de equipamentos sem necessidade de acesso local;
5.8.28 Deverá permitir a configuração de política de conformidade de versão de software dos equipamentos por grupo de configuração;
5.8.29 Deverá executar a atualização de software automática quando o equipamento for associado ao grupo de destino, obedecendo a versão definida na política de conformidade;
5.8.30 Deverá permitir programar a atualização de software por localidade, definindo a data e horário para execução;
5.8.31 Deverá possuir API (Application Programming Interface) aberta que permita o acesso e integração a solução de gerenciamento, não só para monitoramento, mas também para configuração dos equipamentos e seus grupos;
5.8.32 Deverá possuir Streaming API, que permita o envio de informações a partir da solução de gerenciamento sem depender de requisições externas, entre elas:

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

5.8.32.1 Auditoria (conexão, configuração e firmware de equipamentos)
5.8.32.2 Monitoramento (status e estatísticas) de clientes
5.8.33 Deverá permitir o encaminhamento de alertas utilizando e-mail e WEBHOOK, considerando, no mínimo, os seguintes escopos de alertas para encaminhamento:
5.8.33.1 Alertas de Usuários
5.8.33.2 Alertas de Switches
5.8.33.3 Alertas de conectividade com a solução de gerência
5.8.33.4 Alertas de auditoria
5.8.33.5 Alertas de localidade
5.8.34 Deverá permitir a integração, através de API, com solução que permita validar a experiência dos usuários no acesso aos recursos de rede e aplicações internas, externas (SaaS) e customizadas, permitindo visibilidade do status verificado nos últimos 5 minutos através do dashboard por localidades.
5.8.35 Funcionalidade de relatórios:
5.8.35.1 Capacidade de geração de relatório para armazenagem de informações;
5.8.35.2 Coleta de informações da rede por períodos pré-definidos;
5.8.35.3 Capacidade de geração e envio automático de relatórios por e-mail;
5.8.36 Caso seja utilizado soluções de terceiros para a geração de relatórios, estas devem ser homologadas pelo fornecedor dos equipamentos de rede.

6. ITEM 5 – SOLUÇÃO DE CONECTIVIDADE DE REDE SEGURA – ACESSO – TIPO 4

6.1 CARACTERÍSTICAS DE CAPACIDADE

6.1.1 Deve possuir no mínimo 48 portas 10/100/1000BaseT Gigabit Ethernet BaseT
6.1.2 Deve possuir 4 portas adicionais com velocidade de 1/10G SFP+;
6.1.3 Deve possuir 1 interface RJ-45, USB-C ou serial para acesso console local
6.1.4 Deve possuir memória RAM de no mínimo 4 Gbytes;
6.1.5 Deve possuir buffer de pacotes de no mínimo 12MB;
6.1.6 Deve possuir capacidade de encaminhamento de no mínimo 97 Mpps;
6.1.7 Deve possuir capacidade de comutação de no mínimo 174 Gbps;
6.1.8 O switch deve ser do tipo empilhável, com altura máxima de 1RU e instalação em rack (19”). Deve acompanhar todos os componentes necessários para sua fixação no rack;
6.1.9 Deve possuir fonte de alimentação interna 100/240VAC
6.1.10 Deve possuir Certificado de Homologação na Anatel, de acordo com a Resolução nº 242;

6.2 FUNCIONALIDADES DE CAMADA 2

6.2.1 Deve implementar VLAN 802.1Q;
6.2.2 Deve implementar BPDU;
6.2.3 Deve suportar Jumbo Packets de pelo menos 9000 bytes;
6.2.4 Port Mirroring com no mínimo 4 grupos de espelhamento;
6.2.5 Deve implementar funcionalidade que permita a detecção de links unidirecionais;
6.2.6 Deve implementar 4094 VALN Ids
6.2.7 Deve suportar 512 VLANS Comnfiguradas simultanmeamente
6.2.8 Deve implementar MVRP (Multiple VLAN Registration Protocol);
6.2.9 Deve implementar LLDP (IEEE 802.1ab);
6.2.10 Deve implementar LLDP-MED;
6.2.11 Deve implementar RPVST+ ou protocolo compatível;
6.2.12 Deve implementar MSTP (IEEE 802.1s);
6.2.13 MVRP
6.2.14 IGMP
6.2.15 Possuir tabela ARP de pelo menos 1024 entradas
6.2.16 Deve possuir capacidade mínima da tabela MAC de 8 mil entradas

6.3 FUNCIONALIDADES DE CAMADA 3

6.3.1 Deve implementar roteamento estático;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

6.3.2 Deve suportar dual stack
6.3.3 Deve suportar DHCP Client para IPv4 e IPv6
6.3.4 Deve suportar no mínimo 512 rotas IPV4 e 512 rotas IPv6

6.4 MULTICAST

6.4.1 Deve implementar MLD snooping;
6.4.2 Deve implementar IGMP v2 e v3;

6.5 QOS E ACL

6.5.1 Deve implementar controle de Storm de broadcast e multicast;
6.5.2 Deve implementar rate limiting para pacotes ICMP;
6.5.3 Deve implementar Strict priority (SP) queuing
6.5.4 Deve implementar priorização de trafego em tempo real
6.5.5 Deve implementar priorização de tráfego com no mínimo os seguintes parâmetros: endereço IP, Tipo de Serviço, Numero da porta TCP/UDP, porta de origem e Diffserv.
6.5.6 Deve suporta no mínimo oito filas por porta
6.5.7 Deve suportar ACL para IPv4 e IPv6
6.5.8 Deve implementar Acl com base no IP de origem e destino, porta TCP e UDP de origem e destino baseada em VLAN ou por Porta.

6.6 SEGURANÇA

6.6.1 Deve suportar controle de acesso baseado em perfis (Role Based Access Control);
6.6.2 Deve implementar 802.1x;
6.6.3 Deve implementar autenticação baseada em web;
6.6.4 Deve implementar autenticação baseada em endereço MAC;
6.6.5 Deve permitir a utilização simultânea de autenticação 802.1x, WEB e MAC em uma mesma porta, com suporte a até 32 sessões simultâneas;
6.6.6 Deve implementar protocolo padrão de AAA para autenticação, autorização e contabilização de acesso administrativo, como TACACS+ ou RADIUS, com suporte a criptografia de sessão e integração com diretórios corporativos;
6.6.7 Deve possuir proteção contra ataques na CPU do switch para prevenção de desligamento do appliance
6.6.8 Deve suportar SSHv2;

6.7 GERENCIAMENTO

6.7.1 Deve implementar NTP;
6.7.2 Deve suportar duas imagens de software na flash;
6.7.3 Deve suportar múltiplos arquivos de configuração na flash;
6.7.4 Deve suportar detecção de falha e link entre switches;
6.7.5 Deve implementar sFlow;
6.7.6 Deve possuir interface web e via linha de comando para configuração;
6.7.7 Deve implementar Syslog;
6.7.8 Deve implementar Secure SFTP (SFTP);
6.7.9 Deve suportar RMON
6.7.10 Deve suportar Ping e Tracerout para IPv4 e IPv6
6.7.11 Deve implementar SNMP v1/v2/v3
6.7.12 Deve implementar compatibilidade com o protocolo CDP para provisionamento de telefones IP;

6.8 CARACTERÍSTICAS DE GERENCIAMENTO CENTRALIZADO

6.8.1 A solução de gerenciamento deve ser acessada através de provedores de nuvem pública, sem depender de instalações locais de software ou hardware para o seu funcionamento;
6.8.2 As funcionalidades descritas deverão ser providas no modelo SaaS (Software as a Service), como serviço, ou seja, todos os recursos de hardware, software, suporte, manutenção e segurança, para funcionamento da solução deverão ser providos pelo fornecedor;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

6.8.3 A solução de gerenciamento deverá ser acessível através de navegador WEB padrão, com criptografia de tráfego SSL v1.3;
6.8.4 Todo acesso deverá ser controlado com autenticação de usuário em base própria e externa utilizando para isso Single Sign-on através do protocolo SAML;
6.8.5 Os privilégios de acesso deverão ser controlados através de RBAC (Role Base Access Control) permitindo derivar privilégios por usuário baseado em Roles para determinar quais níveis de acesso será permitido;
6.8.6 A solução de gerenciamento deverá permitir a gestão, monitoramento e ferramentas de diagnóstico para switches e pontos de acesso de rede sem fio, através de um único painel;
6.8.7 Toda a comunicação entre a solução de gerenciamento e os dispositivos gerenciados deverá ser feita através de conexão segura SSL v1.3, utilizando porta TCP 443;
6.8.8 Os certificados digitais utilizados para estabelecimento desta comunicação segura deverão estar armazenados em hardware específicos (TPM - Trusted Platform Module) nos dispositivos a serem gerenciados;
6.8.9 As URLs de destino necessárias para estabelecimento da comunicação com os dispositivos a serem gerenciados deverão ser disponibilizadas;
6.8.10 A solução de gerenciamento deverá encaminhar por e-mail o convite para o usuário concluir seu cadastro, incluindo a definição de senha, para acesso a plataforma, assim que seu e-mail for incluído como novo usuário;
6.8.11 Deve permitir que as licenças sejam migradas entre equipamentos da mesma família, para o caso de substituição de equipamentos com defeito ou outros, sem depender de abertura de chamado técnico para isso;
6.8.12 Deve contemplar todas as atualizações disponibilizadas de maneira automática durante o período de vigência das licenças, sem depender de intervenção manual do operador;
6.8.13 Deve disponibilizar aplicativo gratuito através das lojas oficiais (App Store e Google Play);
6.8.14 A utilização do aplicativo para ativação deverá ser controlada, permitindo definir, o usuário, localidade, data e hora em que poderá ser realizada;
6.8.15 O aplicativo para ativação deverá permitir o envio de foto para comprovar o término da implantação pelo usuário, além de permitir o envio de instruções básicas para o instalador através do painel de acompanhamento e gestão da implantação;
6.8.16 Após marcada como concluída, ou finalizado o período para implantação, o usuário do aplicativo não terá mais acesso a referida rotina para implantação;
6.8.17 Toda a configuração, bem como a versão de software em que os equipamentos deverão utilizar, deverão ser automaticamente enviadas após a conclusão da implantação através do aplicativo;
6.8.18 Os equipamentos deverão permitir o acesso local, sem necessidade de abertura de chamado técnico com o fabricante, para realização das configurações iniciais para acesso a solução de gerenciamento, nos casos em que não houver serviço de configuração dinâmica de endereços IPs para acesso à Internet;
6.8.19 Toda a solução de gerenciamento deverá estar disponível em Português, permitindo alternar para o Inglês conforme desejado pelo operador;
6.8.20 A solução de gerenciamento deve permitir a configuração baseada em grupos, permitindo que em um mesmo grupo possam ser definidas graficamente as configurações para switches e pontos de acesso de rede sem fio;
6.8.21 As configurações do grupo ao qual o equipamento está associado deverão ser

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

substituídas pelas configurações associadas ao equipamento específico (interfaces, VLAN, endereçamento IP, gateway, hostname);

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

6.8.23 Os arquivos templates em linha de comando deverão permitir a criação de variáveis e condicionantes para definição de parâmetros da configuração

6.8.24 Deverá permitir a visualização das diferenças de configuração entre o arquivo template e a configuração vigente no equipamento;

6.8.25 Deverá permitir que os equipamentos sejam movimentados entre grupos diferentes, assumindo sempre a configuração do grupo de destino;

6.8.26 Deverá permitir que as configurações sejam salvas através de acesso direto aos equipamentos via FTP, SFTP e TFTP;

6.8.27 Deverá promover o ZTP (Zero Touch Provisioning) das configurações de equipamentos sem necessidade de acesso local;

6.8.28 Deverá permitir a configuração de política de conformidade de versão de software dos equipamentos por grupo de configuração;

6.8.29 Deverá executar a atualização de software automática quando o equipamento for associado ao grupo de destino, obedecendo a versão definida na política de conformidade;

6.8.30 Deverá permitir programar a atualização de software por localidade, definindo a data e horário para execução;

6.8.31 Deverá possuir API (Application Programming Interface) aberta que permita o acesso e integração a solução de gerenciamento, não só para monitoramento, mas também para configuração dos equipamentos e seus grupos;

6.8.32 Deverá possuir Streaming API, que permita o envio de informações a partir da solução de gerenciamento sem depender de requisições externas, entre elas:

6.8.32.1 Auditoria (conexão, configuração e firmware de equipamentos)

6.8.32.2 Monitoramento (status e estatísticas) de clientes

6.8.33 Deverá permitir o encaminhamento de alertas utilizando e-mail e WEBHOOK, considerando, no mínimo, os seguintes escopos de alertas para encaminhamento:

6.8.33.1 Alertas de Usuários

6.8.33.2 Alertas de Switches

6.8.33.3 Alertas de conectividade com a solução de gerência

6.8.33.4 Alertas de auditoria

6.8.33.5 Alertas de localidade

6.8.34 Deverá permitir a integração, através de API, com solução que permita validar a experiência dos usuários no acesso aos recursos de rede e aplicações internas, externas (SaaS) e customizadas, permitindo visibilidade do status verificado nos últimos 5 minutos através do dashboard por localidades.

6.8.35 Funcionalidade de relatórios:

6.8.35.1 Capacidade de geração de relatório para armazenagem de informações;

6.8.35.2 Coleta de informações da rede por períodos pré-definidos;

6.8.35.3 Capacidade de geração e envio automático de relatórios por e-mail;

6.8.36 Caso seja utilizado soluções de terceiros para a geração de relatórios, estas devem ser homologadas pelo fornecedor dos equipamentos de rede.

7. ITEM 6 – SOLUÇÃO DE CONECTIVIDADE DE REDE SEGURA – CORE

7.1 CARACTERÍSTICAS GERAIS

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

7.1.1 Os equipamentos instalados devem ser novos.
7.1.2 Todos os componentes necessários para o correto funcionamento dos equipamentos ofertados devem ser fornecidos pela empresa eventualmente contratada;
7.1.3 Equipamento tipo comutador ethernet com capacidade de operação em camada 3 (Layer 3) do modelo OSI.
7.1.4 Deve possuir, no mínimo, 4 portas com suporte a 40 / 100 Gigabit Ethernet conforme padrão QSFP28.
7.1.5 Deve possuir, pelo menos, 24 interfaces SFP+ para conexão de fibras ópticas monomodo ou multimodo com velocidades de 10 Gigabit Ethernet.
7.1.6 Deve acompanhar 1 cabo DAC (Direct Attach Cable) para conexão entre duas portas de 100Gbps com pelo menos 1 metro de comprimento.
7.1.7 Caso a solução utilize KeepAlive, deve ser entregue com 01(um) cabo adicional do tipo DAC de no mínimo 3 metros de comprimento de 10Gbps de velocidade de conexão;
7.1.8 O switch deve apresentar arquitetura wire-speed ou non-blocking em todas as portas (capacidade de encaminhamento deve atender a soma das velocidades de todas as portas disponíveis no switch);
7.1.9 O switch deve ser do tipo standalone, com altura máxima de 1RU e instalação em rack (19”). Deve acompanhar todos os componentes necessários para sua fixação no rack;
7.1.10 Possuir LEDs para a indicação do status das portas e atividade;
7.1.11 Possuir porta de console para ligação direta, de terminal RS-232 ou RJ- 45 ou USB ou micro USB para acesso à interface de linha de comando.
7.1.12 Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V com comutação automática e que deverá ser capaz de sustentar a carga de todo o equipamento com todas as portas ativas;
7.1.13 Deve incluir fonte de alimentação redundante automática;
7.1.14 Deve possuir fontes de alimentação e ventiladores do tipo hot-swappable que possam ser trocados sem que seja necessário desligar o equipamento ou interromper seu funcionamento
7.1.15 Deverá ser fornecido com todos os acessórios necessários para operacionalização do equipamento, tais como software, cabos de console e cabos de energia elétrica;
7.1.16 Todas as portas devem estar licenciadas para uso.
7.1.17 Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento;
7.1.18 Os equipamentos, materiais e produtos a serem fornecidos deverão atender a todas as Normas e Resoluções da Agência Nacional de Telecomunicações - ANATEL de acordo com a Resolução nº 242 ou superior;

7.2 CARACTERÍSTICAS DE DESEMPENHO
7.2.1 Possuir backplane de, no mínimo, 1.2 Tbps.
7.2.2 O equipamento deve ter capacidade mínima de encaminhamento de 940 Mpps.
7.2.3 Possuir capacidade para pelo menos 140.000 endereços MAC na tabela de comutação;
7.2.4 Deve implementar, no mínimo, 1.000 VLANs simultaneamente, compatíveis com o padrão IEEE 802.1q;
7.2.5 Deve possuir buffer de pacotes (Packet Buffer) com capacidade de pelo menos 30 MB;

7.3 CARACTERÍSTICAS DE FACILIDADES
7.3.1 A arquitetura deve permitir “Cluster” de Switches (par de switches) em que dois (02)

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

switches interligados operem em conjunto."

7.3.2 Deve implementar a solução de MC-LAG (MultiChassis Link Aggregation Group) ou tecnologia semelhante que possibilite funcionalidade idêntica, em que mesmo havendo conexões entre diferentes equipamentos pertencentes ao mesmo par de switches, seja disponibilizado somente um único caminho lógico e agregado de comunicação, eliminando desta forma a necessidade do uso do protocolo STP (Spanning Tree Protocol).

7.3.3 O par de switches deve operar em alta-disponibilidade e possibilitar o upgrade de software sem que haja a parada do ambiente, com a mudança de tráfego entre os switches, caso necessário;

7.3.4 Deve implementar ERPS (Ethernet Ring Protection Switching)

7.3.5 Permitir a virtualização das tabelas de roteamento em camada 3 através de VRFs “Virtual Routing and Forwarding” ou VRF-Lite;

7.3.6 Implementar o protocolo NTP (Network Time Protocol);

7.3.7 Deve suportar o protocolo IPv6;

7.3.8 Deve implementar os protocolos Device Link Detection Protocol (DLDP), Unidirectional Link Detection (UDLD) ou protocolo similar para detecção de tráfego unidirecional com o objetivo de prevenir loops na rede;

7.3.9 Deve implementar Virtual Extensible LAN (VXLAN);

7.4 CARACTERÍSTICAS DE PADRÕES

7.4.1 Implementar padrão IEEE 802.1d (Spanning Tree Protocol);

7.4.2 Implementar padrão IEEE 802.1w (Rapid spanning Tree Protocol);

7.4.3 Implementar padrão IEEE 802.1s (Multi-Instance Spanning-Tree), com suporte a, no mínimo, 16 instâncias simultâneas do protocolo Spanning-Tree;

7.4.4 Implementar padrão IEEE 802.1Q (Vlan Frame Tagging);

7.4.5 Implementar padrão IEEE 802.1p (Class of Service);

7.4.6 Implementar padrão IEEE 802.3ad (LACP);

7.4.7 Permitir a descoberta de outros dispositivos na rede de forma automática através do protocolo LLDP (IEEE 802.1AB) ou semelhantes;

7.4.8 Deve suportar LLDP MED

7.5 FUNCIONALIDADES DE CAMADA 2

7.5.1 Deve implementar funcionalidade que permita a detecção de links unidirecionais conforme RFC 5171;

7.5.2 Deve implementar funcionalidade que permita a detecção de falhas de uplink;

7.5.3 Deve implementar jumbo frame 9.000 Bytes;

7.5.4 Deve implementar espelhamento de portas para monitoramento do tráfego de TX e RX de forma simultânea (Inbound/Outbound);

7.5.5 Deve implementar BPDU com suporte a tunelamento;

7.5.6 Deve implementar agregação de links através de LACP conforme IEEE 802.3ad;

7.5.7 Deve implementar link aggregation com suporte a 50 grupos com até 8 portas por LAG;

7.5.8 Deve implementar IEEE 802.1AB (LLDP) Link Layer Discovery Protocol;

7.5.9 Deve implementar IEEE 802.1d (STP) Spanning Tree Protocol;

7.5.10 Deve implementar IEEE 802.1w (RSTP) Rapid Spanning Tree Protocol;

7.5.11 Deve implementar IEEE 802.1s (MSTP) Multiple Spanning Tree Protocol;

7.5.12 Deve implementar Rapid Per-VLAN spanning tree (RPVST+);

7.5.13 Deve implementar ICMP Router Discovery Messages

7.5.14 Deve implementar IEEE 802.1ak (MVRP) Multiple VLAN Registration Protocol.

7.6 FUNCIONALIDADES DE CAMADA 3

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

7.6.1 Implementar roteamento estático IPv4 e IPv6;
7.6.2 Implementar roteamento dinâmico RIPv2 e RIPng;
7.6.3 Implementar protocolo de roteamento dinâmico OSPF;
7.6.4 Deve implementar OSPF com “Graceful Restart”, que permita o encaminhamento de pacotes mesmo que o software de OSPF seja reiniciado;"
7.6.5 Implementar mecanismo de análise de indisponibilidade de um vizinho OSPF por meio de LSA (link-state advertisements)
7.6.6 Deve implementar roteamento OSPF com suporte a autenticação MD5 ou texto claro;
7.6.7 Deve implementar roteamento OSPF com ECMP (Equal Cost MultiPath) de no mínimo, 8 caminhos balanceados;
7.6.8 Implementar protocolo de roteamento BGPv4;
7.6.9 Suportar, ao menos, 20.000 rotas BGP;
7.6.10 Implementar o protocolo VRRP ou mecanismo similar de redundância de gateway;
7.6.11 Deve suportar ao menos 250 grupos VRRP por switch;
7.6.12 Implementar VRRP, suportando ao menos 8 endereços IPV4 por grupo VRRP e ao menos 4 endereços IPV6 por grupo VRRP;
7.6.13 Deve suportar ao menos 8 grupos VRRP em uma única interface;
7.6.14 Deve implementar VRF, permitindo a vinculação de rotas estáticas IPV4 e IPV6 a cada uma das VRFs;
7.6.15 Implementar roteamento baseado em política (Policy-based Routing);
7.6.16 Deve implementar DHCP Client e DHCP Relay
7.6.17 Deve implementar funcionalidade que especifica o número máximo de entradas no ARP;
7.6.18 Deve suportar VTEP routing

7.7 QUALIDADE DE SERVIÇO (QoS):

7.7.1 Possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p;
7.7.2 Deve permitir a configuração do volume de broadcast, Multicast e unicast desconhecido aceito por porta, o excesso deve ser descartado;
7.7.3 Uma vez classificado o tráfego, o equipamento deve marcar os seguintes campos: Class of Service (CoS) e Differentiated Services Code Point (DSCP).
7.7.4 Deve possuir algoritmos de enfileiramento SP e WRR ou WFQ ou DWRR
7.7.5 Deve suportar PFC (Piority Flow Control) e DCBX (DCB Exchange Protocol), visando minimizar perdas de pacotes quando ocorre overflow de filas;

7.8 MULTICAST

7.8.1 Deve implementar PIM-SM e PIM-DM
7.8.2 Deve implementar IGMP nas versões v2 e v3 e Snooping;
7.8.3 Deve implementar MLD Snooping;
7.8.4 Deve implementar MSDP
7.8.5 Deve implementar gateway mDNS;

7.9 GERENCIAMENTO

7.9.1 Implementar os padrões abertos de gerência de rede SNMP v2/ v2c e v3, incluindo geração de traps;
7.9.2 Implementar MIB privativa que forneça informações relativas ao funcionamento do equipamento;
7.9.3 Possuir descrição completa da MIB implementada no equipamento;
7.9.4 Possibilitar a obtenção via SNMP de, no mínimo, informações de alarmes RMON, Agent Porf, VRFe Trap;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

7.9.5 Ser configurável e gerenciável via CLI (Command Line Interface) e SSHv2;
7.9.6 Deve suportar NTP (Network Time Protocol);
7.9.7 Deve suportar NTP com mecanismo de segurança e autenticação MD5;
7.9.8 Deve suportar os protocolos TFTP (Trivial File Transfer Protocol) e SFTP (Secure File Transfer Protocol);
7.9.9 Permitir a gravação de log externo (syslog);
7.9.10 Possuir 1 porta 10/100/1000BaseT, com conector RJ-45, exclusivamente para gerência do equipamento;
7.9.11 Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace e log de eventos;
7.9.12 Deverá acompanhar licença específica para software de gerenciamento gráfico para a família do equipamento com direito de atualização durante a vigência da garantia do equipamento.

7.10 SEGURANÇA

7.10.1 Implementar mecanismo de AAA (Authentication, Authorization e Accounting) para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS/TACACS+ e RADIUS;
7.10.2 Deve suportar ao menos 2 tipos de contas de usuários: Operadores e administradores
7.10.3 Deve permitir a criação de listas de acesso (ACLs), internamente ao equipamento, baseadas em endereço IP de origem, endereço IP de destino, portas TCP e UDP, VLAN ID e MAC;
7.10.4 As políticas de classificação de tráfego (Acl) devem ser aplicadas por porta, por interface link aggregation e por VLAN.
7.10.5 Deve implementar ACL´s IPv4 e IPv6;
7.10.6 Deve ser possível habilitar o log das ACLs IPv4;
7.10.7 Implementar funcionalidade para controle do volume de tráfego unknown unicast, multicast e broadcast com limites definidos pelo administrador;
7.10.8 Implementar mecanismo para suspensão do recebimento de BPDUs (Bridge Protocol Data Units) em uma determinada porta do switch;
7.10.9 Deverá suportar autenticação Radius através de TLS (RADSEC)
7.10.10 Deverá suportar servidor e cliente SSH;

7.11 Software Defined Networking:

7.11.1 Deve possuir tecnologia que permite a separação do plano de dados (encaminhamento de pacotes) e do plano de controle;
7.11.2 Deve permitir a automação de tarefas de reconfiguração da rede mediante eventos que impactem o seu comportamento através de scripts internos ou ferramentas externas que neste caso deverão ser fornecidas;
7.11.3 Deve possuir interface REST API;
7.11.4 Deve suportar configurações via REST API com, no mínimo, os seguintes métodos: GET, POST, PUT e DELETE;
7.11.5 Deverá permitir escritas de scripting via Python
7.11.6 Deve possuir embarcado ferramenta customizável e programável para monitoração e análise de eventos que possa auxiliar na identificação e correção de problemas de redes, aplicações e eventos de segurança da informação. Caso não possua este recurso é possível entregar uma ferramenta similar, podendo ser composto por hardware ou software adicional;
7.11.7 Suporte nativo ao protocolo “open vSwitch Database” (OVSDB);
7.11.8 Suporte a configuração estática de VXLAN, de forma a pertimir a um operador

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

manualmente conectar dois ou mais endpoints de túneis VXLAN (VTEP – VXLAN Tunnel Endpoints);

7.11.9 Suporte a configuração dinâmica de VXLAN com BGP-EVPN (Border Gateway Protocol - Ethernet Virtual Private Network);

7.12 CARACTERÍSTICAS DE GERENCIAMENTO CENTRALIZADO

7.12.1 A solução de gerenciamento deverá permitir acesso via plataforma centralizada, podendo ser oferecido em modelo SaaS (nuvem pública) ou on-premise (local), desde que garantida a disponibilidade, segurança e integração com os dispositivos gerenciados;

7.12.2 Caso a solução seja oferecida em modelo SaaS, todos os recursos de hardware, software, suporte, manutenção e segurança para funcionamento da solução deverão ser providos pelo fornecedor. Se on-premise, a CONTRATADA deverá fornecer as licenças e infraestrutura necessárias;

7.12.3 A solução de gerenciamento deverá ser acessível através de navegador WEB padrão, com criptografia de tráfego TLS 1.2 ou superior;

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

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

7.12.6 A solução de gerenciamento deverá permitir a gestão, monitoramento e ferramentas de diagnóstico para switches e pontos de acesso de rede sem fio, através de um único painel;

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

7.12.8 Os certificados digitais utilizados para estabelecimento desta comunicação segura deverão estar armazenados em hardware específicos (TPM - Trusted Platform Module) nos dispositivos a serem gerenciados;

7.12.9 As URLs de destino necessárias para estabelecimento da comunicação com os dispositivos a serem gerenciados deverão ser disponibilizadas;

7.12.10 A solução de gerenciamento deverá encaminhar por e-mail o convite para o usuário concluir seu cadastro, incluindo a definição de senha, para acesso a plataforma, assim que seu e-mail for incluído como novo usuário;

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

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

7.12.13 Deve disponibilizar aplicativo gratuito através das lojas oficiais (App Store e Google Play);

7.12.14 A utilização do aplicativo para ativação deverá ser controlada, permitindo definir, o usuário, localidade, data e hora em que poderá ser realizada;

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

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

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

7.12.17 Toda a configuração, bem como a versão de software em que os equipamentos deverão utilizar, deverão ser automaticamente enviadas após a conclusão da implantação através do aplicativo;
7.12.18 Os equipamentos deverão permitir o acesso local, sem necessidade de abertura de chamado técnico com o fabricante, para realização das configurações iniciais para acesso a solução de gerenciamento, nos casos em que não houver serviço de configuração dinâmica de endereços IPs para acesso à Internet;
7.12.19 Toda a solução de gerenciamento deverá estar disponível em Português, permitindo alternar para o Inglês conforme desejado pelo operador;
7.12.20 A solução de gerenciamento deve permitir a configuração baseada em grupos, permitindo que em um mesmo grupo possam ser definidas graficamente as configurações para switches e pontos de acesso de rede sem fio;
7.12.21 As configurações do grupo ao qual o equipamento está associado deverão ser substituídas pelas configurações associadas ao equipamento específico (interfaces, VLAN, endereçamento IP, gateway, hostname);
7.12.22 Os grupos devem permitir dois modos de configuração dos equipamentos, interface gráfica e através de templates em arquivos de linha de comando;
7.12.23 Os arquivos templates em linha de comando deverão permitir a criação de variáveis e condicionantes para definição de parâmetros da configuração
7.12.24 Deverá permitir a visualização das diferenças de configuração entre o arquivo template e a configuração vigente no equipamento;
7.12.25 Deverá permitir que os equipamentos sejam movimentados entre grupos diferentes, assumindo sempre a configuração do grupo de destino;
7.12.26 Deverá permitir que as configurações sejam salvas através de acesso direto aos equipamentos via FTP, SFTP e TFTP;
7.12.27 Deverá promover o ZTP (Zero Touch Provisioning) das configurações de equipamentos sem necessidade de acesso local;
7.12.28 Deverá permitir a configuração de política de conformidade de versão de software dos equipamentos por grupo de configuração;
7.12.29 Deverá executar a atualização de software automática quando o equipamento for associado ao grupo de destino, obedecendo a versão definida na política de conformidade;
7.12.30 Deverá permitir programar a atualização de software por localidade, definindo a data e horário para execução;
7.12.31 Deverá possuir API (Application Programming Interface) aberta que permita o acesso e integração a solução de gerenciamento, não só para monitoramento, mas também para configuração dos equipamentos e seus grupos;
7.12.32 Deverá possuir Streaming API, que permita o envio de informações a partir da solução de gerenciamento sem depender de requisições externas, entre elas:
7.12.32.1 Auditoria (conexão, configuração e firmware de equipamentos)
7.12.32.2.Monitoramento (status e estatísticas) de clientes
7.12.33 Deverá permitir o encaminhamento de alertas utilizando e-mail e WEBHOOK, considerando, no mínimo, os seguintes escopos de alertas para encaminhamento:
7.12.33.1 Alertas de Usuários
7.12.33.2. Alertas de Switches
7.12.33.3. Alertas de conectividade com a solução de gerência

7.12.33.4. Alertas de auditoria

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

7.12.33.5. Alertas de localidade

7.12.34 Deverá permitir a integração, através de API, com solução que permita validar a experiência dos usuários no acesso aos recursos de rede e aplicações internas, externas (SaaS) e customizadas, permitindo visibilidade do status verificado nos últimos 5 minutos através do dashboard por localidades.

7.12.35 Funcionalidade de relatórios:

8.12.35.1 Capacidade de geração de relatório para armazenagem de informações;

8.12.35.2 Coleta de informações da rede por períodos pré-definidos;

7.12.35.3. Capacidade de geração e envio automático de relatórios por e-mail;

7.12.36 Caso seja utilizado soluções de terceiros para a geração de relatórios, estas devem ser homologadas pelo fornecedor dos equipamentos de rede.

8. ITEM 7 – SOLUÇÃO DE CONECTIVIDADE DE REDE SEGURA - TIPO WI-FI

8.1 CARACTERÍSTICAS GERAIS

8.1.1 Equipamento de Ponto de Acesso para rede local sem fio com três rádios, configurável via software, com funcionamento simultâneo nos padrões IEEE 802.11a/n/ac/ax/be em 5GHz, padrão IEEE 802.11ax/be em 6GHz, e IEEE 802.11b/g/n/ax/be em 2.4GHz;

8.1.2 Os pontos de acesso deverão possuir certificado emitido pelo "WIFI Alliance" comprovando os seguintes padrões, protocolos e funcionalidades:

8.1.2.1 IEEE 802.11a;
8.1.2.2 IEEE 802.11b;
8.1.2.3 IEEE 802.11g;
8.1.2.4 IEEE 802.11n;
8.1.2.5 IEEE 802.11ac;
8.1.2.6 IEEE 802.11ax (Wi-Fi 6) – Obrigatório;
8.1.2.7 Wi-Fi 802.11be (Wi-Fi 7) – Desejável (será considerado como fator de classificação técnica ou desempate, se aplicável);
8.1.2.8 WPA Enterprise/Personal (SAE);
8.1.2.9 WPA2 Enterprise/Personal (SAE);
8.1.2.10 WPA3 Enterprise/Personal (SAE);
8.1.2.11 Enhanced Open (OWE);
8.1.2.12 WMM, WMM-PS, Wi-Fi Agile Multiband;

8.1.3 Deve possuir instalado interno ao Ponto de Acesso um módulo de confiança para maior garantia do dispositivo, para armazenamento seguro de credenciais e chaves, além de código de inicialização.

8.2 ESPECIFICAÇÕES DE RADIO

8.2.1 Deve permitir, simultaneamente, usuários configurados nos padrões IEEE 802.11a, 802.11b, 802.11g, 802.11n, 801.11ac, 802.11ax e 802.11be;

8.2.2 Implementar as seguintes taxas de transmissão (Mbps) e com fallback automático:

8.2.3 802.11b: 1, 2, 5.5, 11;
8.2.4 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54;
8.2.5 802.11n: 6.5 a 300 (MCS0 a MCS15, HT20 a HT40);
8.2.6 802.11ac: 6.5 a 860 (MCS0 a MCS9, NSS = 1 a 2, VHT20 a VHT-80);
8.2.7 802.11ax: 7.3 a 2,400 (MCS0 a MCS11, NSS = 1 a 2, HE20 a HE160);
8.2.8 802.11be: 7.3 a 5,760 (MCS0 a MCS13, NSS = 1 a 2, EHT20 a EHT320);
8.2.9 Deve suportar 802.11n high-throughput (HT): HT20/40;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

8.2.10 Deve suportar 802.11ac very high throughput (VHT): VHT20/40/80/160(80+80);
8.2.11 Deve suportar 802.11ax high efficiency (HE): HE20/40/80/160;
8.2.12 Deve suportar 802.11be extreme high throughput (EHT): HE20/40/80/160/320;
8.2.13 Deve suportar 802.11n/ac packet aggregation: A-MPDU, A-MSDU;
8.2.14 Operar nas seguintes tecnologias de rádio:
8.2.14.1 802.11b: direct-sequence spread-spectrum (DSSS);
8.2.14.2 802.11a/g/n/ac: Orthogonal frequency-division multiplexing (OFDM);
8.2.14.3 802.11ax/be: Orthogonal frequency-division multiple access (OFDMA);
8.2.15 Operar nos seguintes tipos de modulação:
8.2.15.1 802.11b: BPSK, QPSK, CCK;
8.2.15.2 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM;
8.2.15.3 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM;
8.2.15.4 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM;
8.2.15.5 802.11be: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM, 4096-QAM;
8.2.16 Possuir capacidade de selecionar automaticamente o canal de transmissão - DFS;
8.2.17 Deve implementar 802.11ax TWT (Target Wait Time) para suportar dispositivos de baixa potência;
8.2.18 Deve implementar 802.11mc/az FTM (Fine Timing Measurement) para alcance de distância de precisão;
8.2.19 Suportar até 512 clientes associados por rádio;
8.2.20 Possuir suporte a pelo menos 16 SSIDs por rádio;
8.2.21 Possuir antenas integradas ao equipamento, com padrão de irradiação omnidirecional, tri-band, com ganho de, pelo menos, 5.0 dBi em 2.4GHz, com ganho de, pelo menos, 5.4 dBi em 5GHz, e com ganho de, pelo menos, 5.2 dBi em 6GHz;
8.2.22 Deve suportar, utilizando a modulação OFDMA, a capacidade de transmitir simultaneamente clientes por canal, com as seguintes possibilidades:
8.2.23 Deve suportar utilização das três bandas 2.4GHz, 5GHz e 6GHz, permitindo uma flexibilidade máxima na seleção de canais de 5 GHz e 6 GHz sem degradação do desempenho;
8.2.24 Deve permitir funcionamento simultâneo de duas interfaces IOT, podendo ser duas interfaces BLE simultaneamente ou uma interface BLE e uma interface Zigbee simultaneamente;
8.2.25 Deve possuir uma interface Bluetooth Low Energy (BLE 5.4) integrada, com as seguintes características:
8.2.25.1 No mínimo 9dBm de potência de transmissão e -105 dBm de sensibilidade de recepção de sinal;
8.2.26 Deve possuir uma interface IoT (Internet of Things) tipo Zigbee (802.15.4), Lora ou similar integrada, com as seguintes características:
8.2.26.1 No mínimo 9dBm de potência de transmissão (class 1) e -100 dBm de sensibilidade de recepção de sinal;
8.2.27 Deve operar em 2.4GHz, 5GHz e 6GHz simultaneamente conforme o padrão 802.11be com MIMO 2x2;
8.2.28 Deve suportar operação em 2.4GHz com 02 (dois) Spatial Streams MIMO, com taxa de transmissão de dados de até 680Mbps;
8.2.29 Deve suportar operação em 5GHz com 02 (dois) Spatial Streams MIMO, com taxa de transmissão de dados de até 2.8 Gbps;
8.2.30 Deve suportar operação em 6GHz com 02 (dois) Spatial Streams MIMO, com taxa de transmissão de dados de até 5.7 Gbps;
8.2.31 Deve suportar Multi User MIMO (UM-MIMO) com downlink e uplink em todos os rádios;
8.2.32 Os equipamentos APs devem possuir funcionalidade de coexistência com redes

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

celulares de forma a minimizar as interferências das mesmas;
8.2.33 Possuir potência máxima de transmissão para frequências de 2.4GHz 5GHz e 6GHz de 20 dBm;
8.2.34 Capacidade de configurar a potência de transmissão em incrementos de pelo menos 1 dBm;

8.3 MODOS DE OPERAÇÃO
8.3.1 Deve permitir funcionamento em modo autônomo/standalone, e também deve permitir funcionamento em modo com gateway/controladora;
8.3.2 Deve permitir o gerenciamento através de plataforma nuvem (cloud).
8.3.3 Para implementações em larga escala, o Ponto de Acesso deve implementar a funcionalidade sem intervenção, também conhecida como Zero Touch Provisioning (ZTP);

8.4 OUTRAS INTERFACES
8.4.1 Possuir LEDs multicoloridos indicativos do estado de operação e da atividade do rádio;
8.4.2 Deve possuir, pelo menos, 02 (duas) interfaces de rede SmartRate/Multigigabit (RJ-45) com velocidade auto-sensing 100/1000/2500/5000BASE-T com as seguintes características:
8.4.2.1 Auto-sensing link speed (100/1000/2500/5000BASE-T) e MDI/MDX;
8.4.2.2 PoE-PD: 48Vdc (nominal) 802.3at/802.3bt (classe 4 ou superior);
8.4.2.3 802.3az Energy Efficient Ethernet (EEE);
8.4.3 Suportar a funcionalidade de link aggregation (LACP) nas portas de uplink para redundância ou aumento de capacidade;
8.4.4 Suportar a funcionalidade de MACsec em uma das portas, conforme o padrão 802.1ae;
8.4.5 Deve operar em condições de temperatura entre 5ºC e 45ºC, e umidade entre 10% e 90%;
8.4.6 Deve possuir MTBF (Mean Time Between Failure (MTBF) de no mínimo 630.000 (seiscentos e trinta e cinco mil) horas;
8.4.7 Possuir botão de reset que permita reset de fábrica do equipamento;
8.4.8 Possuir porta de console para gerenciamento e configuração via linha de comando CLI;
8.4.9 Deve possuir duas interfaces USB2.0;
8.4.10 Possuir slot de segurança Kensington;
8.4.11 Deve possuir funcionalidade de desligamento térmico e recuperação automático;
8.4.12 Possuir estrutura que permita fixação do equipamento e fornecer acessórios para que possa ser feita a fixação;
8.4.13 Possuir kits de montagem opcionais para instalar o AP em variedade de superfícies;

8.5 SEGURANÇA E REGULAMENTAÇÃO
8.5.1 O equipamento deverá possuir registro na ANATEL;
8.5.2 O certificado da ANATEL deverá ser apresentado na entrega do equipamento;

8.6 CARACTERÍSTICAS DE GERENCIAMENTO CENTRALIZADO
8.6.1 A solução de gerenciamento deverá permitir acesso via plataforma centralizada, podendo ser oferecido em modelo SaaS (nuvem pública) ou on-premise (local), desde que garantida a disponibilidade, segurança e integração com os dispositivos gerenciados;
8.6.2 Caso a solução seja oferecida em modelo SaaS, todos os recursos de hardware, software,

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

suporte, manutenção e segurança para funcionamento da solução deverão ser providos pelo fornecedor. Se on-premise, a CONTRATADA deverá fornecer as licenças e infraestrutura necessárias;

8.6.3 A solução de gerenciamento deverá ser acessível através de navegador WEB padrão, com criptografia de tráfego TLS 1.2 ou superior;

8.6.4 Todo acesso deverá ser controlado com autenticação de usuário em base própria e também externa utilizando para isso Single-Sign-on através do protocolo SAML;

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

8.6.6 A solução de gerenciamento deverá prover tutoriais interativos como guia para acesso as facilidades básicas, incluindo no mínimo, criação de usuários e roles, configuração e gestão de redes, monitoramento de equipamentos e redes, diagnósticos e interface de usuário;

8.6.7 A solução de gerenciamento deverá permitir a gestão, monitoramento e ferramentas de diagnóstico para access points, controladoras wi-fi e Switches, através de um único painel;

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

8.6.9 Os certificados digitais utilizados para estabelecimento desta comunicação segura deverão estar armazenados em hardware específicos (TPM - Trusted Platform Module) nos dispositivos a serem gerenciados;

8.6.10 As URLs de destino necessárias para estabelecimento da comunicação com os dispositivos a serem gerenciados deverão ser disponibilizadas;

8.6.11 A solução de gerenciamento deverá encaminhar por e-mail o convite para o usuário concluir seu cadastro, incluindo a definição de senha, para acesso a plataforma, assim que seu e-mail for incluído como novo usuário;

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

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

8.6.14 Deve disponibilizar aplicativo gratuito através das lojas oficiais (App Store e Google Play);

8.6.15 A utilização do aplicativo para ativação deverá ser controlada, permitindo definir, o usuário, localidade, data e hora em que poderá ser realizada;

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

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

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

8.6.19 Os equipamentos deverão permitir o acesso local, sem necessidade de abertura de chamado técnico com o fabricante, para realização das configurações iniciais para acesso a solução de gerenciamento, nos casos onde não houver serviço de configuração dinâmica de endereços IPs para acesso à Internet;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

8.6.20 Toda a solução de gerenciamento deverá estar disponível em Português, permitindo alternar para o Inglês conforme desejado pelo operador;
8.6.21 A solução de gerenciamento deve permitir a configuração baseada em grupos, permitindo que em um mesmo grupo possam ser definidas graficamente as configurações para switches e pontos de acesso WI-FI e controladoras;
8.6.22 As configurações do grupo ao qual o equipamento está associado deverão ser substituídas pelas configurações associadas ao equipamento específico (interfaces, VLAN, endereçamento IP, gateway, hostname);
8.6.23 Os grupos devem permitir dois modos de configuração dos equipamentos, interface gráfica e através de templates em arquivos de linha de comando;
8.6.24 Os arquivos templates em linha de comando deverão permitir a criação de variáveis e condicionantes para definição de parâmetros da configuração
8.6.25 Deverá permitir a visualização das diferenças de configuração entre o arquivo template e a configuração vigente no equipamento;
8.6.26 Deverá permitir que os equipamentos sejam movimentados entre grupos diferentes, assumindo sempre a configuração do grupo de destino;
8.6.27 Deverá permitir que as configurações sejam salvas através de acesso direto aos equipamentos via FTP, SFTP e TFTP;
8.6.28 Deverá promover o ZTP (Zero Touch Provisioning) das configurações de equipamentos sem necessidade de acesso local;
8.6.29 Deverá permitir a configuração de política de conformidade de versão de software dos equipamentos por grupo de configuração;
8.6.30 Deverá executar a atualização de software automática quando o equipamento for associado ao grupo de destino, obedecendo a versão definida na política de conformidade;
8.6.31 Deverá permitir programar a atualização de software por localidade, definindo a data e horário para execução;
8.6.32 Deverá possuir API (Application Programming Interface) aberta que permita o acesso e integração a solução de gerenciamento, não só para monitoramento, mas também para configuração dos equipamentos e seus grupos;
8.6.33 Deverá possuir Streaming API, que permita o envio de informações a partir da solução de gerenciamento sem depender de requisições externas, entre elas:
8.6.33.1 Auditoria (conexão, configuração e firmware de equipamentos)
8.6.33.2 Localização (coordenadas de localização de clientes WI-FI)
8.6.33.3 Fluxo de sessões (sessões WEB dos clientes conectados através do WI-FI e gateway SD-WAN)
8.6.33.4 Monitoramento (status e estatísticas) de clientes
8.6.33.5 Presença (detalhes de clientes conectados e não conectados a rede WI-FI)
8.6.33.6 Segurança (reportar alertas de WIDS)"
8.6.34 Deverá permitir o encaminhamento de alertas utilizando e-mail e WEBHOOK, considerando, no mínimo, os seguintes escopos de alertas para encaminhamento:
8.6.34.1 Alertas de Usuários
8.6.34.2 Alertas de Pontos de Acesso WI-FI
8.6.34.3 Alertas de Switches
8.6.34.4 Controladoras
8.6.34.5 Alertas de conectividade com a solução de gerência
8.6.34.6 Alertas de auditoria
8.6.34.7 Alertas de localidade
8.6.35 Deverá identificar o dispositivo conectado a rede através da rede WIFI, expondo os

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

seguintes parâmetros:
8.6.35.1 Categoria
8.6.35.2 Família
8.6.35.3 Sistema Operacional
8.6.35.4 Atributos de fluxo de tráfego por dispositivo:
8.6.35.5 Destinos acessados e host de destino
8.6.35.6 Aplicações e grupos de aplicações
8.6.36 Deverá permitir a integração, através de API, com solução que permita validar a experiência dos usuários no acesso aos recursos de rede e aplicações internas, externas (SaaS) e customizadas, permitindo visibilidade do status verificado nos últimos 5 minutos através do dashboard por localidades.
8.6.37 Funcionalidade de relatórios:
8.6.37.1 Capacidade de geração de relatório para armazenagem de informações;
8.6.37.2 Coleta de informações da rede por períodos de tempo pré-definidos;
8.6.37.3 Capacidade de geração e envio automático de relatórios por e-mail;
8.6.37.4 Caso seja utilizado soluções de terceiros para a geração de relatórios, estas devem ser homologadas pelo fornecedor dos equipamentos de rede.
8.6.38 Funcionalidade de Gerenciamento de Convidados (Guests)
8.6.38.1 Deve possuir recurso de gerenciamento de convidados permite que os usuários convidados se conectem à rede e, ao mesmo tempo, permite que o administrador controle o acesso dos usuários convidados à rede.
8.6.38.2 Os administradores podem criar um perfil de página inicial para seus usuários convidados.
8.6.38.3 Deve permitir a personalização do layout da página inicial (vertical ou horizontal) com base no tipo de dispositivo.
8.6.38.4 Permitir que os convidados acessem a Internet fornecendo as credenciais configuradas pelos operadores convidados ou suas respectivas credenciais de login na rede social.
8.6.38.5 Permitir acesso utilizando logins sociais das redes Facebook, Google, Twitter, and LinkedIn
8.6.38.6 Deve permitir o serviço Wi-Fi do Facebook, de forma que os usuários que se conectam a hotspots Wi-Fi sejam apresentados a uma página de negócios antes de obter acesso à rede.
8.6.38.7 A ferramenta deve ter capacidade de criar uma conta com permissão apenas de poder criar contas de usuários da rede Wi-Fi sem que tenha acesso as configurações dos elementos de rede ou outros serviços
8.6.38.8 Permitir a criação de contas de usuários da rede Wi-Fi com prazos de tempo
8.6.38.9 Deve permitir que os visitantes ou usuários convidados podem se registrar usando a página inicial ao tentar acessar a rede. A senha é entregue aos usuários por meio de impressão, SMS ou e-mail dependendo das opções selecionadas durante o cadastro.
8.6.38.10 Deve fornecer as credenciais de login por meio de impressão, mensagens de texto SMS ou e-mail.

9. ITEM 8 – SOLUÇÃO DE MONITORAMENTO DE REDE

9.1 CARACTERÍSTICAS PRINCIPAIS

9.1.1.1 Trata-se de equipamento/sensor dedicado, destinado ao monitoramento físico de rede e experiência do usuário em tempo real;
9.1.1.2 Deve suportar solução baseada em nuvem (Cloud-based/SaaS);
9.1.1.3 Deve simular o acesso do usuário ou dispositivo único para teste em redes sem fio e com fio;
9.1.1.4 Deve possuir dashboard gráfica e amigável para possibilitar visibilidade de diagnóstico

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

de maneira intuitiva.
9.1.1.5 A solução deverá ser ofertada em modelo de appliance físico e dedicado para a função de análise de rede.
9.1.1.6 Soluções baseadas somente em agente, deverão fornecer o agente instalado em appliance físico com as características mínimas de hardware exigidas para este item.
9.1.1.7 Deve possuir recursos de IA para análise em tempo real de problemas possibilitando identificar a causa raiz de casos complexos para as redes WLAN e LAN;
9.1.1.8 Deve suportar a instalação de agentes em dispositivos Android, Windows e MAC.
9.1.1.9 Deve permitir integração através do celular para troubleshooting
9.1.1.10 Deve suportar testes para WI-FI, LAN, DHCP, DNS, Autenticação, Capitive portal, aplicações internas e em nuvem;
9.1.1.11 Deve identificar automaticamente se a rede que está sendo acessada possui um captive portal configurado;
9.1.1.12 Deve ser possível criar perfil de teste para acesso ao captive portal;
9.1.1.13 Deve suportar integração com a plataforma de gerenciamento de rede LAN e WLAN do mesmo fabricante;
9.1.1.14 Deve suportar diagnósticos de usuários e aplicativos.
9.1.1.15 Deve suportar captura de pacotes sob demanda ou quando ocorrerem incidentes, gerando arquivos PCAP.
9.1.1.16 Deve suportar pelo menos 3 SSIDs por sensor
9.1.1.17 Deve possuir funcionalidade que permita visualizar os saltos de camada 3 na WAN, do destino até a origem a aplicação, permitindo identificar gargalos ou caminhos com maior sensibilidade para determinadas aplicações.
9.1.1.18 Deve suportar a criação de testes predefinidos ou sob demanda para análise contínua de serviços de redes e aplicações;
9.1.1.19 Deve permitir que os resultados dos testes sejam enviados para plataformas de armazenamento e análise de dados como: AWS S3, Google BigQuery, Elasticsearch, Splunk, BigPanda, ServiceNow ou para um endpoint HTTP Genérico.
9.1.1.20 Deve ser possível gerar testes para serviços de VOIP com análise no padrão MOS;
9.1.1.21 Dede possuir capacidade de gerar relatórios sob demanda ou agendados, podendo incluir os resultados dos testes e os principais problemas e incidentes encontrados;
9.1.1.22 Deve ser possível configurar os relatórios para envio por e-mail e com período diário, semanal ou mensal;
9.1.1.23 Deve ser possível criar relatórios por redes ou grupos;

9.2 SEGURANÇA
9.1.1.1. Deve possuir os seguintes requisitos mínimos de segurança:
9.1.1.1.1. Criptografia SSL;
9.1.1.1.2. WPA2 PSK;
9.1.1.1.3. WPA2 Enterprise;
9.1.2. WPA3 SAE;INTERFACES COMPATÍVEIS
9.1.2.1. Wi-Fi 802.11n/AC/ AX de banda tripla (2,4, 5 e 6Ghz)
9.1.2.2. Deve possuir no mínimo uma interface Gigabit Ethernet 10/100/1000
9.1.2.3. Deve possuir uma interface BLE 5.1;

9.1.3. ALIMENTAÇÃO
9.1.3.1. Deve suportar os seguintes padrões de alimentação do dispositivo:
9.1.3.2. Power over Ethernet (PoE) – 802.3af
9.1.3.3. Adaptador CA

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

9.1.4. AMBIENTAL

9.1.4.1. Deve suportar os seguintes padrões de operação:

9.1.4.2. Temperatura de operação: de 0 a 40

9.1.4.3. Umidade: 5% a 93% sem condensação

9.1.5. MONTAGEM

9.1.5.1. Deve suportar montagem na parede ou no teto.

9.1.6. REGULAMENTAÇÃO

9.1.6.1. Deve possuir certificação Anatel

10. ITEM 9 – SOLUÇÃO DE SEGURANÇA DE ACESSO A REDE

10.1 Solução de autenticação de usuários e dispositivos para controle de acesso a rede baseada em appliance físico ou virtual, sendo compatível com os seguintes Hypervisors:

10.1.1 vmware ESXi 7.0 ou superior;

10.1.2 Hyper-V em Windows Server 2019 ou superior;

10.1.3 KVM em Ubuntu 20.04LTS ou superior;

10.2 Cada item contratado da solução deverá permitir autenticação de até 1000 dispositivos conectados à rede de formas simultânea.

10.3 Possuir plataforma unificada que combina acesso de convidado incorporando identidade, informações físicas de dispositivo e elementos condicionais em um conjunto de políticas.

10.4 Suporte a seguintes fontes para autenticação:

10.4.1 Microsoft Active Directory

10.4.2 Kerberos

10.4.3 Base SQL interna

10.4.4 LDAP-compliant directory

10.4.5 Radius

10.4.6 Microsoft Azure Active Directory

10.4.7 Google G Suite

10.4.8 HTTP

10.4.9 Lista estática de endereços MAC

10.5 Deve suportar "Single Sign-on" (SSO) através de SAML v2.0 e/ou OpenID Connect e/ou OAuth 2.0

10.6 Deve implementar gerenciamento e aplicação de políticas de autorização de acesso de usuários com base em:

10.6.1 Atributos do usuário autenticado

10.6.2 Hora do dia, dia da semana

10.6.3 Tipo de dispositivo utilizado

10.6.4 Localização do usuário

10.6.5 Tipo de autenticação utilizado

10.7 Permitir a visualização de todas as informações relativas a cada transação/autenticação em uma única tela, como Data e Hora, Mac Address do dispositivo, classificação do dispositivo, Usuário, equipamento que requisitou a autenticação (origem), Método de autenticação utilizado, fonte de autenticação utilizada para validação, perfil de acesso aplicado, todos atributos de entrada do protocolo utilizados na requisição (ex. RADIUS), informações de resposta da solução para o elemento de rede, alertas em caso de falha, e exibição dos Log já filtrados para a requisição em análise

10.8 Deve possuir Dashboard customizável, onde deve permitir a visualização em forma de gráfico e/ou tabela de no mínimo as seguintes informações:

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

10.8.1 Lista com os últimos Alertas do sistema;
10.8.2 Requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ e Web Authentication;
10.8.3 Status das autenticações aceitas e rejeitadas nos últimos 7 dias;
10.8.4 Últimas falhas de autenticação;
10.8.5 Lista com as últimas autenticações;
10.8.6 Lista com as últimas autenticações com sucesso;
10.8.7 Utilização de CPU do sistema;
10.9 Deve implementar funcionalidade de classificação automática de dispositivos (device profiling), de forma a descobrir, classificar e agrupar os dispositivos conectados na rede;
10.10 Deve categorizar os dispositivos em pelo menos 3 níveis, por tipo de dispositivo (ex. computador, smart device, impressora, etc.), por sistema operacional (ex. Windows, Linux, MacOS etc.) e versão do sistema (ex. Windows 7, Windows 2008 Server etc.);
10.11 Deve suportar a coleta de informações, para classificação, usando no mínimo DHCP, HTTP User-Agent, MAC OUI, SNMP, Subnet Scanner e TCP Fingerprinting;
10.12 Caso exista licenciamento distinto para usuários/dispositivos da rede sem fio (wireless) e usuários/dispositivos da rede cabeada (wired), deverão ser fornecidas as duas licenças para o número total de usuários solicitados;
10.13 Deve permitir que cada dispositivo receba uma chave pré-compartilhada exclusiva durante o registro do dispositivo.
10.14 Deve suportar, no mínimo, 5 dos seguintes métodos de autenticação:
10.14.1 EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)
10.14.2 PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP- Public, EAP- PWD)
10.14.3 TTLS (EAP-MSCHAPv2, EAP-GTC, EAP- TLS, EAP-MD5, PAP, CHAP)
10.14.4 EAP-TLS
10.14.5 PAP, CHAP, MSCHAPv1, MSCHAPv2, e EAP-MD5
10.14.6 Windows Machine Authentication
10.14.7 SMB v2/v3
10.14.8 WPA3
10.14.9 MPSK e/ou DPSK
10.14.10 Autenticação WEB;
10.14.11 TACACS+;
10.15 Deve suportar EDUROAM;
10.16 Suporte a integração com plataforma de terceiros usando HTTP/RESTful API.
10.17 A solução deve possuir ferramenta para geração de relatórios de maneira centralizada, permitindo o agendamento e envio por e-mail em formato HTML e PDF.
10.18 Suporte aos seguintes recursos através de IPv6:
10.18.1 Administração via WEB e CLI
10.18.2 Servidores de autenticação e autorização com endereçamento IPv6;
10.18.3 Syslog, DNS, NTP;
10.18.4 Fontes de Syslog para processamento de eventos
10.19 A solução deve permitir a geração e o envio através de e-mail ou SMS de alertas relativos as seguintes atividades anormais detectadas na rede:
10.19.1 Autenticações
10.19.2 Acesso a dispositivos de rede
10.19.3 Atividades irregulares nos servidores da solução
10.20 Deve possuir ferramenta para gerenciar os processos de credenciamento, autenticação, autorização e contabilidade de usuários visitantes através de um portal web seguro;
10.21 Deve implementar a criação de grupos de autorizadores com privilégios distintos, por SSID, de criação de credenciais temporárias e atribuição de permissões de acesso aos clientes;
10.22 Deve realizar a autenticação dos autorizadores em base externa do tipo Microsoft Active Directory ou LDAP e atribuir o privilégio ao autorizador de acordo com o seu perfil;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

10.23 Deve implementar as funcionalidades de geração aleatória de lotes de credenciais temporárias pré-autorizadas;
10.24 Deve implementar a importação e exportação da relação de credenciais temporárias através de arquivos txt ou csv;
10.25 Deve permitir a criação de validade das credenciais, baseando o início da validade na criação da conta ou no primeiro login da conta;
10.26 Deve permitir que o visitante crie sua própria credencial temporária ("self-service") através do portal web, sem a necessidade de um autorizador;
10.27 Deve permitir a customização do formulário de criação de credenciais, a ser preenchido pelo autorizador ou pelo visitante, em caso de autosserviço, especificando quais informações cadastrais dos visitantes são obrigatórias ou opcionais;
10.28 Deve permitir a customização do nível de segurança da senha temporária que será gerada ao visitante, especificando a quantidade mínima de caracteres e o uso de caracteres especiais e números para compor a senha;
10.29 Deve exigir que o usuário visitante aceite o "Termo de uso da rede" a cada login ou apenas no primeiro login;
10.30 Deve permitir o envio das credenciais aos usuários registrados através de mensagens SMS (Short Message Service), e-mail e impressão local
10.31 Deve permitir que a customização da página de registro de visitantes para campos relacionados a confirmação de sponsorship;
10.32 Deve permitir o gerenciamento das credenciais de visitantes;
10.33 Deve permitir a configuração de contas de usuários visitantes com as seguintes características: prazo de validade, largura de banda;
10.34 Deve permitir o login automático de usuários que realizem o auto-registro;
10.35 Deve permitir a autenticação de usuário anônimo sem necessidade de prover usuário e senha;
10.36 Deve permitir a criação de token de acesso;
10.37 Deve permitir a criação e gerenciamento de múltiplas contas de usuários visitantes;
10.38 Deve permitir a desconexão de múltiplas sessões ativas;
10.39 Deve permitir autenticação através de social login nativa na solução;
10.40 Deve possuir funcionalidade para verificação das políticas de segurança implementadas nos dispositivos conectados a rede, através de agentes instalados ou temporários.
10.41 Para a verificação de postura, deve ter a capacidade de analisar até 1000 dispositivos simultaneamente;
10.42 Deve suportar a verificação, no mínimo, nos sistemas operacionais:
10.42.1 Windows 7 e superior;
10.42.2 Mac OSX 10.10 e superior;
10.42.3 Ubuntu 16.x LTS e superior;
10.42.4 Fedora Core 24 e superior;
10.42.5 SUSE 12.x e superior;
10.42.6 CentOS 5 e superior;
10.43 Permitir a execução do agente como serviço quando instalado em sistemas Windows;
10.44 Permitir o uso de agentes instalados nos dispositivos, ou agente temporários para o uso em dispositivos de terceiros que necessitem acesso a rede.
10.45 Permitir o gerenciamento centralizado das políticas, e permitir que os usuário/dispositivos que estiverem fora das políticas de segurança, sejam direcionados para um segmento de rede específico ou determinação de uma política de acesso restritiva, permitindo ainda que estes consigam se adequar a respectiva política através da remediação dos problemas;
10.46 Permitir que a solução realize a adequação da política (remediação) de forma automática, sem necessidade de intervenção do usuário.
10.47 Deve suportar a verificação de pelos menos os seguintes serviços:
10.47.1 Firewall

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

10.47.2 Conexões de rede
10.47.3 Windows Hotfixes
10.47.4 Aplicações instaladas
10.47.5 Serviços
10.47.6 Dispositivos USB
10.47.7 Processos
10.47.8 Checagem de arquivos
10.48 Deve suportar a verificação de antivírus com pelos menos os seguintes parâmetros:
10.48.1 Produto instalado
10.48.2 Versão instalada
10.48.3 Data da última atualização
10.48.4 Data da última verificação
10.49 A plataforma deve suportar a integração com SCCM ou WSUS.
10.50 Deve permitir a verificação de postura de dispositivos Windows 10 sem a necessidade de instalação prévia de agentes, executando todas as operações de verificação em "background", ou seja, transparente ao usuário final;
10.51 É permitida a composição de soluções para atendimento, desde que não sejam software livre/open source;

11. ITEM 10 – SOLUÇÃO DE SEGURANÇA DAS APLICAÇÕES

11.1 PROTEÇÃO DE APLICAÇÕES WEB E API

11.1.1 Implementar serviço em nuvem de proteção de ataques às aplicações web e APIs, disponíveis em qualquer infraestrutura pública ou privada, exposta para a Internet.
11.1.2 Implementar defesa automática de ataques de Distributed Denial-Of-Service (DDoS), protegendo continuamente todas as aplicações publicadas através do serviço contratado em nuvem.
11.1.3 Deve mitigar ataques de forma transparente para a aplicação, absorvendo e bloqueando ataques.Deve ser capaz de detectar ataques através da análise das taxas de requisição, erros, latência e throughput da aplicação.
11.1.4 Implementar proteção de ataques na camada de aplicação, incluindo os protocolos HTTP e DNS, incluindo, no mínimo, proteções de HTTP GET Flood, HTTP POST Flood, Slowloris e DNS Flood.
11.1.5 Implementar proteção de ataques volumétricos, incluindo SYN Flood, UDP Flood, TCP Flood e ICMP Flood.
11.1.6 Implementar proteção de ataques de negação de serviço através da exaustão de recursos (“Slow DDoS”), incluindo Slow POST e Slowloris.
11.1.7 Implementar proteção de ataques à pilha TCP.
11.1.8 Implementar proteção de ataques que utilizam falsificação de endereços IP de origem (IP spoofing).
11.1.9 Implementar detecção e mitigação automática de ataques em Camada 7 em larga escala.
11.1.10 Implementar proteção através de bloqueio geográfico e de, pelo menos, 95 (noventa e cinco) prefixos IP.
11.1.11 Permitir criar regras de bloqueio personalizadas.
11.1.12 Permitir configurar o bloqueio de clientes com base no TLS fingerprint.
11.1.13 Permitir configurar o bloqueio de clientes com base na classificação e reputação do IP.
11.1.14 Deve possuir, pelo menos, a classificação de IP para botnets, scanners, proxies anônimos, proxies ToR e origens conhecidas por ataques web.
11.1.15 Permitir configurar o bloqueio de clientes com base no ASN do BGP.
11.1.16 Permitir configurar de mitigações específicas por aplicação.
11.1.17 Implementar gestão automática de certificados digitais, incluindo a renovação dos

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

certificados, devendo possuir integração com no mínimo o serviço Let's Encrypt (https://letsencrypt.org/).

11.1.18 Permitir a gestão manual de certificados através da importação de certificado digital e chave privada da CONTRATANTE, devendo esta ser armazenada em repositório seguro e protegido.

11.1.19 Suportar OCSP.

11.1.20 Permitir a configuração de até 10 (dez) aplicações;

11.1.21 Suportar a configuração de até 32 (trinta e dois) domínios (FQDN) para uma mesma aplicação;

11.1.22 Suportar a gestão automática dos certificados de todos os domínios.

11.1.23 Suportar a gestão manual de certificados digitais e chaves privadas de todos os domínios.

11.1.24 Permitir a configuração de diferentes pools de servidores de origem da aplicação (origin servers) com algoritmos de balanceamento para escolha do pool.

11.1.25 Permitir configurar pesos e prioridades diferentes para cada pool de origin servers.

11.1.26 Permitir configurar um algoritmo de balanceamento de Origin Servers de um pool diferente do algoritmo de balanceamento de pools.

11.1.27 Permitir configurar monitores de disponibilidade de Origin Servers.

11.1.28 Permitir configurar persistência de Origin Pool por IP de origem.

11.1.29 Permitir a configuração de persistência do IP de origem da solução para uma mesma sessão de um usuário destinada para o mesmo Origin Server.

11.1.30 Permitir a configuração de diferentes pools de Origin Servers selecionados a partir de atributos da aplicação, incluindo no mínimo método HTTP, prefixos, expressões regulares da URL e cabeçalhos HTTP.

11.1.31 Permitir inserir cabeçalho HSTS (HTTP Strict-Transport-Security).

11.1.32 Implementar TLS 1.2 e superiores, com algoritmos fortes e cifras que suportem PFS (Perfect Forward Secrecy).

11.1.33 Implementar Mutual TLS (mTLS) com a opção de enviar o certificado do cliente como cabeçalho HTTP para o Origin Server.

11.1.34 Permitir especificar a lista de Autoridades Certificadoras (CA) de validação do certificado.

11.1.35 Permitir validar o certificado do cliente em uma lista de CAs diferente do CA que assina o certificado do servidor.

11.1.36 Permitir verificar o certificado do cliente em listas de revogação (CRL).

11.1.37 Permitir enviar o certificado completo como cabeçalho.

11.1.38 Suportar HTTP/1.1 e HTTP/2.

11.1.39 Implementar proteção de aplicações web com capacidade para tratar 29 (vinte e nove) milhões de requisições por mês.

11.1.40 Implementar inspeção e varredura com base em assinaturas para detecção de requisições maliciosas, incluindo, no mínimo proteções de:

11.1.40.1 Cross-Site Scripting (XSS);

11.1.40.2 Cross-Site Request Forgery (CSRF);

11.1.40.3 Directory Traversal;

11.1.40.4 Directory Climbing;

11.1.40.5 SQL injection;

11.1.40.6 Cookie Injection;

11.1.40.7 Command Injection;

11.1.40.8 Code Injection;

11.1.40.9 Web Parameter Tampering;

11.1.40.10 Cookie Tampering.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

11.1.41 Implementar a configuração para identificação e mascaramento de dados sensíveis enviados pelo servidor para o cliente.
11.1.42 Implementar detecção e mitigação de violações do protocolo HTTP.
11.1.43 Implementar proteção contra exploração de vulnerabilidade (exploit).
11.1.44 Implementar proteção contra adulteração de cookies do serviço de proteção de aplicações.
11.1.45 Permitir a configuração de políticas de segurança de permissão e bloqueio.
11.1.46 Permitir a criação de regras de exclusão de forma granular, considerando cookies, parâmetros, cabeçalhos e outros.
11.1.47 Permitir a configuração de regras de segurança positiva, onde será definido o que é permitido e todo o restante é rejeitado.
11.1.48 Permitir a configuração de políticas e regras que protejam as aplicações de ameaças e vulnerabilidades listadas no OWASP Top 10 e atualizações dessa lista.
11.1.49 Implementar proteções de campanhas de ataques e ameaças, informando a ação, o ator e a vulnerabilidade explorada.
11.1.50 Permitir criar diferentes políticas de segurança para inspeção e proteção por aplicação.
11.1.51 Permitir habilitar uma política de segurança sem bloqueios, ou seja, apenas para geração de alertas ou monitoramento.
11.1.52 Implementar mecanismos de ajuste automático de assinaturas para redução de falso-positivos.
11.1.53 Implementar fase de preparação de assinaturas de ataque, quando assinaturas novas e atualizadas são configuradas no modo de monitoramento por um período.
11.1.54 Permitir configurar exclusões para tipos de ataques específicos.
11.1.55 Permitir configurar exclusões para assinaturas de ataques específicas.
11.1.56 Permitir definir os códigos de respostas HTTP (status code) que serão aceitos vindos da aplicação original, quando os demais códigos serão bloqueados.
11.1.57 Permitir ocultar atributos e parâmetros sensíveis, tais como senhas ou outros dados sensíveis, em mensagens de log da plataforma.
11.1.58 Permitir a criação de diferentes páginas de respostas de bloqueio, fornecendo um identificador de requisição.
11.1.59 Permitir a criação de diferentes páginas de respostas por códigos de respostas HTTP (status code).
11.1.60 Implementar a identificação de usuários e clientes a partir de informações extraídas de cabeçalhos IP, HTTP, parâmetros, cookies, JWT e fingerprint do TLS.
11.1.61 Não serão aceitas soluções que classificam usuários apenas a partir do IP de origem.
11.1.62 Permitir configurar rate limit por aplicação.
11.1.63 Implementar limitação de tráfego (rate limit) por usuário.
11.1.64 Permitir a criação de regras de bloqueio com base na classificação do IP de origem e sua reputação.
11.1.65 Deve possuir, pelo menos, a classificação de IP para botnets, scanners, proxies anônimos, proxies ToR e origens conhecidas de ataques web.
11.1.66 Permitir a definição de taxa máxima de requisições (rate limit).
11.1.67 Permitir definir uma lista de clientes confiáveis que não serão bloqueados por regras da política de segurança.
11.1.68 Permitir definir uma lista de clientes suspeitos que devem ser bloqueados.
11.1.69 Implementar a inspeção com base no IP do cliente que iniciou a conexão e permitir utilizar o IP do cliente, o cabeçalho X-Forwarded-For por exemplo, presente no cabeçalho HTTP.
11.1.70 Permitir inserir cabeçalho HTTP na requisição e na resposta.
11.1.71 Permitir remover cabeçalhos HTTP da requisição.
11.1.72 Implementar o redirecionamento automático de HTTP para HTTPS.
11.1.73 Permitir a configuração de políticas de CORS (Cross-Origin Resource Sharing).
11.1.74 Implementar mitigação automática de DDoS em camada 7.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

11.1.75 Implementar mitigação automática de ataques “Slow and low”.
11.1.76 Implementar descoberta de APIs para pelo menos 01 (uma) aplicação.
11.1.77 Implementar, a partir da descoberta, a construção automática do esquema (Swagger) da API.
11.1.78 Implementar através da análise do tráfego.
11.1.79 Implementar através de crawlers de aplicações web.
11.1.80 Implementar através da análise de código-fonte em repositórios GitHub, GitLab ou BitBucket.
11.1.81 Permitir agrupar as APIs descobertas para definição de políticas de segurança.
11.1.82 Implementar mecanismos para identificar “Shadow API”, ou seja, API que foram expostas pela aplicação, mas não foram aprovadas, documentadas ou homologadas.
11.1.83 Permitir configurar a descoberta de API por aplicação.
11.1.84 Permitir comparar o esquema definido da API com o que foi descoberto.
11.1.85 Implementar detecção do tipo de autenticação utilizada na API e o local de utilização nas chamadas da API.
11.1.86 Implementar análise de vulnerabilidades da API, como dados sensíveis expostos, falta de autenticação, autenticação fraca, e fornecer nota de risco automática calculada a partir das vulnerabilidades descobertas, impacto de ataque, impacto sobre o negócio, possibilidade de ataque e mitigação.
11.1.87 Implementar a descoberta e análise de cabeçalhos, conteúdo e assinaturas dentro dos campos de JSON Web Token (JWT), incluindo validação do algoritmo de assinatura, detecção de atributos do usuário e identificação de dados confidenciais.
11.1.88 Permitir definir expressões para classificar informações e identificar possíveis vazamento de dados.
11.1.89 Permitir definir paths de endpoints que serão excluídos do processo de descoberta.
11.1.90 Implementar proteção de APIs para até 500 (quinhentos) mil transações por mês.
11.1.91 Implementar a validação de APIs através de arquivos swagger compatível com OpenAPI.
11.1.92 Permitir importar diferentes versões de especificações de uma API.
11.1.93 Implementar a validação da API com base no arquivo swagger, permitindo que as ações de bloqueio, permissão e alerta sejam criadas para tráfego fora de conformidade.
11.1.94 Deve validar dados de entrada e saída, considerando o tipo de dados, comprimento mínimo e máximo, caracteres permitidos, intervalos de valores válidos.
11.1.95 Permitir a configuração de validação por endpoint da API, por grupos de API e com base no caminho.
11.1.96 Permitir configurar determinados IPs que não serão submetidos a validação.
11.1.97 Implementar a validação de autenticação presente nas requisições de API, de acordo com o esquema de autenticação configurado de forma que somente clientes autenticados possam acessar a API.
11.1.98 Permitir a configuração de proteções de APIs contra ameaças e vulnerabilidades listadas no OWASP API Security Top 10 e evoluções dessa lista.
11.1.99 Implementar a identificação por URL e método utilizado.
11.1.100 Implementar a identificação e classificação de usuários. Entende-se por usuário como sendo um cliente identificado e classificado a partir de informações de endereço IP, de cabeçalhos, parâmetros e cookies do HTTP.
11.1.101 Não serão aceitas soluções que classificam usuários apenas a partir do IP de origem.
11.1.102 Implementar análise comportamental para detectar atividades anormais ou suspeitas a partir da análise do usuário, requisição e resposta.
11.1.103 Implementar a detecção e mitigação de usuários maliciosos, correlacionando eventos do WAF, requisições e respostas, rate limits e outros eventos.
11.1.104 Implementar análise da requisição e da resposta em busca de indícios de tráfego malicioso, abusos e vazamento de informações.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

11.1.105 Implementar regrar de controle de API por endpoint, método e cliente.
11.1.106 Implementar políticas de controle de acesso da API a partir da descoberta.
11.1.107 Implementar proteção de ataques DDoS direcionados a API detectados a partir da análise comportamental.
11.1.108 Avaliação automática de vulnerabilidades
11.1.109 Implementar serviço de varredura automáticas de vulnerabilidades de, pelo menos, 02 (duas) aplicações web.
11.1.110 Implementar testes de penetração de aplicações totalmente automáticos, ou seja, sem a necessidade de escrita de scripts, roteiros ou playbooks.
11.1.111 Implementar identificação, navegação, varredura e testes completos, independentemente da tecnologia da aplicação.
11.1.112 Implementar relatórios com a vulnerabilidades encontradas, incluindo capturas de tela, vídeos e detalhes técnicos, permitindo uma compreensão completa.
11.1.113 Fornecer relatórios online e em PDF.
11.1.114 Informar com detalhes as requisições realizadas que apontaram vulnerabilidades e a resposta da aplicação.
11.1.115 Permitir o download da resposta da aplicação.
11.1.116 Permitir a configuração de contas de usuários para testes, inclusive contas que utilizam MFA.
11.1.117 Permitir configuração de alertas a respeito das varreduras e problemas encontrados.
11.1.118 Implementar avaliação de exposição de acordo com OWASP Top 10.
11.1.119 Fornecer orientações de mitigação e correção dos problemas encontrados.
11.1.120 Permitir inserir notas e observações sobre os problemas encontrados.
11.1.121 Implementar serviço de varredura de domínios para identificação e análise de aplicações expostas para a Internet.
11.1.122 Deve identificar domínios.
11.1.123 Deve identificar portas e serviços hospedadas pelos domínios.
11.1.124 Deve identificar a aplicações hospedada pelos domínios.
11.1.125 Permitir a configuração de varreduras de aplicações de forma automática a partir da descoberta.
11.1.126 Permitir a configuração de agendas de execução de testes e varreduras periódicos.
11.1.127 Gerenciamento e Proteção de DNS
11.1.128 Implementar serviço DNS primário e secundário para, pelo menos, 200 (duzentas) zonas.
11.1.129 Implementar zona de pesquisa direta (Forward DNS Lookup Zone) e reverso (Reverse Lookup Zone).
11.1.130 Para as zonas hospedadas na solução, implementar a configuração automática de domínios e FQDN utilizados nas aplicações publicadas pela solução.
11.1.131 Possuir interface gráfica para gerenciamento de registros do DNS.
11.1.132 Permitir configuração de registros individuais via API.
11.1.133 Permitir a importação de arquivos de configuração do BIND.
11.1.134 Implementar DNSSEC (Domain Name System Security Extensions) com gerenciamento automático de chaves.
11.1.135 Implementar proteções de ataques direcionados aos serviços de DNS.
11.1.136 Implementar proteções de ataques de DDoS.
11.1.137 Implementar a configuração de registros de DNS para funcionalidade de balanceamento de sites (Global Server Load Balancer – GSLB).
11.1.138 Suportar, pelo menos, 45 (quarenta e cinco) destinos de GSLB.
11.1.139 Implementar a verificação de disponibilidade dos sites através de testes HTTP e ICMP.
11.1.140 Implementar, pelo menos, os algoritmos de balanceamento round robin, prioridade, peso e origem.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

11.1.141 Permitir configurar topologias para respostas com base em geolocalização.
11.1.142 Permitir configurar prefixos IP para decisão de respostas.
11.1.143 Permitir configurar ASN (Autonomous System Number) para decisão de respostas.
11.2 ADMINISTRAÇÃO, GERÊNCIA E MONITORAMENTO
11.2.1 Os serviços devem ser prestados através de infraestrutura em nuvem do próprio fabricante da solução de forma não intrusiva, ou seja, sem a necessidade de instalação de equipamentos ou softwares nas dependências da CONTRATANTE.
11.2.2 O serviço em nuvem deverá ser oferecido em ponto(s) de presença em território nacional.
11.2.3 As atividades de administração, gerenciamento, operação e monitoramento dos serviços deverão ser através de console web única, gráfica e central do fabricante da solução, via HTTPS com algoritmos de criptografia modernos e seguros, compatível com navegadores padrões, não sendo aceitas soluções que dependam de plugins, add-ons ou aplicação exclusiva instaladas nas estações de trabalho.
11.2.4 A console deve possuir controles de segurança, incluindo, mas não se limitando a restrição de acesso administrativo por meio de um login seguro com autenticação de dois fatores de modo a prevenir que os serviços não sejam utilizados por terceiros não autorizados.
11.2.5 Permitir a criação de divisões administrativas de recursos através da criação de segmentos, partições, namespaces ou estrutura semelhante para agrupamento de recursos de diferentes propósitos, áreas ou finalidades da CONTRATANTE, tais como “Produção”, “Homologação” e “Desenvolvimento”, unidade de negócio, departamento, entre outros.
11.2.6 Permitir a criação de usuários com acesso a console.
11.2.7 Permitir a utilização de provedores de identidade para autenticação e autorização de usuários sem a necessidade de importar ou sincronizar com bases externas de usuários e senhas.
11.2.8 Implementar Single Sign-On (SSO) compatível com OpenID Connect (OIDC), tais como Okta, Microsoft, Google e outros.
11.2.9 Permitir a configuração de Segundo Fator de Autenticação.
11.2.10 Permitir a criação de credenciais para acesso via API com data de expiração ou prazo de validade.
11.2.11 Permitir definir políticas de senhas, incluindo tipos de caracteres, tamanho mínimo, validade e tentativas malsucedidas.
11.2.12 Permitir a criação de grupos de usuários e associar usuários aos grupos.
11.2.13 Deve permitir a criação de perfis de acesso com diferentes níveis de acesso aos recursos da solução.
11.2.14 Dispor de diferentes perfis predefinidos com diferentes níveis de acesso para diferentes recursos da solução, incluindo acesso restrito, somente leitura, e leitura e escrita.
11.2.15 Permitir associar perfis de acesso a usuários por divisão administrativa.
11.2.16 Permitir associar perfis de acesso a grupos de usuários por divisão administrativa.
11.2.17 Implementar API REST autenticada através de tokens ou certificados para configuração de recursos, com documentação pública mantida pelo fornecedor do serviço.
11.2.18 Deve ser compatível com mTLS.
11.2.19 Dispor de um cliente de linha de comando (CLI) que implemente a API REST compatível com, pelo menos, Linux e Mac OS.
11.2.20 Possuir implementações específicas para ferramentas de automação no formato de provedores e módulos para Terraform ou coleções para Ansible.
11.2.21 Permitir a exportação de eventos para sistemas externos, incluindo logs da solução e de requisições, segurança, e auditoria das aplicações.
11.2.22 Permitir a exportação para, pelo menos, os seguintes sistemas: Kafka, Splunk, Datadog, Azure, Amazon, QRadar e servidores HTTPS genéricos.
11.2.23 Permitir a configuração de, pelo menos, 02 (dois) destinos para envio de eventos.
11.2.24 Possuir painéis online para visualização de eventos e estatísticas, incluindo, no mínimo:

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

11.2.24.1 Saúde geral da aplicação;
11.2.24.2 Latência fim a fim;
11.2.24.3 Estatísticas de TLS;
11.2.24.4. Status dos certificados e avisos que estão próximos do vencimento;
11.2.24.5. Eventos com origem, destino, ataque e ação;
11.2.24.6. Taxas de requisições, status code e métodos;
11.2.24.7. Latência e throughput da aplicação;
11.2.24.8. Total de requisições ao longo do tempo;
11.2.24.9. Lista de aplicações e requisições, ataques e bloqueios;
11.2.24.10. Tipos de eventos;
11.2.24.11. Ataques, origens e alvos mais comuns;
11.2.24.12. Assinaturas e violações mais comuns;
11.2.24.13. Sumário de segurança;
11.2.24.14. Eventos de DDoS ao longo do tempo;
11.2.24.15. Taxa de requisições de ataques de DDoS;
11.2.24.16. Throughtput do DDoS;
11.2.24.17. Mapa geográfico indicando a origem do DDoS;
11.2.24.18. Origens, regiões e ASN (Autonomous System Number) mais comuns relacionadas ao ataque de DDoS;
11.2.24.19. Mapa geográfico das requisições de DNS por zona;
11.2.24.20. Gráfico de volume de requisições ao longo do tempo de DNS;
11.2.24.21. Lista de nomes de DNS mais solicitados;
11.2.24.22. Lista de tipos de requisições de DNS mais solicitadas e gráfico ao longo do tempo;
11.2.24.23. Gráfico de volume por tipo de resposta de DNS ao longo do tempo.
11.2.25 Possuir relatório de incidentes de segurança para investigação de ataques com agrupamento automático de eventos em incidentes.
11.2.26 Permitir a configuração de agendamento de relatórios (diários, semanais ou mensais) e enviar os resultados por e-mail para usuários específico.
11.2.27 Garantir via console o acesso, busca e consulta de eventos por, no mínimo:
11.2.27.1. 30 (trinta) dias para métricas de desempenho e eventos de auditoria;
11.2.27.2. 07 (sete) dias para eventos de requisições e segurança.

12. ITEM 11 - SOLUÇÃO DE SEGURANÇA DE E-MAIL

12.1 CARACTERISTICAS GERAIS

12.1.1 A solução deve possuir mecanismos de proteção multi-camadas contra as ameaças em serviços de e-mail:
12.1.1.1 Prevenção de ameaças avançadas (APT) ou dia zero (zero day);
12.1.1.2 Proteção contra phishing;
12.1.1.3 Possibilidade de identificar e-mails de SPAM;
12.1.1.4 Gerar visibilidade de aplicações SaaS não autorizadas (Shadow IT);
12.1.1.5 Integração nativa com, pelo menos, Microsoft 365 e Google Workspace;
12.1.1.6 Arquitetura unificada para visibilidade de logs e gerenciamento de políticas;
12.1.1.7 Limpeza e extração contra conteúdo malicioso em anexos (CDR);
12.1.2 Fazer integração via API da ferramenta de segurança para aplicações SaaS;
12.1.3 Durante integração deve fazer busca na base de dados de usuários sem a necessidade de agentes para ter visibilidade dos usuários e grupos;
12.1.4 Durante a integração inicial com o Microsoft 365, deve ser possível determinar qual grupo ou usuários farão parte das políticas de segurança para inspeção dos e-mails;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

12.1.5 A solução de prevenção de ameaças avançadas, deve possuir funcionalidades de sandboxing, antivírus, reputação de URL e anti-phishing;
12.1.6 Nas configurações de políticas de segurança, deve possuir as opções de detectar e prevenir;
12.1.7 Deve identificar os grupos ou usuários que serão inspecionados e ter uma lista de exclusão baseado na conta do Microsoft 365;
12.1.8 Criação de alertas para administradores da ferramenta para qualquer malware identificado, assim como phishing. Tornando também opcional o alerta do usuário de destino sobre possíveis malwares;
12.1.9 A solução de sandboxing, deve ser na nuvem do próprio fabricante, sendo ela proprietária;
12.1.10 Na solução de prevenção de ameaças avançadas, deve apresentar nos logs as seguintes informações:
12.1.10.1 Todas as funcionalidades de segurança que identificaram a ameaça;
12.1.10.2 Nome do arquivo identificado;
12.1.11 Deve informar o MD5 para fazer pesquisas e comparar com outras fontes de terceiros;
12.1.12 Identificar o usuário que recebeu o e-mail malicioso;
12.1.13 Cada log de sandboxing, quando identificada uma ameaça, deve apresentar informações detalhadas do arquivo malicioso para análise:
12.1.13.1 Tamanho do arquivo;
12.1.13.2 Tipo do arquivo;
12.1.13.3 Lista de hash que o arquivo possui;
12.1.13.4 Veredito do ataque;
12.1.13.5 Risco de segurança;
12.1.13.6 Nível de confiança;
12.1.13.7 Classificação do ataque, ou seja, se é uma família já conhecida. Ex.: Trojan;
12.1.14 Apresentar no próprio relatório o malware identificado, evidências do ataque já no Framework do MITRE ATT&CK, classificando as devidas táticas e técnicas do ataque;
12.1.15 Lista dos arquivos encontrados dentro o malware identificado. Ex.: Pode ser um arquivo ZIP com outros arquivos ou executáveis que possuem outros arquivos associados a ele;
12.1.16 Atividades suspeitas no computador do sandboxing que vai simular a ação humana como: eventos no file system, chave de registro, eventos de rede apresentando possíveis URLs ou IPs;
12.1.17 Vídeo da máquina virtual dentro da solução de sandboxing, apresentando o comportamento humano;
12.1.18 A solução deve possuir mecanismo onde no momento que encontrado um conteúdo malicioso no arquivo office ou PDF, a mesma deve reconstruir o arquivo removendo o conteúdo malicioso, sendo capaz de converter arquivos reconstruídos para o formato PDF para melhor segurança, ou manter-se em formato original de acordo com política estabelecida;
12.1.19 Deve possuir console de gerenciamento web na nuvem, sem a necessidade de infraestrutura específica e já incluída nos custos de licenciamento da solução;
12.1.20 Deve inspecionar todos os arquivos previamente existentes com no mínimo de 7 dias retroativos à data inicial da integração dos serviços de e- mail, verificando a presença de malwares;
12.1.21 Toda integração deve ser feita através de API, sem a necessidade de integração com nenhuma solução de proxy local ou agentes.
12.1.22 Deve possuir integração nativa com a nuvem de inteligência de ameaças (Threat Intelligence) do fabricante para prevenção de ameaças e checagem de reputação.
12.1.23 Identificar nos e-mails phishing e apresentar os seguintes parâmetros nos eventos:
12.1.23.1 Remetente;
12.1.23.2 Destinatário;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

12.1.23.3 Destinatários copiados;
12.1.23.4 Título do e-mail;
12.1.23.5 Tipo de conteúdo, exemplo HTML;
12.1.23.6 Data e horário do recebimento do e-mail;
12.1.23.7 Alias do usuário;
12.1.24 Quando identificado um phishing, deve apresentar informações como:
12.1.24.1 Indicadores da detecção como phishing:
12.1.24.2 Análise do ataque;
12.1.24.3 Reputação de quem enviou;
12.1.24.4 Nível de confiança para determinar se é alto ou não;
12.1.24.5 Informações que são identificadas no cabeçalho do e-mail como falta do DMARC e assinatura DKIM
12.1.25 Caso tenha alguma URL no corpo do e-mail que foi caracterizada como phishing, a mesma deve ser apresentada nos logs;
12.1.26 A solução deverá realizar análise dos links enviados no corpo do e- mail. Essa análise deverá apresentar o motivo da caracterização como suspeito ou malicioso.
12.1.27 A solução deve apresentar uma visualização prévia da URL suspeita;
12.1.28 O administrador deve ter a opção de solicitar na ferramenta a reclassificação referente a um evento de prevenção de ameaças que não corresponde ao log apresentado.
12.1.29 Deverá prover mecanismo de proteção para links, onde a solução deverá validar a URL antes de redirecionar para o usuário.
12.1.30 Pesquisar no log do evento de phishing, outros e-mails baseados no ataque recebido que possuam os mesmos critérios como quem enviou, título de e-mail e outros tópicos;
12.1.31 A solução deverá apresentar quais os indicadores que a Inteligência Artificial identificou e caracterizou o evento.
12.1.32 Relatório sumarizado contendo todas as funcionalidades de segurança;
12.1.33 Listar a quantidade de objetos escaneados e a quantidade de ameaças identificadas;
12.1.34 Possuir mecanismo de quarentena onde o administrador consegue visualizar todos os e-mails que foram identificados como maliciosos;
12.1.35 Permitir a restauração do e-mail em quarentena através da ferramenta;
12.1.36 Deverá permitir que o usuário solicite a liberação de um e-mail em quarentena.
12.1.37 Visibilidade dos eventos através de usuários que estão integrados na ferramenta de forma automática;
12.1.38 Deve ser possível selecionar o usuário e identificar todos os eventos de segurança baseado por período e funcionalidade de segurança;
12.1.39 Visibilidade correlacionada de todos os eventos de segurança.
12.1.40 Deve identificar tentativas de acesso anômalas aos serviços, tal como o acesso simultâneo com uma mesma credencial a partir de localizações geograficamente distantes.

12.2 GERENCIAMENTO E VISIBILIDADE
12.2.1 Deve possuir uma dashboard que permita ao administrador de segurança ter visibilidade consolidada das ameaças identificadas nos diferentes serviços SaaS, incluindo eventos de malware, URLs maliciosas, phishing, Shadow IT;
12.2.2 Deve prover uma interface para visualização detalhada dos eventos maliciosos identificados/
12.2.3 A solução deverá ser capaz de oferecer integração com ferramentas de SIEM tanto on-premise quanto em nuvem, oferecendo no mínimo Splunk, AWS e Azure Log.
12.2.4 A gerência centralizada deve permitir visibilidade sumarizada de todas as atividades maliciosas identificadas pela solução de diferentes funcionalidades suportadas pela ferramenta como: Malwares, Phishing, Shadow IT e anomalias. Sendo possível fazer drill-down e navegar

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

nos logs para análise das atividades suspeitas;
12.2.5 Deve possuir gráficos e filtros que permitam ao administrador identificar rapidamente as ameaças identificadas;
12.2.6 A gerência centralizada deve permitir visualizar a quantidade de usuários que estão ativos na solução nas funcionalidades de e-mail assim como a quantidade de e-mails inspecionados;
12.2.7 Deve permitir a configuração de políticas independentes para cada serviço de e-mail;
12.2.8 Deve permitir múltiplas regras de segurança para cada serviço de e-mail, aplicando proteções diferenciadas baseados em usuários ou grupos de usuários
12.2.9 Quando identificado um evento na solução prevenção de ameaças, o administrador deve ter as seguintes opções de ação baseado em cada log:
12.2.9.1 Alertar o usuário sobre a ameaça;
12.2.9.2 Liberar o arquivo inspecionado e bloqueado;
12.2.9.3 Reportar para o fabricante que não é um arquivo malicioso;
12.2.9.4 Desconsiderar evento;
12.2.9.5 Analisar o relatório do incidente.
12.2.10 As regras devem permitir a geração de alertas por e-mail para os administradores para os casos de malware e phishing, bem como a customização das mensagens de alerta;
12.2.11 Quando identificado um evento de phishing, o administrador deve ter as seguintes opções de ação:
12.2.11.1 Categorizar como SPAM;
12.2.11.2 Alertar usuários que é um phishing;
12.2.11.3 Quarantenar e-mail;
12.2.11.4 Criar exceção.
12.2.12 Quando identificado um evento de anomalia, o administrador deve ter as seguintes opções de ação:
12.2.12.1 Desconsiderar evento;
12.2.12.2 Adicionar exceção a partir do evento.
12.2.13 Quando identificado um evento na solução de ShadowIT, o administrador deve ter as seguintes opções:
12.2.13.1 Aprovar aplicação;
12.2.13.2 Desconsiderar evento.
12.2.14 A solução deve possuir painel de quarentena baseado no Microsoft 365 E-mail, permitindo o administrador ter acesso aos itens que foram colocados em quarentena;
12.2.15 A quarentena deve permitir que o administrador possa tomar ação para as requisições de restauração do e-mail Microsoft 365.

13. ITEM 12 - SOLUÇÃO DE SEGURANÇA DOS DISPOSITIVOS DE ACESSO A REDE

13.1 CARACTERÍSTICAS DA CONSOLE DE GERENCIAMENTO

13.1.1 A console de gerenciamento centralizado deverá ser na nuvem do fabricante;
13.1.2 O gerenciamento centralizado deverá suportar gerenciar todos os endpoints solicitados neste termo;
13.1.3 A console de gerenciamento deverá ser acessível através de navegador de internet de mercado, compatível com, pelo menos, Google Chrome;
13.1.4 A solução deverá permitir o acesso e consulta de dados do gerenciamento a partir de API;
13.1.5 A console de gerenciamento deve permitir atribuir permissões diferentes a cada usuário administrativo;
13.1.6 Deve possuir um guia de primeiros passos durante a implementação da solução;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

13.1.7 Deve ser capaz de oferecer controle granular na aplicação de políticas, permitindo que regras sejam configuradas com diferentes níveis de prioridade, tanto para usuários quanto para dispositivos.
13.1.8 A solução deve ser capaz de importar e exportar políticas, total ou parcialmente, pelo menos no formato JSON ou similar, permitindo backup e migração para um novo servidor de gerenciamento.
13.1.9 A solução deve ser capaz de permitir a adição manual dos seguintes tipos de Indicadores de Comprometimento (IoC):
13.1.9.1 URL;
13.1.9.2 Domínio;
13.1.9.3 Endereço IP;
13.1.9.4 MD5 Hash;
13.1.10 A solução deve ser capaz de enviar relatórios de segurança semanais e mensais por e-mail a todos os administradores.
13.1.11 A solução deve ser capaz de enviar operações remotas para as máquinas em que os endpoints estejam instalados;
13.1.12 A console de gerenciamento deve ser capaz de oferecer suporte à Autenticação de Dois Fatores (2FA);
13.1.13 A solução deve ser capaz de permitir a configuração da integração com um Provedor de Identidade (IdP) para controle de autenticação, sendo compatível com, pelo menos:
13.1.13.1 RADIUS;
13.1.13.2 Okta;
13.1.13.3 Microsoft ADFS;
13.1.13.4 Microsoft Entra ID;
13.1.13.5 Servidor SAML genérico;
13.1.14 A solução deve ser capaz de encaminhar logs e eventos para SIEMs, incluindo, mas não se limitando a:
13.1.14.1 Splunk
13.1.14.2 QRadar
13.1.14.3 ArcSight

13.1.15 A solução deve ser capaz de gerenciar grupos virtuais, ou seja, criados no próprio gerenciamento da solução, de usuários e dispositivos para facilitar a administração e segmentação de políticas de segurança.
13.1.16 A solução deve ser capaz de permitir que um usuário ou dispositivo pertença a mais de um grupo virtual simultaneamente.
13.1.17 A solução deve ser capaz de permitir que administradores adicionem usuários, dispositivos ou grupos a um grupo virtual existente, utilizando as opções de gerenciamento;
13.1.18 A solução deve ser capaz de permitir a seleção do período de análise ao gerar relatórios, com as seguintes opções:
13.1.18.1 Último dia
13.1.18.2 Últimos 7 dias
13.1.18.3 Últimos 30 dias
13.1.19 A solução deve ser capaz de permitir o agendamento automático de relatórios, possibilitando a sua geração em datas e horários específicos e o envio por e-mail para destinatários definidos.
13.1.20 A solução deve ser capaz de permitir a edição e exclusão de relatórios agendados,

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

garantindo flexibilidade na gestão da periodicidade e dos destinatários.

13.1.21 Deve possuir, pelo menos, os seguintes modelos de relatórios pré- definidos pelo fabricante:

13.1.21.1 Relatório de ameaças; 13.1.21.2.Relatório de políticas; 13.1.21.3.Relatório de implantação;

13.1.22 A console deve permitir a criação de dashboards customizáveis;

13.1.23 Deve possuir um dashboard de visão operacional da solução, contendo, pelo menos, as seguintes informações:

13.1.23.1 Sistemas operacionais dos endpoints;

13.1.23.2 Alertas recentes;

13.1.23.3. Status de atualização de anti-malware;

13.1.23.4. Status de implementação;

13.1.23.5. Quantidade de endpoints ativos;

13.1.24 A solução deve ser capaz de exibir informações detalhadas de hardware dos dispositivos, incluindo:

13.1.24.1 Configuração da CPU

13.1.24.2 Conexão de rede

13.1.24.3 Uso do disco

13.1.24.4 Memória RAM

13.1.25 A solução deve ser capaz de executar diagnósticos nos endpoints, coletando informações sobre uso total de CPU e RAM nas últimas horas;

13.1.26 A solução deve ser capaz de permitir a análise do uso da CPU para identificar processos que ultrapassam um limite especificado, possibilitando a exclusão desses processos de futuros scans, caso necessário.

13.2 PROTEÇÃO ANTI-MALWARE E ANTI-RANSOMWARE

13.2.1 A solução deve possuir motor de proteção contra malware com base em assinaturas locais e em nuvem, capazes de detectar ameaças conhecidas.

13.2.2 A solução deve possuir motor de proteção comportamental capaz de detectar e bloquear ameaças novas ou desconhecidas com base em anomalias no comportamento do sistema e de processos.

13.2.3 A solução deve ser capaz de detectar e mitigar ataques de ransomware em tempo real, com mecanismos de bloqueio de criptografia maliciosa.

13.2.4 A solução deve ser capaz de realizar cópia de segurança (backup) automático dos arquivos monitorados quando um comportamento de ransomware é detectado.

13.2.5 A solução deve permitir configurar exceções específicas para arquivos, processos, pastas e extensões, tanto para o motor de assinaturas quanto para a proteção comportamental.

13.2.6 A solução deve ser capaz de identificar e bloquear execução de arquivos com extensões suspeitas ou comportamento malicioso, mesmo que esses arquivos sejam desconhecidos pelas bases de assinaturas.

13.2.7 A solução deve ser capaz de realizar varreduras (scans) sob demanda, agendadas ou automáticas após detecção de incidentes.

13.2.8 A solução deve ser capaz de realizar varreduras em tempo real sobre arquivos abertos, modificados ou copiados no sistema.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

13.2.9 A solução deve possuir proteção residente que não possa ser desativada pelo usuário final sem autorização administrativa.
13.2.10 A solução deve permitir configurar diferentes níveis de resposta a uma detecção de ameaça, como quarentena, exclusão automática, notificação ao usuário e envio de alerta ao administrador.
13.2.11 A solução deve permitir a restauração de arquivos que foram movidos para a quarentena.
13.2.12 A solução deve ser capaz de enviar notificações em tempo real ao console de gerenciamento sempre que houver uma detecção de malware ou ransomware.
13.2.13 A solução deve ser capaz de identificar e bloquear malwares baseados em scripts, como PowerShell, JavaScript e VBS.
13.2.14 A solução deve ser compatível com sistemas operacionais Windows e macOS, com recursos de proteção equivalentes em ambos, salvo limitações documentadas.
13.2.15 A solução deve permitir configurar políticas distintas de proteção de malware para diferentes grupos de dispositivos ou usuários.
13.2.16 A solução deve permitir visualização de logs e eventos de detecção com detalhamento do tipo de ameaça, ação tomada, hash do arquivo e processo responsável.
13.2.17 A solução deve permitir ativar o modo silencioso (silent mode) em que as notificações para o usuário final são ocultadas, sem comprometer a proteção.
13.2.18 A solução deve suportar o uso em servidores, com modos de proteção otimizados para cargas de trabalho críticas.
13.2.19 A solução deve ser capaz de operar com consumo reduzido de recursos do sistema, podendo ser ajustada para cenários com limitações de CPU e memória.

13.3 CONTROLE DE APLICAÇÕES
13.3.1 A solução deve ser capaz de identificar, classificar e controlar a execução de aplicações em estações de trabalho e servidores.
13.3.2 A solução deve permitir bloquear, permitir ou colocar em modo de observação (monitoramento) a execução de aplicações específicas.
13.3.3 A solução deve permitir aplicar políticas de controle de aplicações distintas por grupos de usuários ou dispositivos.
13.3.4 A solução deve ser capaz de realizar varredura automática do endpoint para detectar as aplicações instaladas.
13.3.5 A solução deve permitir que o administrador importe a lista de aplicações identificadas em um endpoint de referência para criação de regras de controle.
13.3.6 A solução deve ser capaz de aplicar regras por nome da aplicação, editor, assinatura digital, hash ou caminho do executável.
13.3.7 A solução deve ser capaz de diferenciar e controlar aplicações portáteis (executáveis que rodam sem instalação formal).
13.3.8 A solução deve permitir a criação de regras de controle de aplicações personalizadas pelo administrador, além das categorias fornecidas pelo fabricante.
13.3.9 A solução deve ser capaz de controlar e monitorar scripts e ferramentas utilizadas por desenvolvedores, como PowerShell, Python, cmd, bash, entre outros.
13.3.10 A solução deve gerar logs de execução ou tentativa de execução de aplicações bloqueadas, com informações detalhadas como nome, origem e horário.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

13.3.11 A solução deve permitir configuração de ações diferentes para tentativa de execução de aplicações bloqueadas, como: exibir alerta ao usuário, registrar log, ou bloquear silenciosamente.
13.3.12 A solução deve permitir configurar exceções a regras de bloqueio de aplicações com base em grupos de usuários ou dispositivos.
13.3.13 A solução deve ser compatível com sistemas operacionais Windows e macOS.
13.3.14 A solução deve possuir base de dados de aplicações pré-classificadas por categoria (ex: navegadores, jogos, ferramentas de proxy, ferramentas de desenvolvimento etc.).
13.3.15 A solução deve permitir integração com ferramentas de inventário e gestão de ativos, possibilitando o cruzamento de dados entre o inventário de software e as políticas de controle de aplicação.

13.4 PROTEÇÃO WEB E NAVEGADORES
13.4.1 É permitida a composição de produtos para atendimento ao item, desde que não sejam open source ou software livre;
13.4.2 A solução deve ser capaz de inspecionar o tráfego web em tempo real e bloquear URLs maliciosas com base em inteligência de ameaças atualizada.
13.4.3 A solução deve permitir a aplicação de políticas de filtragem de URL por categoria (ex: redes sociais, pornografia, jogos, proxy, etc.).
13.4.4 A solução deve permitir a criação de listas personalizadas de URLs permitidas e bloqueadas (allow-list e block-list).
13.4.5 A solução deve ser capaz de proteger contra phishing em tempo real, mesmo que o link seja recém-criado e ainda não esteja categorizado.
13.4.6 A solução deve ser capaz de detectar e bloquear o download de arquivos maliciosos via navegador.
13.4.7 A solução deve permitir a emulação e extração de arquivos baixados, com inspeção de conteúdo em sandbox para prevenir exploits.
13.4.8 A solução deve permitir a aplicação de políticas de proteção distintas por grupos de usuários ou dispositivos.
13.4.9 A solução deve ser compatível com navegadores modernos, incluindo Google Chrome, Mozilla Firefox, Microsoft Edge e Safari.
13.4.10 A solução deve ser capaz de operar em modo protegido contra evasões, impedindo que usuários contornem as proteções via proxies ou modos anônimos.
13.4.11 A solução deve permitir o controle sobre o uso do modo incógnito ou InPrivate nos navegadores.
13.4.12 A solução deve permitir a personalização de mensagens de bloqueio exibidas ao usuário no navegador.
13.4.13 A solução deve permitir a exibição de alertas educativos antes de permitir ou bloquear o acesso a determinados conteúdos.
13.4.14 A solução deve gerar logs de acesso à web, incluindo URLs visitadas, categoria, usuário e ação tomada.
13.4.15 A solução deve ser capaz de operar mesmo sem conexão constante com a nuvem, utilizando assinaturas locais quando necessário.

13.5 FIREWALL LOCAL
13.5.1 A solução deve incluir um firewall local integrado ao agente de endpoint, com capacidade

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

de controlar o tráfego de rede em tempo real.
13.5.2 A solução deve permitir criar regras de entrada e saída por porta, protocolo, IP, nome de aplicação e horário.
13.5.3 A solução deve permitir aplicar políticas de firewall distintas por grupo de dispositivos ou usuários.
13.5.4 A solução deve suportar a definição de zonas de segurança (ex: rede corporativa, rede pública, rede doméstica).
13.5.5 A solução deve permitir o bloqueio de conexões não autorizadas mesmo antes do carregamento completo do sistema operacional (pré-boot).
13.5.6 A solução deve permitir a configuração de perfis com regras distintas para diferentes tipos de rede ou contexto de conectividade.
13.5.7 A solução deve permitir a criação de grupos de objetos (IPs, portas, protocolos) reutilizáveis nas regras de firewall.
13.5.8 A solução deve ser capaz de registrar tentativas de conexão negadas e conexões permitidas para fins de auditoria.
13.5.9 A solução deve permitir ações diferentes por tipo de regra (permitir, negar, perguntar, registrar somente).
13.5.10 A solução deve permitir integração com políticas de conformidade e detecção de postura de segurança.
13.5.11 A solução deve ser compatível com sistemas operacionais Windows e macOS.

13.6 CONTROLE DE PORTAS E DISPOSITIVOS
13.6.1 A solução deve ser capaz de controlar o acesso a portas USB, interfaces de rede, dispositivos de armazenamento externos e outros periféricos conectáveis.
13.6.2 A solução deve permitir aplicar políticas de permissão, bloqueio ou acesso somente leitura para diferentes tipos de dispositivos.
13.6.3 A solução deve permitir definir regras com base em tipo de dispositivo (ex: armazenamento, impressora, interface de rede, modem, etc.).
13.6.4 A solução deve ser capaz de aplicar políticas distintas por grupos de usuários ou dispositivos.
13.6.5 A solução deve permitir exceções com base em identificação de dispositivo por número de série, classe ou fabricante.
13.6.6 A solução deve registrar logs de conexão e desconexão de dispositivos externos, com dados como horário, usuário e tipo de dispositivo.
13.6.7 A solução deve suportar notificações ao usuário no momento da conexão de um dispositivo não autorizado.
13.7 A solução deve permitir a aplicação de políticas condicionais, como bloqueio em redes públicas e liberação em redes corporativas.
13.8 A solução deve permitir a aplicação de políticas em modo silencioso (somente auditoria) ou modo ativo (bloqueio).

13.9 INTEGRAÇÕES COM SIEM E ACTIVE DIRECTORY
13.9.1 A solução deve ser capaz de encaminhar logs e eventos para soluções de SIEM por meio de integração nativa ou conectores padrão.
13.9.2 A solução deve suportar integração com, no mínimo, as seguintes soluções de SIEM:

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

Splunk, IBM QRadar e Micro Focus ArcSight.

13.9.3 A solução deve permitir a personalização dos tipos de eventos exportados para o SIEM.

13.9.4 A solução deve suportar integração com o Active Directory para importação de usuários, grupos e unidades organizacionais.

13.9.5 A solução deve ser capaz de realizar sincronização total ou parcial com o Active Directory, de forma agendada ou sob demanda.

13.9.6 A solução deve suportar múltiplos domínios AD e ambientes com múltiplos controladores de domínio.

13.9.7 A solução deve permitir a associação de políticas com base em atributos do Active Directory.

13.9.8 A solução deve ser compatível com integração via Microsoft Entra ID (Azure AD) para ambientes híbridos ou em nuvem.

13.10 CARACTERÍSTICAS E PROTEÇÕES PARA LINUX

13.10.1 A solução deve fornecer agente de proteção compatível com sistemas operacionais baseados em Linux.

13.10.2 A solução deve oferecer, pelo menos, as seguintes funcionalidades para endpoints Linux: proteção anti-malware, proteção comportamental, EDR/Threat Hunting e geração de forense local.

13.10.3 A solução deve permitir varreduras agendadas e em tempo real, conforme configurações administrativas.

13.10.4 A solução deve suportar proteção contra ransomware em tempo real com funcionalidades de mitigação e restauração.

13.10.5 A solução deve ser gerenciada pela mesma console utilizada para os demais sistemas operacionais, mantendo unificação de políticas e visibilidade.

13.10.6 A solução deve operar com baixo consumo de recursos, adaptando-se a diferentes distribuições e cargas de trabalho.

13.10.7 A solução deve ser compatível, no mínimo, com as seguintes distribuições Linux:

13.10.7.1 Ubuntu 20.04 LTS ou superior

13.10.7.2 Red Hat Enterprise Linux 8.x e 9.x

13.10.7.3 CentOS 8

13.10.7.4 Debian 11 ou superior

13.10.7.5 Amazon Linux 2

13.10.7.6 SUSE Linux Enterprise Server (SLES)

13.10.7.7 Oracle Linux 8.x

13.10.7.8. Rocky Linux 8.x

13.11 OTIMIZAÇÕES DE COMUNICAÇÃO VIA NÓ DE DISTRIBUIÇÃO LOCAL

13.11.1 A solução deve ser capaz de operar com arquitetura de distribuição inteligente de atualizações e comunicação, por meio da designação de um ou mais nós de distribuição local.

13.11.2 A solução deve permitir designar dispositivos da rede como nós de distribuição local, que atuem como ponto de disseminação de políticas, atualizações de assinatura e arquivos para outros endpoints na mesma localidade.

13.11.3 A solução deve possibilitar a comunicação entre endpoints e a console de

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

gerenciamento mesmo em ambientes com acesso restrito à internet, utilizando o nó de distribuição local como intermediário.

13.11.4 A solução deve manter cópias locais das atualizações e políticas nesses nós, otimizando o uso de banda e garantindo a continuidade da proteção em locais com baixa conectividade.

13.11.5 A solução deve permitir definir critérios de seleção ou eleição para os dispositivos que atuarão como nós de distribuição.

13.11.6 A solução deve permitir o monitoramento dos nós de distribuição local definidos, incluindo disponibilidade, volume de dados transferidos e endpoints atendidos.

13.11.7 A solução deve ser capaz de operar em ambientes semi-isolados, como redes industriais, escritórios remotos com proxy ou zonas de DMZ.

13.12 OPERAÇÕES DE COMANDO REMOTO

13.12.1 A solução deve ser capaz de executar comandos e ações remotas diretamente nos endpoints a partir da console de gerenciamento.

13.12.2 A solução deve permitir a execução de comandos administrativos nos endpoints, como pelo menos:

13.12.2.1 Isolamento de rede;

13.12.2.2 Reinicialização do dispositivo;

13.12.2.3 Atualização de políticas;

13.12.2.4 Coleta de logs;

13.12.2.5 Reinício do agente;

13.12.3 A solução deve ser capaz de iniciar varreduras antivírus remotamente, com opção de escaneamento rápido ou completo.

13.12.4 A solução deve permitir atualizar manualmente as assinaturas de proteção de malware nos dispositivos.

13.12.5 A solução deve permitir o envio de comandos para restaurar arquivos em quarentena ou aplicar ações corretivas em arquivos detectados como maliciosos.

13.12.6 A solução deve permitir o envio de comandos personalizados para execução no sistema operacional, com controle de escopo e permissões por administrador.

13.12.7 A solução deve permitir a coleta de informações de diagnóstico detalhadas do endpoint, como uso de CPU, RAM, status de serviços, e eventos recentes.

13.12.8 A solução deve permitir a exclusão de arquivos, limpeza de rastros maliciosos e execução de scripts de remediação aprovados pelo administrador.

13.12.9 A solução deve permitir o envio de arquivos específicos para análise forense, bem como a solicitação de snapshots do sistema em tempo real.

13.12.10 A solução deve registrar logs completos de todas as ações remotas executadas, incluindo data, hora, administrador responsável, dispositivo de destino e status da execução.

13.12.11 A solução deve permitir a aplicação dessas operações individualmente ou em lote, com seleção múltipla de endpoints.

13.12.12 A solução deve permitir restrições de permissão para uso dessas ações, com base em perfis de administrador e níveis de responsabilidade.

13.13 GESTÃO DE POSTURA DE SEGURANÇA

13.13.1 É permitida a composição de produtos para atendimento ao item, desde que não sejam

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

open source ou software livre;
13.13.2 A solução deve possuir módulo de postura de segurança capaz de verificar a conformidade dos endpoints com políticas definidas pelo administrador.
13.13.3 A solução deve permitir a definição de regras de conformidade com base em critérios como: presença de antivírus, firewall ativo, versões de software, e configurações de segurança.
13.13.4 A solução deve ser capaz de classificar os dispositivos como conformes, não conformes ou parcialmente conformes com base nos critérios definidos.
13.13.5 A solução deve permitir a geração de relatórios de conformidade por grupo, dispositivo ou unidade organizacional.
13.13.6 A solução deve permitir a aplicação de ações corretivas automatizadas ou manuais nos dispositivos que não atendam aos critérios definidos.
13.13.7 A solução deve permitir a visualização de status de conformidade em tempo real, com dashboards de fácil leitura para auditorias e acompanhamento.
13.13.8 A solução deve ser capaz de integrar-se com Active Directory e outras fontes de identidade para aplicar regras com base em perfil de usuário ou grupo.
13.13.9 A solução deve suportar diferentes perfis de postura por tipo de dispositivo ou uso (ex: notebooks, servidores).
13.13.10 A solução deve manter o histórico de avaliações de conformidade realizadas para cada dispositivo.
13.13.11 A solução deve permitir exportação dos dados de postura em formatos abertos para uso em plataformas de auditoria ou GRC.

13.14 VISIBILIDADE ESTENDIDA
13.14.1 A solução deve demonstrar a quantidade de detecções ou prevenções por origem;
13.14.2 Deve ser capaz de demonstrar uma linha do tempo com a quantidade de incidentes e suas severidades;
13.14.3 Para cada incidente detectado, deverá demonstrar o nível de confiança da detecção em pelo menos os seguintes níveis:
13.14.3.1 Alto;
13.14.3.2 Médio;
13.14.3.3 Baixo;
13.14.4 Na indicação do incidente, deverá informar a origem dos eventos correlacionados;
13.14.5 Cada incidente gerado pela ferramenta deve possuir, pelo menos, as seguintes características:
13.14.5.1 ID único de identificação;
13.14.5.2 Data de criação e data da última atualização; 13.14.5.3.Nível de prioridade, severidade e confiança;
13.14.5.4. Capacidade de adicionar um comentário ao incidente para que sirva de orientação para outros analistas que verificarem o incidente posteriormente;
13.14.5.5. Apresentar todos os ativos e indicadores afetados envolvidos no incidente;
13.14.6 Os indicadores do incidente devem ser automaticamente adicionados ao gerenciamento de IOCs, garantindo que outros elementos do ambiente não tenham comunicação com esse indicador;
13.14.7 Deverá apresentar um breve descritivo sobre o incidente para servir como orientação para o analista responsável;
13.14.8 A solução deve informar as táticas e técnicas envolvidas no incidente conforme o MITRE ATT&CK;
13.14.9 Deve ser possível criar exclusões a partir de um incidente para casos de, por exemplo,

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

falso positivo e atividade reconhecida;
13.14.10 Deve ser possível aplicar a exclusão criada de forma retroativa à partir de uma data pré-definida;
13.14.11 A ferramenta deve possibilitar a criação de exclusões para que não seja gerado um incidente para um Host, IP ou e-mail específico;
13.14.12 A solução deverá utilizar inteligência artificial (IA) e o aprendizado de máquina (ML) para analisar eventos de segurança e identificar riscos de segurança no ambiente;
13.14.13 Após correlacionar os logs dos produtos, se um risco de segurança for detectado, a solução deverá gerar um incidente (alerta) com uma prioridade apropriada com base na gravidade e no nível de confiança da detecção, e fornecer mitigação ao incidente;
13.14.14 Os incidentes devem ser mapeados de acordo com o framework do MITRE ATT&CK;
13.14.15 Deverá permitir que o incidente seja assinalado para a análise de um analista;
13.14.16 Permitir que os administradores sejam notificados quando um novo incidente for gerado;
13.14.17 A console de administração deve permitir filtrar por um período de até 30 dias, painéis com, no mínimo, as seguintes informações:
13.14.17.1 Número total de eventos de segurança analisados por fonte e a respectiva ação tomada;
13.14.17.2 Incidentes gerados, bem como o status de cada incidente.
Os status devem ser, no mínimo:
13.14.17.2.1. Novo;
13.14.17.2.2. Novo e atribuído;
13.14.17.2.3. Em progresso;
13.14.17.2.4. Fechado;
13.14.18 O dashboard deve permitir filtrar os incidentes por prioridade;
13.14.19 Deve prover uma visão de incidentes abertos e atribuídos por analista;
13.14.20 A ferramenta deve alertar os administradores através das seguintes ferramentas:
13.14.20.1 E-mail;
13.14.20.2 Slack;
13.14.20.3 Teams;
13.14.21 Deverá possuir ferramenta de consulta de indicadores em uma base de inteligência do próprio fabricante;
13.14.22 A consulta deve permitir no mínimo os seguintes indicadores: 13.14.22.1. URL;
13.14.22.2. Domínio;
13.14.22.3. Hash do arquivo (MD5, SHA1 ou SHA256); 13.14.22.4. Endereço IP;
13.14.23 Deve ser possível enviar um arquivo através da console de administração ou já analisar de forma automática os arquivos em ambiente de sandboxing do fabricante, retornando o veredito da emulação;
13.14.24 A console administrativa deve fornecer uma ferramenta investigativa que permite consultas avançadas sobre todos os eventos forenses (maliciosos e benignos) coletados;
13.14.25 A ferramenta de investigação deve possuir filtros de consultas pré- definidas para auxiliar na análise;
13.14.26 A ferramenta deverá ser capaz de reter logs por pelo menos 90 dias;
13.14.27 A solução deverá fornecer um local central para gerenciar indicadores de compromisso (IoCs) de todos os produtos integrados;
13.14.28 O gerenciador de IoCs pode integrar com feeds personalizados de várias fontes e combiná-los em um único feed de fácil acesso;
13.14.29 O gerenciador de IoCs também deve permitir com que o administrador crie ou importe sua própria lista de indicadores de compromisso.
13.14.30 Deverá permitir automatizar operações de segurança com pelo menos as seguintes ações:

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

13.14.30.1 Isolar um endpoint infectado;
13.14.30.2 Deletar um arquivo da máquina;
13.14.30.3 Terminar um processo da máquina;
13.14.30.4 Alertar no caso de uma possível exploração;
13.14.30.5 Alertar no caso de tentativas repetidas de logins em dispositivos Windows;

13.14.31 A solução deve gerar logs de auditoria para registrar mudanças de configurações do produto para, pelo menos:
13.14.31.1 Mudanças de políticas;
13.14.31.2 Notificações enviadas;
13.14.31.3 Criação de exclusões;
13.14.32 Deve ser possível exportar logs de auditoria em pelo menos dois dos seguintes formatos:
13.14.32.1 CSV
13.14.32.2 XLS
13.14.32.3 HTML
13.14.32.4 PDF
13.14.33 Deve permitir gerar relatórios, com capacidade para agendar envios de forma diária, semanal ou mensal;
13.14.34 A solução deve dispor de REST API para consulta de incidentes e dados forenses;
13.14.35 Deve permitir a integração com ferramentas para abertura de tickets de forma automática, sendo elas, no mínimo:
13.14.35.1 Jira
13.14.35.2 ServiceNow
13.14.36 Deve permitir a visualização das automações executadas, bem como dia e hora da execução;

14. SERVIÇO DE INSTALAÇÃO E PARAMETRIZAÇÃO

14.1 CARACTERÍSTICAS GERAIS DE IMPLANTAÇÃO
14.1.1 É/será de inteira responsabilidade da CONTRATADA a correta instalação, configuração e funcionamento dos equipamentos e/ou componentes da solução ofertada como um todo. Os equipamentos e/ou componentes serão implementados pela CONTRATADA de acordo com os termos deste TR.
14.1.2 Não serão admitidos configurações e ajustes que impliquem no funcionamento do equipamento ou componente de hardware fora das condições normais recomendadas pelo fabricante.
14.1.3 Deverá ser realizada uma reunião de kick-off do projeto, nas instalações do CONTRATANTE, com a participação do gerente técnico do projeto, dos responsáveis comercial, de design da solução como um todo, pelo técnico responsável pela implementação do projeto;
14.1.4 O planejamento dos serviços de instalação deve resultar num documento tipo SOW (Scope of Work, em tradução livre, escopo de trabalho). Neste documento devem conter a relação, descrição e quantidades dos produtos fornecidos, descrição da infraestrutura atual e desejada, topologia do ambiente, detalhamento dos serviços que serão executados, premissas do projeto, locais e horários de execução dos serviços, condições de execução dos serviços, pontos de contato do CONTRATANTE e CONTRATADA, cronograma de execução do projeto em etapas, com responsáveis e data e início e fim (se aplicável), relação da documentação a ser entregue ao final da execução dos serviços, responsabilidade do CONTRATANTE e CONTRATADA, plano de gerenciamento de mudanças, itens excluídos no projeto e termo de aceite;
14.1.5 Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, devendo a CONTRATADA sugerir as configurações de acordo com normas técnicas e boas práticas, cabendo à contratante a sua aceitação expressa ou recusa nos

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

casos de não atendimento das condições estabelecidas;

14.1.6 Os serviços deverão ser realizados por pessoal técnico experiente e certificado pelo fabricante dos equipamentos. Em momento anterior à instalação, a contratante poderá solicitar os comprovantes da qualificação profissional do técnico que executará os serviços, sendo direito da mesma a sua aceitação ou exigência de troca de profissional no caso de este não satisfizer às condições supramencionadas;

14.1.7 Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (relatório as-built), etapas de execução e toda informação pertinente para posterior continuidade e manutenção da solução instalada como um todo, como usuários e endereços de acesso, configurações realizadas e o resumo das configurações dos equipamentos. Este relatório deve ser enviado com todas as informações em até 15 (quinze) dias após a finalização dos serviços;

14.1.8 A CONTRATADA deverá fornecer documentação completa da solução, incluindo especificação do(s) equipamento(s), características e funcionalidades implementadas, desenho lógico da implantação, comentários e configurações executadas. Deverá conter também todas as configurações executadas em equipamentos de terceiros, quando for o caso;

14.2 CARACTERÍSTICAS ESPECÍFICAS DE IMPLANTAÇÃO DO ITEM 1 – SOLUÇÃO DE SEGURANÇA DE REDE

14.2.1 A CONTRATADA deverá realizar a instalação física e lógica dos appliances de segurança de perímetro, incluindo montagem em rack, energização, conexão de interfaces e verificação de integridade do hardware.

14.2.2 A parametrização da solução deverá contemplar o modo de operação definido no projeto (standalone, cluster ativo-passivo ou ativo-ativo),configurando sincronização de estado, políticas de failover e testes de redundância.

14.2.3 A criação e/ou migração de políticas de segurança deverá seguir critérios de mínima permissão, segmentação lógica da rede, regras baseadas em aplicação e identificação de usuários, quando aplicável.

14.2.4 A CONTRATADA deverá implementar os serviços de inspeção de tráfego tais como filtragem de aplicações, IPS, controle de URL, anti-malware e quaisquer outros módulos habilitados durante o projeto.

14.2.5 Deverá ser realizado o hardening da solução, incluindo configuração de perfis administrativos, métodos de autenticação, registro de logs, políticas de auditoria, parâmetros de segurança recomendados pelo fabricante e desativação de serviços desnecessários.

14.2.6 A CONTRATADA deverá realizar a integração da solução com sistemas externos quando previsto, tais como diretórios de usuários, servidores de log, SIEM, orquestradores de eventos ou demais ferramentas de gerenciamento.

14.2.7 Deverão ser realizados testes completos de operação, incluindo validação de políticas, inspeção de tráfego, failover, desempenho básico e simulação de fluxos críticos da rede do CONTRATANTE.

14.3 CARACTERÍSTICAS ESPECÍFICAS DE IMPLANTAÇÃO DOS ITENS 2 A 6 – SOLUÇÃO DE CONECTIVIDADE DE REDE SEGURA

14.3.1 A instalação deverá contemplar a montagem física dos equipamentos, conexões de uplinks, organização de cabos, energização adequada e identificação visual conforme padrões do CONTRATANTE.

14.3.2 Os switches deverão ser configurados conforme a topologia prevista no SOW, observando boas práticas de segmentação com VLANs, trunking, redundância de enlaces, agregação de portas e spanning-tree, quando aplicável;

14.3.3 Deverão ser aplicados os parâmetros de segurança de acesso ao plano de

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

gerenciamento, tais como AAA, perfis administrativos, SNMP seguro, desativação de protocolos legados e proteção contra ataques de camada 2, quando aplicável;

14.3.4 A CONTRATADA deverá definir e aplicar parâmetros de QoS, quando necessários, com priorização de tráfego crítico, classificação e marcação conforme requisitos do CONTRATANTE;

14.3.5 A solução deverá ser integrada ao sistema de gerenciamento centralizado previsto no escopo, possibilitando monitoramento unificado, telemetria, templates de configuração, relatórios e notificações.

14.3.6 Deverão ser realizados testes de conectividade fim a fim, validação de redundância, verificação de tabelas MAC e roteamento (quando aplicável), além de confirmação do funcionamento dos enlaces com os equipamentos adjacentes;

14.4 CARACTERÍSTICAS ESPECÍFICAS DE IMPLANTAÇÃO DO ITEM 7 – SOLUÇÃO DE CONECTIVIDADE DE REDE SEGURA – TIPO WI-FI

14.4.1 A CONTRATADA deverá realizar estudo de posicionamento dos pontos de acesso de rede sem fio, utilizando, para isso, ferramenta especializada de *survey*, com relatórios que demonstrem, em planta baixa fornecida pela CONTRATANTE, o mapa de sinal e melhores pontos de fixação dos pontos de acesso de rede sem fio;

14.4.2 A CONTRATADA deverá realizar a instalação física dos pontos de acesso, incluindo fixação em estruturas, passagem e organização de cabos, conexão a switches, conferência de PoE conforme o posicionamento definido no estudo de posicionamento;

14.4.2.1 Para fins de dimensionamento dos materiais, acessórios e insumos necessários à instalação física dos pontos de acesso, a CONTRATADA deverá considerar, no mínimo, as seguintes diretrizes técnicas:

14.4.2.1.1 Utilização obrigatória de cabo de par trançado UTP categoria 6 ou superior, devidamente certificado, para interligação dos pontos de acesso aos switches PoE;

14.4.2.1.2 Previsão de um cabo dedicado por ponto de acesso, com margem mínima adicional de 10% para folga técnica e acomodações no percurso;

14.4.2.1.3 Fornecimento e instalação de suportes adequados ao modelo de ponto de acesso, incluindo suportes de teto, parede, forro mineral ou metálico, quando aplicável, devendo o licitante prever suportes universais ou específicos, garantindo a fixação adequada;

14.4.2.1.4 Previsão de fixadores, buchas, parafusos e materiais de sustentação, compatíveis com os tipos mais comuns de superfície (alvenaria, drywall, madeira ou estrutura metálica);

14.4.2.1.5 Fornecimento de cordoalhas, abraçadeiras, velcros, canaletas simples ou similares, a critério da CONTRATADA, para organização do cabeamento até o ponto de terminação;

14.4.2.1.6 Previsão de ponto de terminação em patch panel categoria
6 ou superior, quando aplicável, incluindo conectorização conforme padrões TIA/EIA vigentes;

14.4.2.1.7 Entrega e instalação de patch cords CAT6 ou superior, com comprimento adequado ao rack ou ponto de concentração;

14.4.2.1.8 Previsão de eventuais extensões de cabo UTP para acomodar variações de rota durante a execução, respeitando o comprimento máximo de 80 metros por enlace;

14.4.2.1.9 Previsão de identificação física dos cabos, pontos e portas correspondentes nos switches, utilizando etiquetas permanentes, legíveis e padronizadas;

14.4.2.1.10 O licitante deverá prever materiais de acabamento para a passagem de cabos quando não houver infraestrutura adequada disponível, tais como canaletas plásticas, conduítes flexíveis ou equivalentes, limitados a trechos curtos necessários à proteção e organização imediata da instalação;

14.4.3 A configuração lógica deverá incluir SSIDs, autenticação, controle de acesso, segmentação por VLAN, limitação de banda, políticas de RF e parâmetros avançados de rádio conforme boas práticas.

14.4.4 Deverá ser configurado e integrado o controlador ou gerenciador central, garantindo

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

provisionamento automático (zero-touch, quando aplicável), atualização de firmware e aplicação de perfis padronizados.

14.4.5 A solução deverá implementar mecanismos de segurança adequados, incluindo WPA3 ou equivalente, proteção contra rogue AP, detecção de interferência, isolamento de clientes e controles adicionais aplicáveis;

14.4.6 Deverão ser realizados testes de cobertura, testes de roaming, aferição de desempenho, validação de autenticação e conectividade fim a fim.

14.5 CARACTERÍSTICAS ESPECÍFICAS DE IMPLANTAÇÃO DO ITEM 8 – SOLUÇÃO DE MONITORAMENTO DE REDE

14.5.1 A CONTRATADA deverá instalar os sensores de monitoramento em pontos estratégicos definidos pela CONTRATANTE, garantindo alimentação, conectividade e visibilidade do ambiente para o monitoramento da experiência do usuário;

14.5.2 Os sensores deverão ser integrados à plataforma de monitoramento central, garantindo recebimento de telemetria, visibilidade de tráfego e funcionamento de mecanismos de detecção;

14.5.3 Deverá ser ajustado o baseline operacional da rede para que o sistema diferencie comportamentos normais de eventos anômalos, possibilitando geração de alertas consistentes;

14.5.4 A CONTRATADA deverá realizar testes de validação, simulando eventos, interrupções, quedas de enlace ou anomalias de tráfego para confirmar o funcionamento dos mecanismos de monitoramento;

14.6 CARACTERÍSTICAS ESPECÍFICAS DE IMPLANTAÇÃO DO ITEM 9 – SOLUÇÃO DE SEGURANÇA DE ACESSO À REDE

14.6.1 A instalação deverá contemplar a montagem dos servidores/appliances, configuração de rede, integração com diretórios de usuários e validação de comunicação entre componentes da arquitetura;

14.6.2 Deverá ser realizado o onboarding do ambiente, incluindo definição de perfis de acesso, roles, enforcement, autenticação 802.1X ou mecanismos alternativos previstos no projeto;

14.6.3 Deverá ser estabelecido o fluxo de avaliação de postura de dispositivos (Posture Assessment), quando previsto, incluindo verificações de antivírus, patches, políticas e parâmetros adicionais;

14.6.4 A solução deverá ser integrada aos switches e controladores Wi-Fi do CONTRATANTE, configurando mecanismos de autorização dinâmica, atribuição de VLAN e aplicação de políticas conforme perfil do usuário ou dispositivo;

14.6.5 A CONTRATADA deverá realizar testes de acesso autenticado, não autenticado, convidado, dispositivo corporativo e dispositivo não conforme, garantindo o funcionamento completo de todos os fluxos;

14.7 CARACTERÍSTICAS ESPECÍFICAS DE IMPLANTAÇÃO DO ITEM 10 – SOLUÇÃO DE SEGURANÇA DAS APLICAÇÕES

14.7.1 A instalação deverá contemplar provisionamento, configuração de ambientes, criação de serviços, validação de conectividade com backends e integração com provedores externos quando necessário.

14.7.2 A configuração deverá incluir proteção de aplicações, políticas de segurança, mitigação de ataques, certificados digitais, controle de acesso e demais funcionalidades previstas no edital;

14.7.3 Quando aplicável, a CONTRATADA deverá configurar conectores, edges locais ou componentes que permitam integração entre o ambiente do CONTRATANTE e a plataforma;

14.7.4 Deverá ser configurado o balanceamento de carga, regras de encaminhamento, health checks e políticas de disponibilidade conforme arquitetura definida no SOW;

14.7.5 A CONTRATADA deverá realizar testes de acesso às aplicações, comportamento sob

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

falhas, validação de políticas de segurança e simulação de eventos de proteção.

14.8 CARACTERÍSTICAS ESPECÍFICAS DE IMPLANTAÇÃO DO ITEM 11 – SOLUÇÃO DE SEGURANÇA DE E-MAIL

14.8.1 A implantação deverá contemplar integração com o provedor de e-mail do CONTRATANTE, configurando APIs, conectores ou métodos de autenticação necessários ao funcionamento da solução.

14.8.2 Deverão ser configuradas políticas de proteção contra phishing, malware, spam, anexos, links, BEC e demais mecanismos previstos no edital.

14.8.3 Deverá ser realizada a sincronização de usuários e grupos, definição de perfis, escopos de proteção e parâmetros administrativos.

14.8.4 A CONTRATADA deverá configurar fluxos de quarentena, relatórios, dashboards, alertas e automações previstas no projeto.

14.8.5 Testes deverão ser executados, incluindo envio de mensagens internas, externas, simulações de mensagens maliciosas e verificação do comportamento da solução.

14.9 CARACTERÍSTICAS ESPECÍFICAS DE IMPLANTAÇÃO DO ITEM 12 – SOLUÇÃO DE SEGURANÇA DOS DISPOSITIVOS DE ACESSO À REDE

14.9.1 A CONTRATADA deverá realizar o provisionamento da plataforma de gerenciamento, configurando políticas de segurança, perfis de agentes e integrações necessárias.

14.9.2 Deverá ser realizada a instalação dos agentes nos dispositivos do CONTRATANTE conforme inventário, incluindo validações de compatibilidade, métodos de distribuição e testes de operação.

14.9.3 As políticas deverão contemplar proteção antimalware, controle de acesso, firewall de endpoint, proteção comportamental, prevenção contra ransomware, controle de dispositivos e demais módulos previstos.

14.9.4 Quando aplicável, deverá ser configurado o módulo de visibilidade estendida, incluindo coleta de telemetria, correlação de eventos, automações, workflows e integrações com SIEM ou plataformas equivalentes.

14.9.5 Deverão ser executados testes práticos de funcionamento, incluindo verificação de detecções, resposta automatizada, geração de alertas, bloqueios e validação de análises de endpoint.

14.10 REPASSE DE CONHECIMENTO

14.10.1 Ao término da implantação de cada solução contemplada neste edital, a CONTRATADA deverá realizar sessão de repasse técnico de conhecimento para a equipe designada pela CONTRATANTE, com o objetivo de apresentar o funcionamento básico da solução instalada, suas principais funcionalidades, parâmetros configurados e procedimentos operacionais essenciais para acompanhamento rotineiro do ambiente.

14.10.2 O repasse técnico de conhecimento não se caracteriza como treinamento oficial, não substitui cursos certificados do fabricante e não confere certificação, devendo restringir-se à apresentação prática da solução, topologia final, políticas aplicadas, rotinas de operação e documentação entregue.

14.10.3 A sessão deverá contemplar, no mínimo:

14.10.3.1 Visão geral da arquitetura implantada e da comunicação entre os componentes;

14.10.3.2 Descrição dos principais parâmetros configurados e das políticas aplicadas;

14.10.3.3 Demonstração dos painéis, dashboards e interfaces administrativas essenciais ao acompanhamento do ambiente;

14.10.3.4 Explicação dos procedimentos mínimos para abertura de chamados, coleta de evidências e acompanhamento de incidentes;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

14.10.3.5 Orientações sobre acesso administrativo, boas práticas básicas de operação e pontos de atenção.
14.10.4 O repasse técnico deverá ocorrer após a conclusão do as-built, em data acordada entre as partes, preferencialmente de forma presencial ou por videoconferência em ambiente compartilhado, devendo ter duração compatível com a complexidade da solução instalada, não inferior a 2 (duas) horas por solução.
14.10.5 A CONTRATADA deverá disponibilizar profissional tecnicamente qualificado e experiente na solução instalada, sendo vedada a utilização de pessoal sem domínio técnico do ambiente entregue ou sem participação direta na implantação.
14.10.6 Após a realização do repasse técnico, a CONTRATADA deverá registrar a sessão em ata detalhada contendo: participantes, data, tópicos abordados e eventuais dúvidas esclarecidas. A ata deverá ser assinada pelas partes e anexada ao processo de aceite definitivo da implantação.

15. SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO 24X7

15.1 A CONTRATADA será responsável pela administração e manutenção do serviço em regime de 24x7x365 para atendimentos remotos e o regime 8x5 para atendimentos que possam ser necessários na forma presencial, durante todo o período do serviço contemplado nesse edital.
15.2 As tarefas atinentes ao transporte, deslocamento e remessa necessários, seja na implementação, substituição e/ ou remoção de equipamentos defeituosos será de responsabilidade da CONTRATADA.
15.3 A CONTRATANTE poderá solicitar qualquer relatório ou informação de qualquer parte da solução com uma frequência mensal o que deverá ser provido pela contratada num prazo de 5 dias úteis.
15.4 Para garantir a qualidade e disponibilidade do serviço, deverá ser disponibilizado pela empresa CONTRATADA uma ferramenta de visibilidade e monitoramento com estrutura dedicada para a CONTRATANTE que atenda as características mínimas descritas no ANEXO A.
15.5 A ferramenta deve ser acompanhada de todos os itens necessários para operacionalização, tais como: softwares de apoio (sistema operacional, etc) e licenças de softwares;
15.6 O serviço de monitoramento 24x7 deverá ser prestado OBRIGATÓRIA E INDISPENSAVELMENTE através de NOCs (Network Operation Center) redundantes da empresa CONTRATADA que já deverão estar em pleno funcionamento até a data da assinatura do contrato. Será o ponto único de contato com a equipe técnica da CONTRATANTE para abertura de chamados, incidentes, problemas, dúvidas e requisições relacionadas aos serviços contratados, atuando como a primeira instância de atendimento à CONTRATANTE.
15.7 Os serviços prestados pelo NOC compreendem, entre outros, os seguintes procedimentos:
15.7.1 Suporte técnico para identificação e resolução de problemas em software e hardware;
15.7.2 Resolução de problemas quanto acesso à internet, sites remotos, serviços de rede oferecidos aos funcionários do CONTRATANTE;
15.7.3 Suporte em criação de políticas, configurações, parametrizações de quaisquer ordens relativos aos equipamentos ofertados;
15.7.4 Resolução de problemas referente a políticas, configurações, parametrizações de quaisquer ordens relativos aos equipamentos ofertados;
15.7.5 Suporte à criação, geração e parametrização de relatórios e eventos de segurança/rede de quaisquer naturezas detectados e prevenidos pelos equipamentos ofertados;
15.7.6 Encaminhar incidentes ao fabricante da solução;
15.7.7 Suporte em demais configurações de segurança, redundância e gerência;
15.7.8 Suporte, administração e monitoramento das políticas e tarefas de backup das configurações;
15.7.9 Apoio técnico para tarefas de auditoria e análise de logs.
15.8 A CONTRATADA deverá agir de forma reativa para incidentes, restabelecimento do serviço o

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

mais rápido possível minimizando o impacto, seja por meio de uma solução de contorno ou definitiva. Ainda caberá a CONTRATADA agir de forma proativa aplicando medidas para a boa manutenção afim de garantir a regularidade da operação do serviço.

15.9 O atendimento e suporte técnico especializado de 1º (primeiro nível) será sempre telefônico e remoto em regime 24x7 e assim, responsável pelo acompanhamento e gestão dos chamados, controle dos indicadores de monitoramento, atuando como ponto único de contato entre a CONTRATANTE e profissionais da equipe da CONTRATADA.

15.10 O atendimento e suporte técnico especializado de 2º (segundo nível) poderá ser presencial ou remoto em regime 8x5 em Fortaleza/CE, caso o suporte remoto não seja suficiente para resolução do problema. Responsável pela prevenção e resolução de incidentes, problemas e requisições, identificando a causa raiz de eventual problema e buscando sua solução. Execução de atividades remotas e/ou presenciais em incidentes, solicitações de maior complexidade.

15.11 Os técnicos deverão ser capacitados e certificados para prestação dos serviços, resolução de incidentes, problemas e solicitações nos equipamentos ofertados. O comparecimento de um técnico ao local da necessidade será de no máximo 48 (quarenta e oito) horas para atendimentos na área que abrange e define a Região Metropolitana de Fortaleza devendo sempre atender aos critérios de SLA determinados nesse edital.

15.12 Para abertura dos chamados de suporte, a CONTRATADA deverá disponibilizar número telefônico 0800 (ou equivalente a ligação local), também serviço via portal WEB e/ou e-mail (em português). Na abertura do chamado, o órgão ao fazê-lo, receberá naquele momento, o número, data e hora de abertura do chamado. Este será considerado o início para contagem dos SLAs. O fechamento do chamado deverá ser comunicado pela CONTRATADA para fins de contagem do tempo de atendimento e resolução do chamado.

15.13 A atualização de firmware quando disponibilizado exclusivamente pelo próprio fabricante dos equipamentos deverá ser executada pela CONTRATADA sem custo adicional, sempre que requisitado pela CONTRATANTE. Toda e qualquer atualização só poderá ser aplicada mediante autorização da CONTRATANTE. As atualizações deverão ocorrer em data e horário determinado pela CONTRATADA em comum acordo e autorização da CONTRATANTE visando manter em normal funcionamento a rede onde estiverem funcionando.

15.14 A CONTRATADA deverá fornecer informações de monitoramento on-line, via dashboard que permita o acompanhamento em tempo real do estado dos ativos. Deverá ainda apresentar relatórios mensais, por meio digital (DOCX, XLSX ou PDF), com o diagnóstico e controle dos equipamentos monitorados (dados, informações, descrição, indicadores e métricas que permitam quantificar o desempenho e a disponibilidade da operação do serviço).

15.15 A CONTRATADA deverá disponibilizar uma ferramenta de Service Desk comprovadamente aderente as boas práticas do ITIL e que contenha o detalhamento dos chamados com no mínimo as seguintes informações: o funcionário do órgão/entidade que realizou a abertura do chamado, data e hora de abertura, data e hora de atendimento, data e hora de solução, o funcionário do órgão/entidade que realizou o encerramento do chamado, descrição detalhada do problema e das ações tomadas para sua resolução e a relação dos equipamentos ou componentes substituídos, especificando marca, modelo, fabricante e número de série).

15.16 Os relatórios de chamados abertos poderão ser solicitados a qualquer instante pela CONTRATANTE dentro das condições estipuladas, respeitando, no entanto, um prazo de até 48 (quarenta e oito) horas uteis. Esses relatórios deverão ser retidos pelo tempo mínimo equivalente a vigência do contrato e após o seu encerramento inutilizados.

15.17 A CONTRATADA deverá comunicar ao CONTRATANTE, os casos de eminente falha operacional dos equipamentos ou de qualquer outra ação que possa vir a colocar em risco a operação da rede dela, mesmo que a falha não tenha sido consumada, mas que tenha sido detectada a existência do risco.

15.18 A CONTRATANTE deverá definir pessoas do seu Quadro de Funcionários que terão acesso de Administração nos equipamentos disponibilizados e essas pessoas deverão comunicar à empresa CONTRATADA qualquer alteração de configuração realizada nos equipamentos

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

fornecidos nessa contratação e nessa situação respondendo por sua conta e risco pelas intervenções que possam ter efetuado.

15.19 A CONTRATADA deverá respeitar os tempos máximos de ATENDIMENTOS e SLA (Nível de Acordo de Serviço) abaixo descritos, sob a pena de multa no caso de falhas em seu integral cumprimento:

15.19.1 Operação parada (incidente que gere parada total de algum serviço contemplado nesse contrato) o tempo de atendimento será de até 2 (duas) horas.

15.19.2 Operação impactada (incidente que gere parada parcial de algum serviço contemplado nesse contrato) o tempo de atendimento será de até 4 (quatro) horas.

15.19.3 Requisição de serviço (solicitações de mudanças nos equipamentos ou serviços do contrato) o tempo de atendimento será de até 8 (oito) horas.

15.19.4 Informações de contrato (solicitação de informação, parecer ou relatório de algum serviço contemplado no contrato) o tempo de atendimento será de até 12 (doze) horas.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

ANEXO A

PLATAFORMA DE MONITORAMENTO

1. A Plataforma de Monitoramento deverá permitir a monitoração dos firewalls, a partir de um servidor central, possibilitando a geração de notificações específicas para cada equipe, através de acesso WEB à aplicação de gerenciamento com as seguintes características:
2. A interface de gerenciamento deverá ser em modo WEB acessada através de navegador.
3. Deverá ser compatível com, pelo menos, um dos seguintes navegadores atuais: Google Chrome, Mozilla Firefox ou Microsoft Edge.
4. Permitir que as informações gerenciadas, coletadas em diversos pontos de captura, sejam consolidadas em uma única visão em um console gráfico central.
5. Possuir a capacidade de reiniciar serviços de monitoração automaticamente após a ocorrência de "queda" e alertar em sequência o retorno do equipamento que está sendo gerenciado.
6. Deverá ter capacidade de monitoração dos equipamentos ofertados neste edital em, pelo menos, os seguintes itens:

6.1. Modelo do equipamento;
6.2. Utilização de CPU;
6.3. Uso de memória RAM;
6.4. Espaço livre em disco;
6.5. Versão do sistema operacional;
6.6. Status ou data de expiração do licenciamento;
6.7. Temperatura de operação do equipamento;
6.8. Status da (s) fonte (s) de alimentação;
6.9. Número de conexões ou sessões concorrentes;
6.10. Lista de interfaces de rede, contemplando, também:
6.11. Status das interfaces;
6.12. Throughput das interfaces;
6.13. Status da funcionalidade de alta disponibilidade;

7. Gatilhos e alertas:

7.1. A plataforma deve permitir a construção para a detecção de eventos (gatilhos) de acordo com a necessidade de gerenciamento dos sistemas, gerando os alertas necessários. Como exemplo, ela deve permitir a criação de gatilhos quando limites forem excedidos. Os alertas devem ser configuráveis para criação de SLAs. Os alertas devem ser visualizados também pela interface gráfica.

7.2. O envio de E-mail e SMS devem ser configurados por tipo de alerta em cada recurso monitorado, permitindo, por exemplo, que em diferentes interfaces de um mesmo equipamento existam gatilhos e formas de envios diferentes.

7.3. Prover o envio de alarmes para a console de gerenciamento de aplicações e E-mails e SMS para os Administradores quando os recursos monitorados atingirem os seus respectivos gatilhos.

7.4. Para o mesmo item podem ser gerados vários gatilhos com criticidade diferentes, permitindo assim, um melhor controle do tipo de problema.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

8. Possuir processo de coleta que não necessite a instalação de agentes nos equipamentos monitorados;
9. Deve suportar o monitoramento através do protocolo SNMP nas versões 1, 2c e 3 e SNMP Traps;
10. Análise, relatórios e comparação:
10.1. Armazenar informações para posterior análise, que possa permitir comparações para acertos nos equipamentos.
11. A solução deverá possuir uma interface interna para geração de relatórios.
12. A solução deve possuir interface WEB para geração e visualização de relatórios.
13. A interface WEB deve possibilitar o envio de relatórios por E-mail manualmente ou mesmo préagendar a geração e o envio em uma data ou horários especificados.
14. A solução deve possibilitar a exportação dos relatórios em pelo menos dois dos seguintes formatos:
14.1. PDF.
14.2. HTML.
14.3. CSV.
15. Todos os relatórios devem ter a flexibilidade de exibir informações em tempo real e também dados históricos, coletados em períodos anteriores.
16. A solução deve permitir a publicação automática de relatórios no formato HTML em um servidor WEB, permitindo uma análise sobre a situação dos servidores monitorados, com as seguintes características:
16.1. Apresentação dos nomes dos equipamentos no relatório.
16.2. Apresentação das informações gerenciadas por equipamento.
16.3. Exibição por grupo de equipamentos previamente estabelecidos.
16.4. Opções de periodicidade especificada pelo usuário: diária, semanal, mensal, trimestral, anual ou intervalo de data.
17. Apresentação em modo gráfico:

17.1. Dependência entre objetos monitorados: permitir que sejam cadastradas dependências entre os objetos monitorados, inclusive no nível de subitem de monitoramento, permitindo analisar o impacto de uma parada perante os demais objetos monitorados;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

ANEXO II - MODELO DE PROPOSTA DE PREÇOS

A Pregoeira da Câmara Municipal de Fortaleza
Ref.: PREGÃO ELETRÔNICO nº 02/2026.

Pelo presente instrumento, vimos apresentar nossa proposta de preços relativa ao objeto desta licitação, bem como as informações, condições da proposta e declarações exigidas no edital do pregão acima citado.

1) Identificação do Licitante:
Razão Social: CNPJ e Inscrição Estadual: Endereço completo:
Telefone, fax, e-mail: Banco, Agência e nº da conta corrente:

2) Condições Gerais da Proposta:
A presente proposta é válida por _____ (_____) dias contados da data de sua apresentação.

3) Pelo presente, a empresa acima qualificada, por meio do signatário, que legalmente a representa, declara e garante que:
• examinou cuidadosamente todo o Edital e Anexos e aceita todas as condições nele estipulados e que, ao assinar a presente declaração, renuncia ao direito de alegar discrepância de entendimento com relação ao Edital;
• que cumpre plenamente as disposições normativas relativas ao trabalho do menor, contida na Lei nº 9.854, de 27/10/1999 e na Constituição Federal de 1988;
• que tomou conhecimento de todas as informações e das condições para cumprimento das obrigações, objeto da presente licitação;
• que sua proposta engloba todas as despesas, incluindo todos os tributos, encargos sociais e trabalhistas e quaisquer outras que incidam ou venham incidir sobre o objeto da licitação.

Obs: O proponente deverá declarar, sob as penalidades da lei, a existência de fato superveniente impeditivo de sua habilitação, somente se houver.

PROPOSTA DE PREÇOS:

VALOR TOTAL R$ _____ (Valor por extenso_____)

(Assinatura do Representante legal)
Nome do Signatário
CPF

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

ANEXO III- MODELO DE DECLARAÇÃO DE CONDUTA ÉTICA E ANTICORRUPÇÃO

(NOME DA LICITANTE), declaro para os devidos fins que, como licitante e, eventualmente contratada, observará e fará observar pelos fornecedores e subcontratados, se admitida subcontratação, a prática do mais alto padrão de ética durante todo o processo de licitação, de contratação e de execução do objeto contratual.

I – Para os propósitos desta declaração, definem-se as seguintes práticas:

a) “prática corrupta”: oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer vantagem com o objetivo de influenciar a ação de servidor público no processo de licitação ou na execução de contrato;

b) “prática fraudulenta”: a falsificação ou omissão dos fatos, com o objetivo de influenciar o processo de licitação ou de execução de contrato;

c) “prática colusiva”: esquematizar ou estabelecer um acordo entre duas ou mais licitantes, com ou sem o conhecimento de representantes ou prepostos do órgão licitador, visando estabelecer preços em níveis artificiais e não-competitivos;

d) “prática coercitiva”: causar ou ameaçar causar dano, direta ou indiretamente, às pessoas ou sua propriedade, visando influenciar sua participação em um processo licitatório ou afetar a execução do contrato;

e) “prática obstrutiva”:
(i) destruir, falsificar, alterar ou ocultar provas em inspeções ou fazer declarações falsas aos representantes do organismo financeiro multilateral, com o objetivo de impedir materialmente a apuração de alegações de prática prevista, deste Edital;
(ii) atos cuja intenção seja impedir materialmente o exercício do direito de o organismo financeiro multilateral promover inspeção.

II – Na hipótese de financiamento, parcial ou integral, por organismo financeiro multilateral, mediante adiantamento ou reembolso, este organismo imporá sanção sobre uma empresa ou pessoa física, inclusive declarando-a inelegível, indefinidamente ou por prazo determinado, para a outorga de contratos financiados pelo organismo se, em qualquer momento, constatar o envolvimento da empresa, diretamente ou por meio de um agente, em práticas corruptas, fraudulentas, colusivas, coercitivas ou obstrutivas ao participar da licitação ou da execução de um contrato financiado pelo organismo.

III – Considerando os propósitos das cláusulas acima, a licitante vencedora, como condição para a contratação, deverá concordar e autorizar que, na hipótese de o contrato vir a ser financiado, em parte ou integralmente, por organismo financeiro multilateral, mediante adiantamento ou reembolso, permitirá que o organismo financeiro e/ou pessoas por ele formalmente indicadas possam inspecionar o local de execução do contrato e todos os documentos, contas e registros relacionados à licitação e à execução do contrato.

Local/data

Licitante

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

ANEXO IV - JUSTIFICATIVA DA ESCOLHA DO ORÇAMENTO SIGILOSO

O caráter sigiloso do orçamento tem como base obter as melhores propostas, haja vista que a divulgação dos preços traria para o certame empresas sem a devida precisão orçamentária, e ensejaria o alinhamento de propostas, e o contrário é que as empresas apresentem seus preços de reservas, quer-se ainda atrair empresas com expertise na prestação de serviços, objeto deste certame.

Com base no Art. 24 da Lei nº 14.133/21 e no artigo 54 do Decreto Municipal nº 15.595/2023, o orçamento sigiloso poderá ser usado desde que devidamente justificado, sem prejuízo da divulgação dos detalhamentos, sendo eles quantitativos e informações necessárias para a elaboração das propostas, como podemos observar:

> *Art. 24 – Desde que justificado, o orçamento estimado da contratação poderá ter caráter sigiloso, sem prejuízo da divulgação dos detalhamentos dos quantitativos e das demais informações necessárias para a elaboração das propostas...*

Buscando, através do orçamento sigiloso, a transparência da administração pública, na escolha da contratada que, sabendo dos riscos e dificuldades do serviço, apresente uma proposta conforme a realidade a qual possa honrar tal compromisso assumido na fase de propostas, corroborando com tal entendimento, Zymler e Dias (2014, p. 117):

> *A não divulgação do orçamento tem por objetivo evitar que as propostas/lances gravitem em torno do orçamento fixado pela administração. Essa medida deve se mostrar particularmente eficaz quando houver a ocorrência de lances fechados, pois, sem as balizas dos outros licitantes e do orçamento da administração, o competidor deve, já nessa etapa, oferecer um preço realmente competitivo e dentro do limite de sua capacidade de executar a avença com uma lucratividade adequada. Caso assim não proceda, esse competidor corre o risco de ser desclassificado sem as possibilidades de apresentar outra proposta mais competitiva, de acordo com os critérios que regem a apresentação de lances fechados. Amplia-se, assim, a competitividade do certame e propicia-se melhores propostas para a administração. Não se olvida que determinados agentes do mercado participam de licitações e elaboram suas propostas sem analisar sua capacidade de honrá-las. Esses agentes, seja por não disporem de meios para tanto, seja por não estarem dispostos a arcar com as despesas daí decorrentes, simplesmente se baseiam no orçamento efetuado pela administração. Esse procedimento, contudo, é temerário, pois as propostas podem não refletir a realidade econômica do licitante, redundando em dificuldades posteriores na execução contratual. Desta feita, a não divulgação do orçamento obriga os licitantes a efetivamente analisarem sua estrutura de custos para elaborarem suas propostas. Espera-se, pois, a apresentação de propostas mais realistas economicamente.*

Ainda segundo Zymler e Dios (2014),

> *Em relação a eventual violação do princípio da publicidade, explicitado no caput do art. 37 da Constituição Federal, deve-se lembrar o entendimento de que nenhum princípio constitucional é absoluto de forma que se deve buscar harmonizá-los na hipótese de eventual antagonismo entre dois princípios — no caso o da publicidade em contraposição aos da eficiência elou da economicidade. Nesse contexto de ponderação de princípios, entende-se estar justificada a ausência temporária da divulgação do orçamento, pois amparada no*

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

> *princípio da busca da melhor proposta pela administração. Logo as principais razões do princípio da publicidade estarão atendidas, pois será garantida a transparência do procedimento licitatório com a divulgação do orçamento ao final do certame.*

Nessa toada, importante também as lições do Prof. Ronnye Charles quanto à matéria:

> *"Nesta perspectiva econômica, o caráter sigiloso do orçamento" pode ter o intuito de induzir melhores propostas, atendendo aos princípios da competitividade, da eficiência e da economicidade, buscando evitar que o preço de reserva da Administração influencie o alinhamento das propostas apresentadas; outrossim, no sentido contrário, busca induzir as empresas a apresentarem seu preço de reserva. Por fim, importa destacar interessante efeito prático do sigilo do orçamento, com reflexos positivos ao objetivo de alcançar potencial vantagem no processo competitivo. A não publicação da planilha de custos, preenchida com a estimativa feita pela administração, dificulta a participação de empresas sem expertise, com menor capacidade de planejamento, precificação de custos ou mesmo pouca responsabilidade técnica na confecção de suas propostas. Isso porque, normalmente, elas não possuem equipe de orçamentistas com conhecimento aprofundado pela administração como parâmetro, aplicando apenas um percentual de redução dos valores, muitas vezes, sem um trabalho técnico e responsável de sua própria equipe. Essa dificuldade deve ser compreendida positivamente, pois esse tipo de empresa costuma gerar diversos problemas na execução contratual, com prejuízos flagrantes de ordem financeira e no próprio atendimento da pretensão contratual da administração. Ademais, é ônus para os licitantes estimem seus custos para apresentar suas propostas, antes da licitação, pode ser um fator importante para que licitantes deixem de apresentar propostas com preços inexequíveis, evitando frustrações contratuais, tão prejudiciais à Administração Pública."*

Desta forma, e por todo justificado anteriormente, esta Casa Legislativa informa às empresas participantes deste procedimento que o orçamento previamente estimado para a contratação é sigiloso, ressaltando-se que o sigilo aqui estabelecido não prevalecerá para os órgãos de controle.

EMANUEL ÂNGELO PINHEIRO DO VALE
Diretor Geral

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

ANEXO V - JUSTIFICATIVA DA NÃO PARTICIPAÇÃO DE EMPRESA NA FORMA DE CONSÓRCIO

A Câmara Municipal de Fortaleza vem, por meio deste, apresentar justificativa acerca da não participação de empresas em regime de consórcio no presente procedimento licitatório.

Acerca dos consórcios, este órgão informa que a conveniência de admitir a participação dos mesmos em procedimento licitatório é decisão meramente discricionária da Administração, conforme artigo 15 da Lei nº 14.133/2021.

Dessa forma, não seria vantajoso para a Administração Pública contratar empresas em regime de consórcio, tendo em vista que estas empresas passariam a ter responsabilidade solidária no que concerne às obrigações trabalhistas e previdenciárias, e isso traria riscos para a contratação, porque tal empresa poderá, de repente, ter os seus valores financeiros bloqueados pela Justiça, para fins de pagamento de dívidas, com graves repercussões para o cumprimento do contrato celebrado com a Câmara Municipal de Fortaleza – CMFor.

Outro aspecto importante na vedação de participação de empresas em regime de consórcio é quanto à expertise técnica, na comprovação de execução de serviços semelhantes aos de maior relevância. A comprovação da qualificação técnica tem como finalidade gerar para a Administração a presunção de que a licitante já executou com sucesso objeto similar, tendo condições assim fazê-lo novamente. Essa presunção se forma com base na experiência obtida pela licitante com o exercício dessas atividades pretéritas.

A qualificação técnica da determinada empresa não é algo que possa ser emprestado para outra pessoa jurídica, justamente por haver nela um caráter *intuitu personae* e, como tal, resta claro que pertencer ao consórcio não legitima a equivalência entre a experiência dessas empresas.

Portanto, permitir que uma empresa utilize a expertise de outra para adjudicar para si o objeto da presente licitação não é razoável, visto que, embora pertencentes ao consórcio, é certo que estas empresas não atuaram de forma conjunta na obtenção desses atestados.

EMANUEL ÂNGELO PINHEIRO DO VALE
Diretor Geral

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

ANEXO VI – MINUTA DA ATA DE REGISTRO DE PREÇOS

Ata de Registro de Preços nº ___ /20__
Pregão Eletrônico nº:
Processo Administrativo nº:

O(A).....(*órgão ou entidade pública que gerenciará a ata de registro de preços*), com sede no(a) ....., na cidade de ....., inscrito(a) no CNPJ/MF sob o nº ....., neste ato representado(a) pelo(a) ..... (*cargo e nome*), nomeado(a) pela Portaria nº ..... de ..... de ..... de 202..., publicada no ..... de ..... de ..... de ....., portador da matrícula funcional nº .....,, conforme deliberação constante do julgamento do Pregão Eletrônico nº _____/202_ e do respectivo resultado de homologado, publicado no ..... de ...../...../202....., processo administrativo n.º ....., RESOLVE registrar os preços da(s) empresa(s) indicada(s) nesta ATA, de acordo com a classificação por ela(s) alcançada(s) e na(s) quantidade(s) cotada(s), atendendo as condições previstas no Edital de licitação, sujeitando-se as partes às normas constantes na Lei nº 14.133, de 1º de abril de 2021, no Decreto n.º 15.608, de 31 de março de 2023, e em conformidade com as disposições a seguir:

1. DO FUNDAMENTO LEGAL
O presente instrumento fundamenta-se:

I – No Pregão Eletrônico nº XXXXXXXXX.

II – Nos termos dos Decretos Municipais nº 15.608, de 31 de março de 2023, 15.595, de 22 de março de 2023, 15.604, de 28 de março de 2023 e 13.735, de 18 de janeiro de 2016.

III – Na Lei Federal nº 14.133, de 01 de abril de 2021 e na Lei Complementar nº 123, de 14 de dezembro de 2006 e suas alterações.

IV – Na Lei Federal nº 13.709, de 14 de agosto de 2018 (LGPD – Lei Geral de Proteção de Dados).

2. DO OBJETO

2.1. **CONSTITUI OBJETO DA PRESENTE LICITAÇÃO A CONTRATAÇÃO, POR MEIO DE SISTEMA DE REGISTRO DE PREÇOS, DE EMPRESA ESPECIALIZADA PARA FORNECIMENTO DE SOLUÇÕES TECNOLÓGICAS DE SEGURANÇA, CONECTIVIDADE E REDE WI-FI CORPORATIVA, ABRANGENDO SERVIÇOS TÉCNICOS ESPECIALIZADOS, DESTINADOS À IMPLANTAÇÃO, MODERNIZAÇÃO, OPERAÇÃO E GESTÃO DA INFRAESTRUTURA DE REDE SEM FIO DA SEDE E DO PRÉDIO ANEXO DA CÂMARA MUNICIPAL DE FORTALEZA,** conforme edital do Pregão Eletrônico Nº XXXXXXX que passa a fazer parte desta Ata, juntamente com a(s) proposta(s) de preço(s) apresentada(s) pelo(s) fornecedor(es) classificado(s).

2.2. A Ata de Registro de Preços uma vez lavrada e assinada, não obriga a Administração a firmar as contratações que dela poderão advir, ficando-lhe facultada a utilização de procedimento de licitação, sendo assegurada ao detentor do registro de preços a preferência em igualdade de condições.

3. DA ASSINATURA, FORMALIZAÇÃO, VALIDADE DA ATA DE REGISTRO DE PREÇOS E CADASTRO RESERVA

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

3.1 Este instrumento será assinado pela autoridade competente do órgão gerenciador do registro de preços e pelo representante do fornecedor ou procurador legalmente constituído, na forma do art. 17 do Decreto Municipal nº 15.608, de 31 de março de 2023.

3.2. A publicação da Ata do Registro de Preços será realizada no Portal Nacional de Contratações Públicas – PNCP pelo órgão ou entidade gerenciadora do registro de preço.

3.3. O prazo de vigência da presente Ata é de 1 (um) ano, contado a partir do primeiro dia útil subsequente à data da sua publicação no Portal Nacional de Contratações Públicas – PNCP, podendo ser prorrogada uma vez por igual período, desde que comprovado o preço vantajoso.

3.3. Durante a vigência da Ata de Registro de Preços, poderá ser utilizada por qualquer órgão ou entidade da Administração Pública de Fortaleza, na condição de órgão Interessado, mediante consulta prévia ao Órgão Gestor do Registro de Preços e concordância do fornecedor, conforme disciplina o art. 30 a 32 do Decreto Municipal 15.608, de 31 de março de 2023.

3.4. Será incluído nesta ata, na forma de anexo, o registro do(s) fornecedor(es) que aceitarem cotar bens e serviços com preços iguais ao do(s) licitante(s) vencedor(es) na sequência da classificação do certame e os que mantiverem sua proposta original.

4. DA GERÊNCIA DA ATA DE REGISTRO DE PREÇOS

4.1. Caberá ao (à) Câmara Municipal de Fortaleza o gerenciamento deste instrumento, no seu aspecto operacional e nas questões legais, principalmente quanto às atribuições previstas no art. 7º do Decreto Municipal nº 15.608, de 31 de março de 2023.

5. DOS ÓRGÃOS PARTICIPANTES

SEQ.	ÓRGÃO	ENDEREÇO
01	CÂMARA MUNICIPAL DE FORTALEZA	Rua Dr. Thompson Bulcão, 830 - Engenheiro Luciano Cavalcante, Fortaleza – CE.

5.1. O órgão ou entidade participante da Ata de Registro de Preço deverá observar o art. 8º do Decreto nº 15.608, de 31 de março de 2023;

5.2. Fica vedada a participação do órgão ou entidade em mais de uma ata de registro de preços com o mesmo objeto no prazo de validade daquela de que já tiver participado, salvo na ocorrência de ata que tenha registrado quantitativo inferior ao máximo previsto neste instrumento;

6. DA UTILIZAÇÃO DA ATA DE REGISTRO DE PREÇOS PELOS ÓRGÃOS PARTICIPANTES

6.1. Durante o prazo de validade desta Ata, os órgãos e entidades participantes poderão contratar (firmar contratos) com os fornecedores com preços registrados de acordo com os quantitativos e especificações previstos, devendo comunicar ao órgão gestor, a recusa do detentor de Registro de Preços em fornecer os bens/serviços no prazo estabelecido pelo mesmo.

6.2. A contratação com os fornecedores registrados poderá ser realizada por intermédio de instrumento contratual ou outro instrumento hábil, conforme art. 95 da Lei nº 14.133/2021 e art. 33 do Decreto Municipal nº 15.608/2023.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

6.3. O fornecedor terá o prazo de 5 (cinco) dias, contados a partir da convocação, para a assinatura do Contrato. Este prazo poderá ser prorrogado uma vez por igual período, desde que solicitado durante o seu transcurso e, ainda assim, se devidamente justificado e aceito pela administração.

6.4. Para realização da contratação, os órgãos ou entidades participantes deverão abrir processo numerado e instruído contendo obrigatoriamente: solicitação da compra ou contratação; dotação orçamentária; comprovação de vigência da ata de registro de preços; ordem de compra ou de serviço.

6.5. O contrato decorrente da ata de registro de preços terá sua vigência estabelecida no Termo de Referência do edital ou aviso de contratação, observado o disposto no art. 105 da Lei 14.133, de 1º de abril de 2021. (Art. 35 do Decreto Municipal nº 15.608/2023).

6.6. Os contratos decorrentes do sistema de registro de preços poderão ser alterados, observado o art. 124 da Lei nº 14.133, de 1º de abril de 2021. (art. 34 do Decreto Municipal nº 15.608/2023).

6.7. Na assinatura do Contrato será exigida a comprovação das condições de habilitação exigidas no Edital, as quais deverão ser mantidas pela contratada durante todo o período da contratação.

6.8. As quantidades previstas para os itens com preços registrados poderão ser remanejadas pelo órgão gerenciador entre os órgãos participantes do procedimento licitatório para registro de preços, cabendo ao órgão gerenciador autorizar o remanejamento solicitado, mediante procedimento administrativo, com a redução do quantitativo inicialmente informado pelo órgão participante, desde que haja prévia anuência do órgão que vier a sofrer redução dos quantitativos informados.

6.9. O remanejamento somente poderá ser feito de órgão ou entidade participante para órgão ou entidade participante ou de órgão ou entidade participante para órgão ou entidade não participante devendo, neste último caso, ser observados os limites previstos no art. 31 do Decreto nº 15.608, de 31 de março de 2023.

7. DA ADESÃO À ATA DE REGISTRO DE PREÇOS

7.1. Durante o prazo de validade da ata, qualquer órgão ou entidade da Administração Pública que não tenha participado do certame licitatório poderá aderir à ata de registro de preços na condição de não participante, desde que justificada a vantagem da adesão e demonstrado que os valores registrados estão compatíveis com os valores praticados pelo mercado.

7.2. Os órgãos e entidades da Administração Pública que não participaram do registro de preços, quando desejarem fazer uso da ata de registro de preços, deverão consultar o órgão gerenciador para manifestação sobre a possibilidade de adesão.

7.3. Caberá ao fornecedor beneficiário da ata de registro de preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento decorrente de adesão, desde que não prejudique as obrigações presentes e futuras decorrentes da ata, assumidas com o órgão gerenciador e órgãos participantes.

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

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

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

7.6. Após a autorização do órgão gerenciador, o órgão não participante deverá efetivar a aquisição ou contratação solicitada em até 90 (noventa) dias, observado o prazo de vigência da ata.

7.7. Compete ao órgão não participante os atos relativos à cobrança do cumprimento, pelo fornecedor, das obrigações contratualmente assumidas e à aplicação, observada a ampla defesa e o contraditório, de eventuais penalidades decorrentes do descumprimento de cláusulas contratuais, em relação às suas próprias contratações, informando as ocorrências ao órgão gerenciador.

7.8. O quantitativo reservado para aquisição pelo órgão gerenciador, órgãos participantes e não participantes constam em documento anexo parte integrante desta Ata.

7.9. O órgão ou a entidade poderá aderir a item da ata de registro de preços da qual seja integrante, na qualidade de não participante, para aqueles itens para os quais não tenha quantitativo registrado, observados os requisitos previstos no art. 30 do Decreto Municipal nº 15.608, de 31 de março de 2023.

8. DAS OBRIGAÇÕES E RESPONSABILIDADES

8.1. Os signatários desta Ata de Registro de Preços assumem as obrigações e responsabilidades constantes no Decreto Municipal nº 15.608, de 31 de março de 2023.

8.2. Caberá ao órgão participante, as atribuições que lhe são conferidas nos termos do art. 8º do Decreto Municipal nº 15.608, de 31 de março de 2023.

8.3. O detentor do registro de preços, durante o prazo de validade desta Ata, fica obrigado a:

8.3.1 Atender aos pedidos efetuados pelos órgãos ou entidades participantes do Sistema de Registro de Preços, bem como aqueles decorrentes de remanejamento de quantitativos registrados nesta Ata, durante a sua vigência.

8.3.2. Fornecer os bens ofertados por preço unitário registrado nas quantidades indicadas pelos órgãos ou entidades participantes do Sistema de Registro de Preços e nos prazos a serem definidos no instrumento contratual.

8.3.3. Responder no prazo de até 05 (cinco) dias a consultas do órgão gestor de Registro de Preços sobre a pretensão de órgão/entidade não participante (carona).

8.3.4. Cumprir, quando for o caso, as condições de garantia do objeto, responsabilizando-se pelo período oferecido em sua proposta de preços, observando o prazo mínimo exigido pela Administração.

8.3.5. Providenciar a substituição de qualquer profissional envolvido na execução do objeto contratual, cuja conduta seja considerada indesejável pela fiscalização da contratante.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

9. DOS PREÇOS REGISTRADOS E SUAS REVISÕES

9.1. Os preços registrados na Ata de Registro de Preços serão aqueles ofertados nas propostas de preços da(s) licitante(s) vencedora(s), bem como consta no Anexo 01 desta Ata, listagem com o cadastro de reserva dos licitantes que aceitaram cotar o objeto com preços iguais ao(s) do(s) licitante(s) vencedor(es), na sequência da classificação do certame, conforme permissivo legal do art.16, inciso II do Decreto 15.608, de 31 de março de 2023 ou a informação expressa de que não houve licitante que aceitasse cotar o objeto com preços iguais à da licitante vencedora.

9.2. As quantidades previstas no Anexo I – Termo de Referência do edital são estimativas máximas para o período de validade da Ata de Registro de Preços, reservando-se a Administração Pública, através do órgão ou entidade participante, o direito de adquirir o quantitativo que julgar necessário ou mesmo abster-se de adquirir o item especificado.

9.3. Os preços registrados poderão ser revistos a qualquer tempo em decorrência da redução dos preços praticados no mercado ou de fato que eleve os custos dos itens registrados, obedecendo aos parâmetros constantes nos arts. 24 a 26 do Decreto nº 15.608, de 31 de março de 2023.

9.4. O órgão ou entidade gerenciador convocará o fornecedor para negociar o preço registrado e adequado ao preço de mercado, sempre que verificar que o preço registrado está acima do preço de mercado. Caso seja frustrada a negociação, o fornecedor será liberado do compromisso assumido.

9.5. Havendo a liberação do fornecedor, o órgão gerenciador deverá convocar os demais fornecedores classificados, para verificar se aceitam reduzir seus preços aos valores de mercado, e não havendo êxito nas negociações, deverá proceder ao cancelamento do item ou da Ata de Registro de Preços.

9.6. Caso haja redução do preço registrado, o órgão ou entidade gerenciador deverá comunicar aos órgãos e entidades que tiverem formalizado contrato ou instrumento equivalentes, para que avaliem a conveniência e a oportunidade de diligenciar em negociação com vistas à alteração contratual.

9.7. As alterações dos preços registrados, oriundas de suas revisões, serão divulgadas no Portal Nacional de Contratações Públicas – PNCP e disponibilizadas durante a vigência da ata de registro de preço.

10. DO CANCELAMENTO DO REGISTRO DE PREÇOS

10.1. O detentor de preços registrados terá o seu registro cancelado quando:

10.1.1. Descumprir as condições da Ata de Registro de Preços;

10.1.2. Não retirar a nota de empenho ou o instrumento equivalente no prazo estabelecido pela Administração, sem justificativa aceitável;

10.1.3. Não aceitar reduzir os preços registrados quando estes se tornarem superiores aos de mercado;

10.1.4. For declarado inidôneo ou impedido para licitar e contratar com a Administração Pública;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

10.1.5. A pedido do fornecedor, decorrente de caso fortuito ou força maior, devidamente comprovados e justificados, e por razão de interesse público.

10.2. O cancelamento do registro de preço será formalizado por despacho do órgão ou entidade gerenciadora, assegurado o contraditório e ampla defesa.

11. DOS PRAZOS DE ENTREGA E DO PAGAMENTO

11.1. As condições gerais de execução do objeto desta Ata, tais como recebimento, prazo de entrega, obrigações da Administração e do fornecedor registrado, pagamento e demais condições da contratação encontram-se definidos no Anexo I – Termo de Referência do Edital.

12. DAS SANÇÕES ADMINISTRATIVAS

12.1. A aplicação das penalidades decorrentes do descumprimento do pactuado nesta Ata de Registro de Preço será de competência do órgão gerenciador; nas hipóteses em que o descumprimento ocorrer nas contratações realizados pelos órgãos participantes e não participantes caberá ao respectivo órgão a aplicação da penalidade.

12.2. Comete infração administrativa, nos termos da lei, o fornecedor com preço registrado que praticar ato ilícito na forma do art. 155 da Lei Federal nº 14.133, de 1º de abril de 2021, ou quando deixar de cumprir parcial ou totalmente com as regras dispostas nesta Ata de Registro de Preço.

12.3. Nos processos para apuração e aplicação de sanções previstas no art. 156 da Lei Federal nº 14.133, de 1º de abril de 2021, serão observados os procedimentos previstos no Decreto Municipal nº 15.604, de 28 de março de 2023.

12.4. O fornecedor com preço registrado que praticar ato ilícito na forma do art. 155 da Lei Federal nº 14.133, de 1º de abril de 2021, estará sujeito, garantido o direito prévio ao contraditório e à ampla defesa, sem prejuízo das sanções legais nas esferas civil e criminal, às respectivas penalidades, de acordo com o Decreto Municipal nº 15.604, de 31 de março de 2023.

13. DO FORO

13.1 Fica eleito o foro do Município de Fortaleza do Estado do Ceará, para conhecer das questões relacionadas com a presente Ata que não possam ser resolvidas pelos meios administrativos.

Assinam esta Ata, os signatários relacionados e qualificados a seguir, os quais firmam o compromisso de zelar pelo fiel cumprimento das suas cláusulas e condições.

SIGNATÁRIOS:

ÓRGÃO GERENCIADOR	NOME DO TITULAR	CARGO	ASSINATURA

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

DETENTOR DO REGISTRO DE PREÇOS	NOME DO REPRESENTANTE	E-MAIL	ASSINATURA

ANEXO 01 – DAS LICITANTES QUE ACEITARAM COTAR O MESMO PREÇO DA LICITANTE VENCEDORA

Conforme previsto no art. 16, inciso II, do Decreto 15.608, de 31 de março de 2023 o registro das licitantes que aceitarem cotar os bens ou serviços com preços iguais ao da licitante vencedora, na sequência da classificação do certame é o seguinte:

ITEM	CLASSIFICAÇÃO	RAZÃO SOCIAL / CNPJ	ESPECIFICAÇÃO	QTD.	PREÇO UNITÁRIO	VALOR TOTAL

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

ANEXO VII – MINUTA DO CONTRATO

CONTRATO QUE ENTRE SI CELEBRAM A CÂMARA MUNICIPAL DE FORTALEZA E A(O) CONTRATADA(O) _____, PARA A AQUISIÇÃO DE BENS E SERVIÇOS CONFORME ITENS DEFINIDOS NO PREGÃO ELETRÔNICO ___/2026 (PROCESSO Nº ___/2026)

Processo nº ___/2026.
Pregão Eletrônico nº ___/2026.
Contrato nº ___/2026.

CONTRATANTE: CÂMARA MUNICIPAL DE FORTALEZA, inscrita no CNPJ sob o n.° 06.621.791/0001-53, com sede à Rua Thompson Bulcão, nº 830, bairro Luciano Cavalcante, Fortaleza – CE, CEP.: 60.810-460, neste ato representado pelo seu Diretor-Geral, Sr(a). _____, inscrito no CPF sob o nº ***.XXX.***-XX, domiciliado nesta Capital;

CONTRATADA: _____ (CONTRATADA(O)), inscrita(o) no CNPJ sob o nº XX.XXX.XXX/XXXX-XX, com sede à _____, neste ato representada pelo(a) Sr(a). _____, inscrito(a) no CPF sob o nº ***.XXX.***-XX, domiciliado _____, já qualificado nos autos do processo administrativo acima epigrafado, resolvem firmar o presente Contrato, decorrente do processo de Pregão Eletrônico n° ___/2026, e em conformidade com as disposições contidas na Lei nº 14.133/21, e mediante as Cláusulas e condições a seguir:

CLÁUSULA PRIMEIRA – DA FUNDAMENTAÇÃO LEGAL

1.1. O presente contrato tem como fundamento o Edital do Pregão Eletrônico nº ___/2026, os preceitos do Direito Público, as disposições contidas na Lei Federal nº 14.133, de 1º de abril de 2021, com suas alterações posteriores, nos Decretos Municipais nº 15.595, de 22 de março de 2023, nº 15.604, de 28 de março de 2023; Lei Municipal nº 10.350, de 28 de maio de 2015 na Lei Complementar nº 123, de 14 de dezembro de 2006; na Lei Federal 13.709, de 14 de agosto de 2018 (LGPD - Lei Geral de Proteção de Dados), bem como na Resolução nº 1.684, de 20 de dezembro de 2024, da Câmara Municipal de Fortaleza.

CLÁUSULA SEGUNDA – DO OBJETO

2.1. **CONTRATAÇÃO, POR MEIO DE SISTEMA DE REGISTRO DE PREÇOS, DE EMPRESA ESPECIALIZADA PARA FORNECIMENTO DE SOLUÇÕES TECNOLÓGICAS DE SEGURANÇA, CONECTIVIDADE E REDE WI-FI CORPORATIVA, ABRANGENDO SERVIÇOS TÉCNICOS ESPECIALIZADOS, DESTINADOS À IMPLANTAÇÃO, MODERNIZAÇÃO, OPERAÇÃO E GESTÃO DA INFRAESTRUTURA**

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

DE REDE SEM FIO DA SEDE E DO PRÉDIO ANEXO DA CÂMARA MUNICIPAL DE FORTALEZA, DE ACORDO COM AS ESPECIFICAÇÕES E QUANTITATIVOS PREVISTOS NO TERMO DE REFERÊNCIA.

2.2. A CONTRATADA fica obrigada a aceitar nas mesmas condições contratuais os acréscimos ou supressões no volume do objeto deste contrato, nos termos da Lei Federal nº 14.133/2021.

2.3. Vinculam esta contratação, independentemente de transcrição:

2.3.1. O Termo de Referência;

2.3.2. O Edital de Licitação;

2.3.3. A Proposta do contratado;

2.3.4. Eventuais anexos dos documentos supracitados.

CLÁUSULA TERCEIRA – DA VIGÊNCIA

3.1. O prazo de vigência da contratação é de 12 (doze) meses contados da data da assinatura do contrato, podendo ser prorrogado na forma do art. 107 da Lei 14.133/2021.

3.1.1. A eficácia do contrato fica condicionada à publicação e divulgação integral no PNCP - Portal Nacional de Compras Públicas, nos moldes e prazos estabelecidos nos artigos 91, caput, 94 e 174 da Lei nº 14.133/2021, podendo ainda ser realizada a devida publicação no Diário Oficial do Município de Fortaleza.

CLÁUSULA QUARTA – DO PREÇO

4.1. O valor total da contratação é de R$ _____ (_____).

4.1.1. Para fins de referência, o valor total da contratação é composto de:

ITEM	DESCRIÇÃO	UNIDADE	QTD.	VALOR UNIT.	VALOR TOTAL
1	SOLUÇÃO DE SEGURANÇA DE REDE	FORNECIMENTO	2		
2	SOLUÇÃO DE CONECTIVIDADE DE REDE SEGURA – ACESSO – TIPO 1	FORNECIMENTO	20		
3	SOLUÇÃO DE CONECTIVIDADE DE REDE SEGURA – ACESSO – TIPO 2	FORNECIMENTO	20		
4	SOLUÇÃO DE CONECTIVIDADE DE REDE SEGURA – ACESSO – TIPO 3	FORNECIMENTO	10		
5	SOLUÇÃO DE CONECTIVIDADE DE REDE SEGURA – ACESSO – TIPO 4	FORNECIMENTO	20		
6	SOLUÇÃO DE CONECTIVIDADE DE REDE SEGURA – CORE	FORNECIMENTO	2		
7	SOLUÇÃO DE CONECTIVIDADE DE REDE SEGURA – WI-FI	FORNECIMENTO	100		
8	SOLUÇÃO DE MONITORAMENTO DE REDE	FORNECIMENTO	20		

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

9	SOLUÇÃO DE SEGURANÇA DE ACESSO A REDE	FORNECIMENTO	2		
10	SOLUÇÃO DE SEGURANÇA DAS APLICAÇÕES	FORNECIMENTO	2		
11	SOLUÇÃO DE SEGURANÇA DE E-MAIL	FORNECIMENTO	700		
12	SOLUÇÃO DE SEGURANÇA DOS DISPOSITIVOS DE ACESSO A REDE	FORNECIMENTO	700		
13	SERVIÇO DE INSTALAÇÃO E PARAMETRIZAÇÃO	SERVIÇO	1		
14	SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO	SERVIÇO MENSAL	12		

4.2. 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, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

4.3. O CONTRATANTE se reserva o direito de, a seu juízo, executar ou não a totalidade do valor contratual.

4.4. As quantidades anuais apresentadas na tabela do item 4.1.1. representam apenas estimativas e serão executadas na medida da necessidade e conveniência do CONTRATANTE, sem que caiba qualquer tipo de reclamação ou indenização por parte da contratada.

CLÁUSULA QUINTA – DO PAGAMENTO

5.1. O pagamento será efetuado até 30 (trinta) dias contados da data da apresentação da nota fiscal/fatura devidamente atestada pelo fiscal do contrato, mediante crédito em conta corrente em nome da CONTRATADA.

5.1.1. A nota fiscal/fatura que apresente incorreções será devolvida à contratada para as devidas correções. Nesse caso, o prazo de que trata o subitem anterior começará a fluir a partir da data de apresentação da nota fiscal/fatura corrigida.

5.2. Não será efetuado qualquer pagamento à contratada, em caso de descumprimento das condições de habilitação e qualificação exigidas na licitação.

5.3. É vedada a realização de pagamento antes da execução do objeto ou se o mesmo não estiver de acordo com as especificações deste instrumento.

5.4. Os pagamentos encontram-se ainda condicionados à apresentação dos seguintes comprovantes:
5.4.1. Documentação relativa à regularidade para com a Seguridade Social (INSS), Fundo de Garantia por Tempo de Serviço (FGTS), trabalhista e Fazendas Federal, Estadual e Municipal.

5.5. Toda a documentação exigida deverá ser apresentada em original ou por qualquer processo de reprografia, obrigatoriamente autenticada em cartório ou autenticação digital. Caso esta documentação tenha sido emitida pela Internet, só será aceita após a confirmação de sua autenticidade.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

CLÁUSULA SEXTA – DO REAJUSTE

6.1. Os preços contratuais poderão ser reajustados, após o prazo de 12 (doze) meses, contados da data do orçamento estimado, mediante aplicação do índice de Preços ao Consumidor Amplo – IPCA/IBGE, em conformidade com a legislação em vigor, tomando-se por base o índice vigente no mês de apresentação da proposta a que essa se referir.

6.2. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

6.3. O reajuste poderá ser concedido mediante simples apostila, conforme dispõe o art. 136 da Lei Federal nº 14.133, de 2021.

6.4. Poderá haver revisão de preços na hipótese de ocorrência de fatos imprevisíveis ou previsíveis, porém de consequências incalculáveis durante a gestão contratual, bem como ocorra majoração legal de preços; devendo a Contratada se manifestar e, comprovadamente, demonstrar o desequilíbrio econômico-financeiro do contrato.

CLÁUSULA SÉTIMA – DO REGIME DE EXECUÇÃO DO OBJETO

7.1. Quanto ao local de execução dos Serviços / fornecimento dos equipamentos:

7.1.1. Os serviços contratados, bem como os equipamentos e licenças fornecidos, deverão ser executados / entregues nas dependências da Câmara Municipal de Fortaleza – CMFOR, bem como em seus anexos e áreas complementares, nos seguintes endereços:

7.1.1.1. Sede da Câmara Municipal de Fortaleza, situada na Rua Dr. Thompson Bulcão, nº 830, Bairro Luciano Cavalcante, Fortaleza – CE;

7.1.1.2. Prédio Anexo da Câmara Municipal de Fortaleza, localizado na Avenida Rogaciano Leite, nº 1040, Bairro Guararapes, Fortaleza – CE.

7.1.2. A CONTRATADA deverá assegurar que todos os serviços sejam prestados sem prejuízo das atividades institucionais da Câmara, observando os horários, normas internas de segurança e demais orientações fornecidas pela fiscalização contratual.

7.1.3. O objeto contratual deverá ser executado em conformidade com as especificações estabelecidas neste instrumento, e nas condições previstas do Termo de Referência. Os atrasos ocasionados por motivo de força maior ou caso fortuito, desde que justificados até 02 (dois) dias úteis antes do término do prazo de execução, e aceitos pela contratante, não serão considerados como inadimplemento contratual.

7.1.4. Os serviços deverão ser executados por técnicos/profissionais, capacitados, com formação compatível, bem como deverão apresentar-se devidamente uniformizados e identificados com crachá para o pronto atendimento aos chamados.

7.1.5. Para a execução dos serviços, caberá à Contratada disponibilizar e conservar pelo período contratual, todo ferramental e instrumental adequados.

7.1.6. Os profissionais designados pela Contratada para execução dos serviços deverão apresentar-se no local de trabalho, manter boa aparência e trajar uniforme completo e limpo, com o nome da empresa e crachá de identificação. Como uniforme completo entende-se o conjunto de

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

calça, camisa e calçado com solado de borracha em condições de perfeito isolamento, além de outros Equipamentos de Proteção Individual (E.P.I.), exigidos conforme a natureza da tarefa.

7.2. Quanto à forma de execução, acompanhamento e fiscalização da prestação dos serviços
7.2.1. A execução dos serviços licitados, bem como a entrega dos equipamentos e licenças fornecidos, poderá ser feita de forma fracionada ou em sua totalidade, de acordo com a necessidade da Câmara Municipal de Fortaleza, durante o prazo de contratação, mediante a expedição de periódicas de ORDENS DE SERVIÇO pelo órgão demandante, constando a relação e a quantidade de serviços a serem executados.

7.2.2. A execução dos serviços, bem como a entrega dos equipamentos e licenças fornecidos, será acompanhada e fiscalizada por servidor da Câmara Municipal de Fortaleza, o qual deverá atestar os documentos da despesa, quando comprovada a fiel e correta entrega para fins de pagamento.

7.2.3. A presença da fiscalização do órgão demandante não elide nem diminui a responsabilidade da empresa contratada.

7.2.4. Caberá ao servidor designado rejeitar totalmente ou em parte, qualquer bem que não esteja de acordo com as exigências, bem como, determinar prazo para readequação de serviço eventualmente fora de especificação.

7.3. PRAZO PARA INÍCIO

7.3.1. Os serviços, bem como o fornecimento de licenças, deverão ser iniciados no prazo de até 15 (quinze) dias corridos, a contar da emissão da ORDEM DE SERVIÇO ou do instrumento equivalente.

7.3.2. Os equipamentos, objeto do contrato, deverão ser entregues pela CONTRATADA no prazo máximo de 45 (quarenta e cinco) dias corridos, contados a partir da emissão da ORDEM DE SERVIÇO ou do instrumento equivalente.

7.3.3. A demanda correspondente a ORDEM DE SERVIÇO deverá ser entregue em remessa única.

7.3.4. Caso não seja possível o início da realização dos serviços na data assinalada, a empresa deverá comunicar as razões respectivas com pelo menos 03 (três) dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

7.4. DA FORMA DE EXECUÇÃO DO OBJETO E PAGAMENTO

7.4.1. Os serviços, bem como o fornecimento de equipamentos e licenças, serão executados conforme condições editalícias, será apresentado a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência, e na proposta.

7.4.1.1. Para os bens objeto de fornecimento (Itens 1 a 12): A nota fiscal deverá acompanhar o termo de recebimento provisório e definitivo.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

7.4.1.2. Para os Serviços (Itens 13 e 14): A nota fiscal deverá ser atestada pelo fiscal do contrato mediante medição mensal ou conforme cronograma de execução, verificando-se o cumprimento dos SLAs e metas estabelecidas.

7.4.2. Os serviços, bem como o fornecimento de equipamentos e licenças, poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 02 (dois) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

7.4.3. O prazo para execução dos serviços, bem como o fornecimento de equipamentos e licenças, poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

7.4.4. O prazo para a solução, pelo contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Órgão durante a análise prévia à liquidação de despesa, não será computado para os fins de execução do objeto.

7.4.5. A execução provisória ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

7.4.6. Após a conclusão dos procedimentos quanto a prestação dos serviços, serão realizados os atos correspondentes a liquidação e pagamento da despesa.

7.5. Quanto ao recebimento:

7.5.1. PROVISORIAMENTE, mediante recibo, para efeito de posterior verificação da conformidade do objeto com as especificações, devendo ser feito por pessoa credenciada pela CONTRATANTE.

7.5.2. DEFINITIVAMENTE, sendo expedido Termo de Recebimento Definitivo, após a verificação da qualidade e quantidade do objeto, certificando-se de que todas as condições estabelecidas foram atendidas e a consequente aceitação das Notas Fiscais pelo gestor da contratação, devendo haver rejeição no caso de desconformidade.

7.5.3. Caso o objeto licitado não atenda às especificações exigidas ou apresente defeitos, não será aceito, sujeitando-se o fornecedor à aplicação das penalidades previstas no termo do contrato.

CLÁUSULA OITAVA – DA DOTAÇÃO ORÇAMENTÁRIA

8.1. As despesas decorrentes deste contrato correrão à conta da dotação consignada abaixo:

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.

CLÁUSULA NONA - DA GARANTIA TÉCNICA

9.1. Será exigido do licitante adjudicatário a disponibilidade de suporte técnico para ajustes e melhorias no sistema durante o período de garantia de 36 (trinta e seis) meses, após o recebimento definitivo do objeto contratada, devendo a empresa oferecer suporte técnico para

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

quaisquer ajustes ou necessidades que surjam durante o período de garantia, ainda que após a vigência do presente contrato.

CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DA CONTRATADA

10.1. Prestar os serviços, bem como fornecer os equipamentos e licenças, em conformidade com as condições deste contrato e do Termo de Referência.

10.2. Manter durante toda a execução do objeto, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

10.3. Aceitar, nas mesmas condições contratuais, os percentuais de acréscimos ou supressões limitadas ao estabelecido no art. 125, da Lei Federal nº 14.133/2021, tomando-se por base o valor inicial atualizado do contrato.

10.4. Responsabilizar-se pelos danos causados diretamente à contratante ou a terceiros, decorrentes da sua culpa ou dolo, quando da execução do objeto, não podendo ser arguido para efeito de exclusão ou redução de sua responsabilidade o fato de a contratante proceder à fiscalização ou acompanhar a execução contratual.

10.5. Responder por todas as despesas diretas e indiretas que incidam ou venham a incidir sobre a execução contratual, inclusive as obrigações relativas a salários, previdência social, impostos, encargos sociais e outras providências, respondendo obrigatoriamente pelo fiel cumprimento das leis trabalhistas e específicas de acidentes do trabalho e legislação correlata, aplicáveis ao pessoal empregado na execução contratual.

10.6. Prestar imediatamente as informações e os esclarecimentos que venham a ser solicitados pela contratante, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidas no prazo de 24 (vinte e quatro) horas.

10.7. Reparar, corrigir, remover, reconstruir ou substituir, imediatamente, à suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados, ou em desconformidade com as especificações deste termo.

10.8. Cumprir, quando for o caso, as condições de garantia do objeto, responsabilizando-se pelo período oferecido em sua proposta comercial, observando o prazo mínimo exigido pela Administração.

10.9. Providenciar a substituição de qualquer profissional envolvido na execução do objeto contratual, cuja conduta seja considerada indesejável pela fiscalização da CONTRATANTE.

10.10. É de responsabilidade da CONTRATADA, estar em conformidade com os fundamentos da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), no que tratar-se da manipulação dos dados da CONTRATANTE e de terceiros, em sua criptografia, armazenamento e demais tratativas resguardando os dados utilizados, ficando vedado o tratamento de dados pessoais sensíveis por parte da CONTRATADA com objetivo de obter vantagem econômica de qualquer espécie, com exceção daquelas hipóteses previstas no parágrafo 4º do art. 11 da Lei nº 13.709, de 14 de agosto de 2018.

10.11. Cumprir as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

10.12. Assumir total responsabilidade pelo sigilo das informações, dados, nos termos da Lei Geral de Proteção de Dados - LGPD (Lei nº 13.709/2018), contidos em quaisquer mídias e documentos que seus empregados ou prepostos vierem a obter em função dos serviços prestados à CONTRATANTE, respondendo pelos danos que eventual vazamento de informações, decorrentes de ação danosa ou culposa, nas formas de negligência, imprudência ou imperícia, venha a ocasionar à CONTRATANTE.

10.13. Assumir total responsabilidade pelo sigilo das informações, dados, contidos em quaisquer mídias e documentos que seus empregados ou prepostos vierem a obter em função dos serviços prestados à CONTRATANTE, respondendo pelos danos que eventual vazamento de informações, decorrentes de ação danosa ou culposa, nas formas de negligência, imprudência ou imperícia, venha a ocasionar à CONTRATANTE.

10.14. A Contratada deverá disponibilizar, durante a vigência do contrato, mão de obra capacitada, idônea e experiente, de modo a reunir permanentemente em serviço equipe homogênea e suficiente de técnicos, que possa assegurar a prestação satisfatória dos serviços.

10.15. A Contratada deverá prestar suporte técnico para ajustes, manutenções preventivas, corretivas e melhorias nos sistemas e equipamentos, durante o período de vigência do contrato, assegurando a funcionalidade contínua dos sistemas, não se incluindo evoluções tecnológicas, novas funcionalidades ou melhorias que caracterizem desenvolvimento adicional.

10.16. A Contratada deverá prestar treinamento inicial e operação assistida para os sistemas instalados, com o objetivo de capacitar a equipe interna e promover sua autonomia operacional.

10.17. Entregar o produto/prestar o serviço, onde o mesmo deverá obedecer às exigências contidas nas especificações do Termo de Referência, bem como todas e quaisquer normas ou regulamentações intrínsecas ao tipo de fornecimento.

10.18. É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

10.19. Serão de responsabilidade exclusiva da empresa contratada os custos com transporte e alimentação de seus funcionários.

10.20. Assumir inteira responsabilidade por qualquer extravio causado durante o transporte e demais serviços pertinentes ao fornecimento, devendo comunicar ao fiscal do Contrato, tempestivamente, a fim de que sejam adotadas as providências.

10.21. Não transferir a outrem, no todo ou em parte, a execução do objeto, sob pena de responsabilidade.

10.22. Manter, durante todo o período de vigência Contrato a ser firmado, um preposto aceito pela Contratante, para representação da Contratada sempre que for necessário e comunicando, por escrito, à Contratante qualquer mudança de endereço ou telefone de contato.

10.23. Acatar as orientações da Contratante, sujeitando-se à mais ampla e irrestrita fiscalização, prestando os esclarecimentos solicitados e atendendo às reclamações formuladas.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

10.24. Cumprir todas normas e regulamentos alusivos à segurança na realização dos serviços, bem como aquelas inerentes à preservação patrimonial.

10.25. Sem prejuízo das demais determinações e especificações contidas no Termo de Referência (que vincula a presente contratação), a CONTRATADA será responsável pela administração e manutenção do serviço em regime de 24x7x365 (vinte e quatro horas, sete dias por semana, trezentos e sessenta e cinco dias por ano) para atendimentos remotos e o regime 8x5 para atendimentos que possam ser necessários na forma presencial, durante todo o período do serviço contemplado nesse termo.

10.26. As tarefas atinentes ao transporte, deslocamento e remessa necessários, seja na implementação, substituição e/ ou remoção de equipamentos defeituosos será de responsabilidade da CONTRATADA.

10.27. Para garantir a qualidade e disponibilidade do serviço, deverá ser disponibilizado pela empresa CONTRATADA uma ferramenta de visibilidade e monitoramento com estrutura dedicada para a CONTRATANTE. A ferramenta deve ser acompanhada de todos os itens necessários para operacionalização, tais como: softwares de apoio (sistema operacional, etc) e licenças de softwares.

10.28. O serviço de monitoramento 24x7 deverá ser prestado OBRIGATÓRIA E INDISPENSAVELMENTE através de NOCs (Network Operation Center) redundantes da empresa CONTRATADA que já deverão estar em pleno funcionamento até a data da assinatura do contrato. Será o ponto único de contato com a equipe técnica da CONTRATANTE para abertura de chamados, incidentes, problemas, dúvidas e requisições relacionadas aos serviços contratados, atuando como a primeira instância de atendimento à CONTRATANTE.

CLÁUSULA DÉCIMA PRIMEIRA – DAS OBRIGAÇÕES DA CONTRATANTE

11.1. Solicitar a execução do objeto à CONTRATADA através da emissão de Ordem de Serviço, nota de empenho ou documento equivalente.

11.2. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, em conformidade com o Edital e seus anexos.

11.3. Receber o objeto no prazo e condições estabelecidas no Termo de Referência.

11.4. Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas.

11.5. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado.

11.6. Comunicar a empresa para emissão de Nota Fiscal em relação à incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021.

11.7. Efetuar o pagamento ao Contratado do valor correspondente a execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

11.8. Aplicar ao Contratado as sanções previstas na Lei nº 14.133, de 2021 e neste Contrato.

11.9. Cientificar os órgãos responsáveis para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado.

11.10. Emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

11.11. Responder eventuais pedidos de restabelecimento do equilíbrio econômico-financeiro feitos.

11.13. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

11.14. A Administração não responderá por quaisquer compromissos assumidos pelo Contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do Contratado, de seus empregados, prepostos ou subordinados.

11.15. A Contratante se compromete a zelar pelo tratamento dos dados pessoais dos titulares, pessoas naturais vinculadas à Contratada, sem prejuízo de qualquer responsabilidade, admitindo-se o tratamento nas hipóteses de consentimento específico e destacado por termo de compromisso e ou nas hipóteses previstas nos incisos II a X do art. 7º da Lei Federal nº 13709, de 14 de agosto de 2018, quando for o caso.

11.16. Fica vedado o tratamento de dados pessoais sensíveis por parte do CONTRATANTE com objetivo de obter vantagem econômica de qualquer espécie, com exceção daquelas hipóteses previstas no parágrafo 4º do art. 11 da Lei Federal nº 13.709, de 14 de agosto de 2018, quando for o caso.

11.17. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, em conformidade com o Edital e seus anexos.

11.18. Receber o objeto no prazo e condições estabelecidas no Termo de Referência.

11.19. Comunicar a empresa para emissão de Nota Fiscal em relação à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021.

CLÁUSULA DÉCIMA SEGUNDA – DA FISCALIZAÇÃO

12.1. A execução do objeto da presente contratação deverá ser acompanhada e fiscalizada por servidor ou equipe de fiscalização, especialmente designada para esse fim, conforme o disposto no art. 117 da Lei 14.133/2021, nos termos descritos e detalhados do Termo de Referência anexo.

CLÁUSULA DÉCIMA TERCEIRA - DA SUBCONTRATAÇÃO

13.1. Será admitida a subcontratação parcial do objeto, nos termos do art. 122 da Lei nº 14.133/2021, desde que previamente autorizada pela CONTRATANTE.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

13.1.2 A subcontratação não poderá abranger a totalidade do objeto, nem as parcelas de maior relevância técnica e econômica, assim consideradas aquelas relacionadas ao fornecimento dos equipamentos principais e à responsabilidade técnica pela solução.

13.1.3 A CONTRATADA permanecerá integralmente responsável pela execução do contrato, inclusive quanto às obrigações assumidas por eventuais subcontratadas.

13.1.4 A subcontratação dependerá de autorização formal da fiscalização contratual, mediante apresentação da qualificação técnica da subcontratada compatível com a parcela a ser executada.

13.1.5 É vedada a subcontratação para mera intermediação de mão de obra ou transferência integral da execução contratual.

CLÁUSULA DÉCIMA QUARTA – DAS INFRAÇÕES E DAS SANÇÕES ADMINISTRATIVAS

14.1. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o contratado que, com dolo ou culpa:

a) der causa à inexecução parcial do contrato;
b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
c) der causa à inexecução total do contrato;
d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
f) praticar ato fraudulento na execução do contrato;
g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

14.2. Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

a) Advertência, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);

b) Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);

c) Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).

d) Multa:

d.1) A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor do contrato licitado, recolhida no prazo máximo de 5 (cinco) dias úteis, a contar da comunicação oficial.

e) A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, §9º, da Lei nº 14.133, de 2021).

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

14.3.1. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).

14.3.2. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133, de 2021).

14.3.3. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia eventual prestada ou será cobrada judicialmente (art. 156, §8º, da Lei nº 14.133, de 2021).

14.3.4. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

14.4. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

14.5. Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133, de 2021):

I. a natureza e a gravidade da infração cometida;
II. as peculiaridades do caso concreto;
III. as circunstâncias agravantes ou atenuantes;
IV. os danos que dela provierem para o Contratante;
V. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

14.6. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159).

14.7. A personalidade jurídica da contratada poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160, da Lei nº 14.133, de 2021).

14.8. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.

14.9. Os débitos da contratada para com a Administração contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o contratado possua com o mesmo órgão ora contratante.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

14.10. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos termos do §4º do art. 156 da Lei nº 14.133, de 1º de abril de 2021 e do art. 15 do Decreto Municipal nº 15.604, de 28 de março de 2023, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

14.11. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos termos do § 5º do art. 156 da Lei nº 14.133, de 1º de abril de 2021, e do art. 16 do Decreto Municipal nº 15.604, de 28 de março de 2023, que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos.

14.12. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, caracteriza o descumprimento total da obrigação assumida e o sujeitará às penalidades e à decadência do direito à garantia de proposta em favor do órgão ou entidade promotora da licitação, nos termos do art. 18 do Decreto Municipal nº 15.604, de 28 de março de 2023.

14.13. O pagamento das multas não eximirá a contratada de ser acionada judicialmente pela responsabilidade civil derivada de perdas e danos junto à contratante, decorrentes das infrações porventura cometidas, inclusive pela inobservância do disposto na Lei 13.709/2018 (LGPD), na forma abaixo estipuladas:

14.13.1. Multa de 20% (vinte por cento) sobre o valor total do CONTRATO, na hipótese de tratamento de dados pessoais sensíveis com o objetivo de obter vantagem econômica, ou outra irregularidade havida no cumprimento do CONTRATO, por culpa da CONTRATADA.

14.13.2. Multa de 10% (dez por cento) sobre o valor total do CONTRATO, na hipótese de descumprimento da obrigação de zelo no tratamento dos dados pessoais da pessoa natural vinculada à CONTRATANTE, ou em caso de tratamento de dados sem o consentimento específico e destacado por termo de compromisso, ou outra irregularidade havida no cumprimento do CONTRATO, por culpa da CONTRATADA.

14.14. O Contratante deverá, no prazo máximo 05 (CINCO) DIAS úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e no Cadastro Nacional de Empresas Punidas (CNEP). (Art. 161, da Lei nº 14.133, de 2021).

CLÁUSULA DÉCIMA QUINTA – DA EXTINÇÃO CONTRATUAL

15.1. O contrato se extingue quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes.

15.1.1. O contrato poderá ser extinto antes do prazo nele fixado, sem ônus para o Contratante, quando este não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

15.1.2. A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação do contratado pelo contratante nesse sentido com pelo menos 02 (dois) meses de antecedência desse dia.

15.2. O contrato pode ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 (da Lei nº 14.133/21), bem como amigavelmente, assegurados o contraditório e a ampla defesa.

15.2.1. Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

15.2.2. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a rescisão se não restringir sua capacidade de concluir o contrato.

15.2.2.1. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

15.3. O termo de rescisão, sempre que possível, será precedido:

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

15.3.2. Relação dos pagamentos já efetuados e ainda devidos;

15.3.3. Indenizações e multas.

15.4. 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.

15.5. Poderá ocorrer a extinção do contrato caso se constate que o contratado mantém vínculo com dirigente ou entidade contratante ou com agente público que desempenhe função na licitação ou na fiscalização do contrato, nos termos do art. 14, IV, da NLL.

CLÁUSULA DÉCIMA SEXTA – DOS CASOS OMISSOS

16.1. Os casos omissos serão decididos pelo contratante, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais e municipais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

CLÁUSULA DÉCIMA SÉTIMA – DA PUBLICAÇÃO

17.1. A eficácia do contrato fica condicionada à publicação e divulgação integral no PNCP - Portal Nacional de Compras Públicas, nos moldes e prazos estabelecidos nos artigos 91, caput, 94 e 174 da Lei nº 14.133/2021, podendo ainda ser realizada a devida publicação no Diário Oficial do Município – DOM.

CLÁUSULA DÉCIMA OITAVA – DAS ALTERAÇÕES DO CONTRATO

18.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos art. 124 e seguintes da Lei nº 14.133, de 2021.

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

18.2. O contratado é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

18.3. Qualquer alteração contratual deverá ser realizada mediante termo aditivo ao presente contrato, inclusive com instrução, pareceres, avaliação do impacto orçamentário e decisão motivada, excetuando-se as hipóteses previstas no art. 132 da Lei nº 14.133/2021.

CLÁUSULA DÉCIMA NONA – DAS DISPOSIÇÕES FINAIS

19.1. A CONTRATANTE analisará, julgará e decidirá, em cada caso, as questões alusivas a incidentes que se fundamentem em motivos de caso fortuito, de força maior ou omissos.

19.1.1. Para os casos previstos no “caput” desta cláusula, a CONTRATANTE poderá atribuir a uma comissão, por este designada por portaria, a responsabilidade de apurar os atos e fatos comissivos ou omissivos que se fundamentem naqueles motivos.

19.1.2. As exceções aqui referenciadas serão sempre tratadas com máxima cautela, zelo profissional, senso de responsabilidade e ponderação, para que ato de mera e excepcional concessão da CONTRATANTE, cujo objetivo final é o de atender tão-somente ao interesse público, não seja interpretado como regra contratual.

19.1.3. Para assegurar rápida solução às questões geradas em face da perfeita execução do presente contrato, fica desde já compelida a CONTRATADA a avisar, por escrito e de imediato, qualquer alteração no endereço ou no telefone da empresa.

19.1.4. Quaisquer tolerâncias entre as partes não importarão em novação de qualquer uma das cláusulas ou condições estatuídas neste contrato, as quais permanecerão íntegras.

CLÁUSULA VIGÉSIMA – DA FRAUDE E DA CORRUPÇÃO

20.1. A contratada deve observar e fazer observar, por seus fornecedores e subcontratados, se admitida subcontratação, o mais alto padrão de ética durante todo o processo de licitação, de contratação e de execução do objeto contratual.

20.2. Para os propósitos desta cláusula, definem-se as seguintes práticas:

20.2.1. “prática corrupta”: oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer vantagem com o objetivo de influenciar a ação de servidor público no processo de licitação ou na execução de contrato;

20.2.2. “prática fraudulenta”: a falsificação ou omissão dos fatos, com o objetivo de influenciar o processo de licitação ou de execução de contrato;

20.2.3. “prática colusiva”: esquematizar ou estabelecer um acordo entre duas ou mais licitantes, com ou sem o conhecimento de representantes ou prepostos do órgão licitador, visando estabelecer preços em níveis artificiais e não-competitivos;

20.2.4. “prática coercitiva”: causar dano ou ameaçar causar dano, direta ou indiretamente, às pessoas ou sua propriedade, visando influenciar sua participação em um processo licitatório ou afetar a execução do contrato;

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

20.2.5. “prática obstrutiva”: (i) destruir, falsificar, alterar ou ocultar provas em inspeções ou fazer declarações falsas aos representantes do organismo financeiro multilateral, com o objetivo de impedir materialmente a apuração de alegações de prática prevista, deste Edital; (ii) atos cuja intenção seja impedir materialmente o exercício do direito de o organismo financeiro multilateral promover inspeção.

20.3. Na hipótese de financiamento, parcial ou integral, por organismo financeiro multilateral, mediante adiantamento ou reembolso, este organismo imporá sanção sobre uma empresa ou pessoa física, inclusive declarando-a inelegível, indefinidamente ou por prazo determinado, para a outorga de contratos financiados pelo organismo se, em qualquer momento, constatar o envolvimento da empresa, diretamente ou por meio de um agente, em práticas corruptas, fraudulentas, colusivas, coercitivas ou obstrutivas ao participar da licitação ou da execução um contrato financiado pelo organismo.

20.4. Considerando os propósitos das cláusulas acima, a licitante vencedora, como condição para a contratação, deverá concordar e autorizar que, na hipótese de o contrato vir a ser financiado, em parte ou integralmente, por organismo financeiro multilateral, mediante adiantamento ou reembolso, permitirá que o organismo financeiro e/ou pessoas por ele formalmente indicadas possam inspecionar o local de execução do contrato e todos os documentos, contas e registros relacionados à licitação e à execução do contrato.

CLÁUSULA VIGÉSIMA PRIMEIRA – DO FORO

21.1. Fica eleito o Foro do município de Fortaleza no Estado do Ceará para dirimir quaisquer questões decorrentes da execução deste contrato, que não puderem ser resolvidas na esfera administrativa.

E, por estarem de acordo, foi mandado lavrar o presente contrato, que está visado pela Assessoria Jurídica da CONTRATANTE, e do qual se extraíram 02 (duas) vias de igual teor e forma, para um só efeito, as quais, depois de lidas e achadas conforme, vão assinadas pelos representantes das partes e pelas testemunhas abaixo.

Fortaleza, _____ de _____ de ____.

CONTRATANTE

CONTRATADA:

TESTEMUNHAS:

1. _____ 2. _____

Assinado por EMANUEL ANGELO PINHEIRO DO VALE em 20/03/2026 11:41
Para acessar o documento assinado digitalmente, clique na URL abaixo:
https://cmfor360.fortaleza.ce.leg.br/documento/17740167371 44_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

Assinaturas Digitais

Documento registrado em 20 de março de 2026 às 11:25

Para conferir o documento assinado digitalmente, acesse o endereço eletrônico abaixo:

https://cmfor360.fortaleza.ce.leg.br/documento/1774016737144_f006a0b3-c8e9-42e9-b2f3-6d18b82dabf9

Documento assinado por

EMANUEL ANGELO PINHEIRO DO VALE