# PROCESSO ADMINISTRATIVO Nº 225/2025

# CONCORRÊNCIA ELETRÔNICA Nº 005/2025

**OBJETO: CONTRATAÇÃO DE EMPRESA PARA PRESTAÇÃO DE SERVIÇO ESPECIALIZADO EM TECNOLOGIA DA INFORMAÇÃO E SEGURANÇA DA INFORMAÇÃO, INCLUINDO SUPORTE TÉCNICO EM MÚLTIPLOS NÍVEIS (N1, N2 E N3), IMPLANTAÇÃO E OPERAÇÃO DE SOLUÇÕES DE SEGURANÇA (BACKUP, ANTIVÍRUS, SIEM, RMM, ITSM, ENTRE OUTRAS), APOIO À RESPOSTA A INCIDENTES, E ESTRUTURAÇÃO DE POLÍTICAS E NORMAS DE SEGURANÇA, VISANDO GARANTIR A CONTINUIDADE DOS SERVIÇOS PÚBLICOS, A ESTABILIDADE DA INFRAESTRUTURA DE TI DO MUNICÍPIO DE MORRO DO CHAPÉU/BA**

**EDITAL**
**CONCORRÊNCIA ELETRÔNICA Nº 005/2025**

O **MUNICÍPIO DE MORRO DO CHAPÉU** – Estado da Bahia, pessoa jurídica de direito público, inscrito no CNPJ nº 13.717.517/0001-48, através da Comissão de Contratação, designada através do Decreto nº 112/2025, torna público, para conhecimento das empresas interessadas que será realizada licitação, na modalidade **CONCORRÊNCIA ELETRÔNICA**, do tipo "**TECNICA E PREÇO**", sob o regime de execução por empreitada por preço global, regido pela Lei Federal nº 14.133, de 1º de abril de 2021, regidos pelos Decretos Municipais nº 314/2023, 316/2023, 317/2023, 318/2023 e 320/2023, Lei Complementar n.º 123/2006, além das demais disposições legais aplicáveis, e pelas condições estabelecidas no presente Edital e seus anexos. O certame será realizado em sessão pública *on line* por meio de recursos de tecnologia da informação – *internet,* através do site – **BNC – BOLSA NACIONAL DE COMPRAS – www.bnc.org.br.**

**RECEBIMENTO E ABERTURA DAS PROPOSTAS:**

**Início de acolhimento das propostas:**..... dia 11/11/2025, às 08h00min.
**Abertura das propostas:** ..... dia 12/01/2026, às 08h00min.

**"Caso as datas previstas para realização de eventos sejam declaradas feriado ou ponto facultativo, e não havendo retificação da convocação, aqueles eventos deverão ser realizados no primeiro dia útil subsequente, no mesmo local e hora anteriormente estabelecidos, independentemente de qualquer comunicação aos interessados;**

**Modo De Disputa:** Será adotada a disputa modo **"FECHADO"**, conforme os critérios definidos no art. 56, inciso II da Lei Federal n.º 14.133/2021.

**Consultas:** Observando o prazo legal, interessados poderão formular consultas por e-mail, informando o número da licitação, por meio do endereço: licitacao@morrodochapeu.ba.gov.br. Tel. nº (74) 3653-1054.

**Referência de tempo:** Para todas as referências de tempo será considerado o horário de Brasília - DF, e para efeitos de contagem de prazo será considerada hora útil o intervalo entre as 08h às 18h, sem interrupções.

**Cópia deste Edital, seus anexos e eventuais alterações** estarão, a partir da data da publicação de seu resumo em Diário Oficial, à disposição no site do BNC – BOLSA NACIONAL DE COMPRAS (www.bnc.org.br), bem como no site do Município por meio do link: http://doem.org.br/ba/morrodochapeu/editais, para todos os interessados.

**Outras informações** sobre a licitação serão prestadas pela Comissão de Contratação da Prefeitura de MORRO DO CHAPÉU, situado na Rua Coronel Dias Coelho, nº 188, Centro – MORRO DO CHAPÉU - BA - CEP: 44.850-000.

**1. DO OBJETO**

**1.1. CONTRATAÇÃO DE EMPRESA PARA PRESTAÇÃO DE SERVIÇO ESPECIALIZADO EM TECNOLOGIA DA INFORMAÇÃO E SEGURANÇA DA INFORMAÇÃO, INCLUINDO SUPORTE TÉCNICO EM MÚLTIPLOS NÍVEIS (N1, N2 E N3), IMPLANTAÇÃO E OPERAÇÃO DE SOLUÇÕES DE SEGURANÇA (BACKUP, ANTIVÍRUS, SIEM, RMM, ITSM, ENTRE OUTRAS), APOIO À RESPOSTA A INCIDENTES, E ESTRUTURAÇÃO DE POLÍTICAS E NORMAS DE SEGURANÇA, VISANDO GARANTIR A CONTINUIDADE DOS SERVIÇOS PÚBLICOS, A ESTABILIDADE DA INFRAESTRUTURA DE TI DO MUNICÍPIO DE MORRO DO CHAPÉU/BA.**

**2. CONDIÇÕES DE PARTICIPAÇÃO**

2.1. Poderão participar desta licitação os interessados que atendam a todas as exigências constantes neste Edital e seus anexos.

**2.2. Estarão impedidos de participar da presente licitação:**

2.2.1. Os interessados suspensos do direito de licitar com a Administração Municipal de Morro do Chapéu-Bahia, cujo conceito abrange a administração direta e indireta, as entidades com personalidade jurídica de direito privado sob o seu controle e as fundações por ela instituída ou mantida, no prazo e nas condições do impedimento;
2.2.2. Os interessados que tenham sido declarados inidôneos pela Administração Municipal, Estadual ou Federal, o que abrange a administração direta e indireta, as entidades com personalidade jurídica de direito privado sob o seu controle e as fundações por ela instituída e mantida, enquanto perdurarem os motivos determinantes da punição ou até que seja reabilitado perante a autoridade que aplicou a penalidade;
2.2.3. Que estejam sujeitos a processo de recuperação judicial ou extrajudicial, concordata, falência, dissolução, fusão, incorporação, cisão e liquidação;
2.2.4. Empresas em forma de consórcio ou coligação.
2.2.5. Servidores de órgãos e entidades da Administração Pública Estadual, inclusive Fundações instituídas e/ou mantidas pelo Poder Público, por si ou por interposta pessoa, direta ou indiretamente, como licitante neste processo licitatório.
2.2.6. Estrangeiros que não estejam autorizados a comercializar no País.
2.2.7. Empresa isoladamente responsável pela elaboração do projeto básico ou executivo ou da qual o autor do projeto seja dirigente, gerente, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto ou controlador, responsável técnico ou subcontratado.
2.2.8. Não será aceito o mesmo representante para empresas diversas.
2.2.9. É vedada a participação de cooperativas (art. 5 da Lei n.º 12.690, de 19 de julho de 2012 e Acórdão 2221/2013 Plenário TC 029.289/2009-0, Relator Ministro Jose Múcio Monteiro, 21.8.2013) nesta licitação, pois, pela natureza do serviço há necessidade de subordinação jurídica entre o obreiro e o contratado, bem como de pessoalidade e habitualidade.
2.2.10. Organizações da Sociedade Civil de Interesse Público - OSCIP, conforme Acórdão nº 746/2014-TCU - Plenário.
2.2.11. Instituições sem fins lucrativos, conforme Acórdão nº 2847/2019 - TCU - Plenário.
2.2.12. Pessoas que possuam vínculo familiar com agente político da Prefeitura Municipal de Morro do Chapéu.
2.2.12.1. Será considerado familiar o cônjuge, o companheiro ou o parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau.
2.2.13. Empresas cujos empregados, diretores, responsáveis técnicos ou sócios figurem como funcionários, empregados ou ocupantes de função gratificada na Prefeitura Municipal de Morro do Chapéu.

**3. DO CREDENCIAMENTO NO SISTEMA E EFETIVA PARTICIPAÇÃO**

3.1. Para acesso ao sistema eletrônico, os interessados em participar da Concorrência Eletrônica deverão dispor de chave de identificação e senha pessoal e intransferível, obtida junto ao BNC – BOLSA NACIONAL DE COMPRAS.
3.2. O credenciamento se dará por intermédio da atribuição de chave de identificação e/ou senha individual.
3.3. O credenciamento será pessoal e intransferível para acesso ao sistema. O usuário credenciado será responsável por todos os atos praticados nos limites de suas atribuições e competências.
3.4. O credenciamento implica em responsabilidade legal do usuário e na presunção de sua capacidade técnica para realização das transações inerentes à Concorrência.
3.5. É de exclusiva responsabilidade do usuário o sigilo da senha, bem como seu uso em qualquer transação efetuada diretamente ou por seu representante, não cabendo ao BNC – BOLSA NACIONAL DE COMPRAS, ao provedor do sistema ou ao órgão promotor da licitação responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.
3.6. O credenciamento do prestador dos serviços de seu representante legal junto ao sistema eletrônico implica a responsabilidade legal pelos atos praticados e a presunção de capacidade técnica para realização das transações inerentes a Concorrência Eletrônica.
3.7. A participação na Concorrência Eletrônica se dará por meio da digitação da senha pessoal e intransferível do representante credenciado e subsequente encaminhamento da proposta de preços, exclusivamente por meio do sistema eletrônico, observados data e horário limite estabelecidos.
3.8. O encaminhamento de proposta pressupõe o pleno conhecimento e atendimento às exigências de habilitação previstas no Edital. O fornecedor será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances.
3.9. Caberá ao prestador de serviços acompanhar as operações no sistema eletrônico durante a sessão pública da Concorrência, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

3.10. Como condição para participação na Concorrência, a licitante assinalará "sim" ou "não" em campo próprio do sistema eletrônico, relativo às seguintes declarações:

1) Declaração que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apta a usufruir do tratamento diferenciado estabelecido em seus arts. 42 a 49 com as alterações promovidas pela Lei Complementar 147/2014.

2) A assinalação do campo "não", apenas produzirá o efeito de a licitante não ter direito ao tratamento diferenciado previsto na Lei Complementar nº 123/2006, com as alterações promovidas pela Lei Complementar 147/2014 mesmo que seja qualificada como microempresa ou empresa de pequeno porte.

**4. DO RECEBIMENTO DAS PROPOSTAS E DOCUMENTOS DE HABILITAÇÃO**

4.1. As propostas técnicas e de preço deverão ser enviadas, **concomitantemente**, com os documentos de habilitação jurídica previstos no item 7 deste edital, até o fim da data e horário de recebimento de propostas, previsto no preâmbulo deste Edital, exclusivamente por meio do sistema eletrônico, mediante a opção "acesso identificado", por meio da digitação da senha de identificação do licitante.

4.1.1. A **não inclusão das propostas técnica e de preço, e dos documentos de habilitação jurídica** nos termos deste instrumento convocatório é motivo para imediata desclassificação da proponente.

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

4.3. O licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances.

4.4. Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública da Concorrência, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

4.5. Até a abertura da proposta de preços, os licitantes poderão retirar ou substituir as propostas de técnica e as propostas de preço apresentadas até o horário limite para recebimento.

4.6. O licitante deverá, nesta etapa, clicar na opção "oferecer proposta" e preencher o formulário eletrônico apresentado na tela, com os dados pertinentes à sua proposta de preços, vedada a identificação da proponente ou do seu representante legal, sob pena de desclassificação.

4.7. No preenchimento da proposta eletrônica o licitante deverá, obrigatoriamente, mencionar, no campo "informações adicionais", os serviços ofertados e anexar sua proposta de preços inicial acompanhada das planilhas de composição de custos e formação de preços dos postos de serviços, vedada a identificação da empresa, sob pena de desclassificação.

4.8. O Agente de Contratação verificará as propostas apresentadas, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, contenham vícios insanáveis ou não apresentem as especificações técnicas exigidas no Termo de Referência:

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

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

4.9. O não preenchimento do campo referido no item anterior, implicará na desclassificação licitante, face a ausência de informação suficiente para classificação da proposta.

4.10. Todas as especificações do objeto contidas na proposta vinculam o fornecedor registrado.

4.11. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente no fornecimento dos bens.

4.12. A apresentação da proposta eletrônica implica plena aceitação, por parte do licitante, das condições estabelecidas neste Edital e seus Anexos.

4.13. A partir do horário previsto no PREÂMBULO para início da sessão pública da Concorrência Eletrônica, terá lugar a divulgação das propostas técnicas e propostas de preços recebidas e em perfeita consonância com as especificações e condições estabelecidas no edital.

4.14. A licitante deverá apresentar declaração expressa indicando seu regime tributário bem como seu enquadramento.

4.15. Serão consideradas irregulares e desclassificadas, de logo, as propostas que não contiverem informação que permita a perfeita identificação e/ou qualificação do objeto proposto; contiverem emenda, rasura ou entrelinha, de forma a não permitir a sua compreensão; apresentarem o prazo de validade da proposta inferior ao estabelecido,

apresentarem prazo de entrega ou de execução superior ao estabelecido. A não apresentação das exigências acima, junto com a proposta de preços, acarretará na desclassificação desta.

4.16. Iniciada a sessão pública da Concorrência Eletrônica, não cabe desistência da proposta.

4.17. Sempre que houver interrupção da sessão da Concorrência, os licitantes deverão ser notificados do dia e hora em que a sessão terá continuidade.

**5. DO PREENCHIMENTO DAS PROPOSTAS**

5.1. O licitante deverá enviar sua proposta técnica, através do sistema eletrônico, contendo os requisitos previstos no item 12 do Termo de Referência, anexo a este edital.

5.1.1 Os documentos complementares à proposta de técnica, quando necessários à confirmação daqueles exigidos no edital de licitação e já apresentados, serão encaminhados pelo licitante mais bem classificado, após o encerramento da etapa competitiva.

5.2. A proposta comercial deverá ser apresentada conforme modelo constante no Anexo I, em uma via, com identificação da empresa proponente, número do CNPJ, endereço, telefones de contato, e-mail, e assinatura do seu representante legal ou procurador, devidamente identificado e qualificado, redigida em português de forma clara, não podendo ser manuscrita e nem conter rasuras ou entrelinhas e incluirá:

a) Descrição do objeto, com a individualização dos itens, em conformidade com as especificações constantes no Anexo I deste Edital;

b) Indicação dos valores unitários e totais do objeto da licitação, em algarismos e por extenso, fixo, expresso em moeda corrente nacional com, no máximo, duas casas decimais, já computados todos os custos relacionados às despesas de pessoal, insumos, tributos, encargos trabalhistas, previdenciários e quaisquer outros relacionados ao objeto desta licitação. Em caso de divergência entre os valores unitários e globais, serão considerados os primeiros, bem como entre os expressos em algarismos numéricos e escritos divergentes, vigorará o valor por extenso;

c) Na formulação da proposta de preços o concorrente deverá computar todas as despesas e custos relacionados com o objeto licitado, tributos de qualquer natureza e todas as despesas diretas ou indiretas, relacionados com a execução do objeto da presente licitação, ficando esclarecido que a Prefeitura não admitirá qualquer alegação posterior que vise o ressarcimento de custos não considerados nos preços, ressalvados as hipóteses de criação ou majoração dos impostos ou encargos sociais;

d) Declaração de que nos preços propostos estão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente no fornecimento dos produtos, conforme anexo deste Edital, ficando esclarecido que o Município não admitirá qualquer alegação posterior que vise o ressarcimento de custos não considerados nos preços, ressalvadas as hipóteses de criação ou majoração dos impostos ou encargos sociais;

e) indicação do Banco, agência e Conta Corrente para depósito bancário;

f) O Prazo mínimo de validade da proposta, que deve ser de 60 (sessenta) dias, a contar da data da sessão da Concorrência.

g) Em circunstâncias excepcionais, antes do término do período original de validade das propostas, o Agente de Contratação poderá solicitar que os licitantes estendam o período de validade das propostas para um período específico adicional. Essa solicitação, bem como as respostas dos licitantes, será feita por escrito via correio eletrônico.

5.3. **Serão desclassificadas as propostas que consignem preços manifestamente inexequíveis, assim considerados aqueles que não venham a ter demonstrada sua viabilidade através de documentação que comprove que os custos dos insumos são coerentes com os de mercado e que os coeficientes de produtividade são compatíveis com a execução do objeto do contrato.**

5.4. A inexequibilidade dos valores referentes a itens isolados da planilha de custos, desde que não contrariem instrumentos legais, não caracterizam motivo suficiente para a desclassificação da proposta.

5.5. Se houver indícios de inexequibilidade da proposta de preços, ou em caso da necessidade de esclarecimentos complementares, poderá ser efetuada diligência, na forma do § 2º do Artigo 59 da Lei nº. 14.133/21 e do artigo 43 do Decreto Municipal 320/2024, para efeito de comprovação de sua exequibilidade.

5.6. Após a apresentação da proposta não caberá desistência.

5.7. Em caso de algum(ns) item(ns) ser(em) apresentado(s) em mais de um item ou lote, o(s) mesmo(s) deverá(ão) apresentar o mesmo valor unitário, sob pena de desclassificação do(s) lote(s) divergente(s).

5.8. A Contratada deverá arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo

complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da licitação,

**5.9. SERÃO DESCLASSIFICADAS AS PROPOSTAS QUE:**

a) Sejam incompletas, isto é, não contenham informações suficientes que permitam a perfeita identificação do objeto licitado.

b) Contiverem qualquer limitação ou condição substancialmente contrastante com o presente Edital, ou seja, manifestamente inexequíveis, por decisão do Agente de Contratação, nos termos do item 5 deste Edital.

c) Que conflitem com as normas deste Edital ou da legislação em vigor.

d) Que apresente qualquer elemento que possa identificar a licitante na proposta inicial (antes da disputa de preços), sem prejuízo das sanções previstas neste edital.

e) Que deixarem de atender as exigências previstas no Edital, Termo de Referência e seus Anexos.

**6. DA ABERTURA DA SESSÃO PÚBLICA E DA FASE DE JULGAMENTO**

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

6.2. Iniciada a sessão pública, a Comissão de Contratação deverá informar no sistema o prazo para a atribuição de notas à proposta de técnica e de preço, e a data e o horário para manifestação da intenção de recorrer do resultado do julgamento.

6.2.1 Eventual postergação do prazo a que se refere o item 6.2 deve ser comunicada tempestivamente pela Comissão de Contratação, via sistema.

6.3. O sistema disponibilizará campo próprio para troca de mensagens entre a Comissão de Contratação e os licitantes.

6.4. Quando a desconexão do sistema eletrônico para a Comissão de Contratação persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pela Comissão de Contratação aos participantes, no sítio eletrônico utilizado para divulgação.

6.5. A Comissão de Contratação verificará as condições de participação no certame de todos os licitantes, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e no item do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

6.5.1 SICAF; e

6.5.2 Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://portaldatransparencia.gov.br/pagina-interna/603244-cnep).

6.6. A consulta aos cadastros será realizada no nome e no CNPJ da empresa licitante.

6.6.1 A consulta no CEIS quanto às sanções previstas na Lei nº 8.429, de1992, também ocorrerá no nome e no CPF do sócio majoritário da empresa licitante, se houver, por força do art. 12 da citada lei.

6.7. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Agente de Contratação/Comissão diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

6.7.1 A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

6.7.2 O licitante será convocado para manifestação previamente a uma eventual desclassificação.

6.7.3 Constatada a existência de sanção, o licitante será reputado inabilitado, por falta de condição de participação.

6.8. Na hipótese de inversão das fases de habilitação e julgamento, caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

6.9. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, a Comissão de Contratação verificará se faz jus ao benefício, em conformidade com os itens deste edital.

6.10. Verificadas as condições de participação e de utilização do tratamento favorecido, a Comissão de Contratação realizará, em conjunto com a banca designada, a verificação da conformidade das propostas.

6.11. Serão desclassificadas as propostas que:

6.12.1 contiverem vícios insanáveis;

6.12.2 não obedecerem às especificações técnicas contidas no Termo de Referência;

6.12.3 apresentarem preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

6.12.4 não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

6.12.5 apresentarem desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

6.13. Na avaliação de conformidade das propostas de técnica e de preço deverão ser indicadas as razões de eventuais desclassificações.

6.14. A análise e avaliação da conformidade das propostas será iniciada pelo exame de conformidade das propostas de técnica, observadas as regras e as condições previstas no Termo de Referência, anexo deste edital (art. 27, da IN SEGES/MGI nº 2/2023).

6.15. A análise dos quesitos de natureza qualitativa será realizada pela banca designada (art. 26, da IN SEGES/MGI nº 2/2023).

6.16. No julgamento das propostas técnicas, será atribuída ao licitante uma Nota da Proposta Técnica (NT), de acordo com o parâmetro matemático definido neste edital.

6.17. Concluída a avaliação e ponderação das propostas técnicas a Comissão de Contratação realizará a verificação da conformidade das propostas de preço.

6.18. 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.

6.18.1 A inexequibilidade, na hipótese de que trata o item anterior, só será considerada após diligência da Comissão de Contratação, que comprove:

6.18.1.1.que o custo do licitante ultrapassa o valor da proposta; e

6.18.1.2.inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

6.19. Em contratação de serviços de engenharia, além das disposições acima, a análise de exequibilidade e sobrepreço considerará o seguinte:

6.19.1 Nos regimes de execução por tarefa, empreitada por preço global ou empreitada integral, semi-integrada ou integrada, a caracterização do sobrepreço se dará pela superação do valor global estimado;

6.19.2 No regime de empreitada por preço unitário, a caracterização do sobrepreço se dará pela superação do valor global estimado e pela superação de custo unitário tido como relevante, conforme planilha anexa ao edital;

6.19.3 No caso de serviços de engenharia, serão consideradas inexequíveis as propostas cujos valores forem inferiores a 75% (setenta e cinco por cento) do valor orçado pela Administração, independentemente do regime de execução.

6.19.4 Será exigida garantia adicional do licitante vencedor cuja proposta for inferior a 85% (oitenta e cinco por cento) do valor orçado pela Administração, equivalente à diferença entre este último e o valor da proposta, sem prejuízo das demais garantias exigíveis de acordo com a Lei.

6.20. 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.

6.21. 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.

6.21.1 Em se tratando de serviços de engenharia, o licitante vencedor será convocado a apresentar à Administração, por meio eletrônico, as planilhas com indicação dos quantitativos e dos custos unitários, seguindo o modelo elaborado pela Administração, bem como com detalhamento das Bonificações e Despesas Indiretas (BDI) e dos Encargos Sociais (ES), com os respectivos valores adequados ao valor final da proposta vencedora, admitida a utilização dos preços unitários, no caso de empreitada por preço global, empreitada integral, contratação semi-integrada e contratação integrada, exclusivamente para eventuais adequações indispensáveis no cronograma físico-financeiro e para balizar excepcional aditamento posterior do contrato.

6.22. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço e que se comprove que este é o bastante para arcar com todos os custos da contratação.

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

6.22.2 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.

6.23. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante do serviço ou da área especializada no objeto.

6.24. Será atribuída ao licitante uma Nota da Proposta de Preço (NP), de acordo com o seguinte parâmetro matemático:

**Cálculo da Nota Final da Proposta**

Para a definição da proposta mais vantajosa à Administração, será adotada metodologia de julgamento pelo critério de Técnica e Preço, conforme disposto no art. 36 da Lei nº 14.133/2021 e conforme detalhamento constante do item 10 deste Termo de Referência. A avaliação das propostas seguirá uma abordagem objetiva e proporcional, que considera a qualificação técnica da licitante e a vantajosidade econômica de sua proposta.

**Etapas de Avaliação e Fórmulas Aplicadas**

**a) Cálculo da Nota Técnica (NT)**

A Nota Técnica será composta pela soma dos pontos obtidos nos seguintes componentes:

- Experiência Técnica (até 60 pontos) – conforme descrito no subitem 10.1.1;
- Fator de Qualidade – Certificações Técnicas (até 40 pontos) – conforme descrito no subitem 10.1.2.
-

A pontuação máxima da NT será, portanto, de 100 (cem) pontos.

**b) Cálculo do Índice Técnico (IT)**

A nota técnica atribuída a cada licitante será convertida em um índice padronizado, proporcional à melhor nota técnica recebida entre todas as concorrentes, mediante a seguinte fórmula:

$$IT = (NPTp / NPTa) \times 10$$

Onde:

- IT = Índice Técnico da licitante avaliada;
- $NPT_p$ = Nota da Proposta Técnica da licitante avaliada;
- $NPT_a$ = Maior Nota Técnica entre todas as propostas apresentadas.

Esse método garante que a proposta tecnicamente mais bem pontuada receba índice igual a 10, servindo de base para a proporcionalidade das demais.

**c) Cálculo do Índice de Preço (IP)**

A pontuação referente ao preço será igualmente convertida em índice, com base no menor preço global apresentado entre todos os licitantes, conforme fórmula:

$$IP = (MP / VPP) \times 10$$

Onde:

- IP = Índice de Preço da licitante;
- MP = Menor Preço Global apresentado entre todas as propostas;
- VPP = Valor da Proposta de Preço da licitante avaliada.

Dessa forma, o menor preço apresentado receberá índice 10, e os demais serão ajustados proporcionalmente.

**d) Cálculo da Nota Final (NF)**

A Nota Final será obtida mediante ponderação entre o Índice Técnico (IT) e o Índice de Preço (IP), segundo os pesos previamente estabelecidos:

- 60% para o componente técnico;
- 40% para o componente preço.

A fórmula de cálculo da NF será:

$$NF = (IT \times 60 + IP \times 40) / 100$$

Onde:

- **NF** = Nota Final da licitante;
- **IT** = Índice Técnico;
- **IP** = Índice de Preço.

**e) Classificação Final**

A licitante que obtiver a **maior Nota Final (NF)** será classificada em **primeiro lugar**, observadas as demais condições de habilitação jurídica, regularidade fiscal e trabalhista, qualificação econômico-financeira e ausência de impedimentos legais. Em caso de empate na Nota Final, aplicar-se-á o disposto nos art. 60 da Lei nº 14.133/2021.

6.26. Encerrados os prazos estabelecidos nos itens 6.2 e 6.2.1, o sistema ordenará e divulgará as notas ponderadas das propostas de técnica e de preço em ordem decrescente, considerando a maior pontuação obtida, bem como informará as notas de cada proposta por licitante. (art. 21, §2º, da IN SEGES/MGI nº 2/2023).

6.27. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de análise das propostas de técnica e de preço, 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 a Nota Final da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

6.27. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 10% (dez por cento) acima da maior Nota Final serão consideradas empatadas com a primeira colocada.

6.27. A melhor classificada nos termos do subitem anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em preço que corresponda a Nota Final superior à da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

6.27. 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 10% (dez por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

6.27. No caso de equivalência das Notas Finais atribuídas às 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 para desempate.

6.28. Havendo eventual empate entre Notas Finais, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133, de 2021, nesta ordem:

6.28. disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta de preço em ato contínuo à classificação;

6.28.1.1.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;

6.28.1.2.desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;

6.28.1.3.desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

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

6.28.2.1.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;

6.28.2.2.empresas brasileiras;

6.28.2.3.empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

6.28. empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de dezembro de 2009.

6.29. Esgotados todos os demais critérios de desempate previsto em lei, a escolha do licitante vencedor ocorrerá por sorteio, em ato público, para o qual todos os licitantes serão convocados, vedado qualquer outro processo.

6.30. Encerrada a etapa de análise das propostas, na hipótese de a proposta de preço do primeiro colocado permanecer acima do preço máximo definido para a contratação, a Comissão de Contratação poderá negociar condições mais vantajosas, após definida a melhor Nota Final entre os licitantes.

6.30.1 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.

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

6.31. O resultado da negociação será registrado na ata da sessão pública e anexado aos autos do processo licitatório.

6.32. A Comissão de Contratação solicitará ao licitante mais bem classificado que, no prazo de 03 (três) horas, envie a proposta adequada à negociação realizada, acompanhada, se for o caso, dos documentos complementares.
6.33. É facultado à Comissão de Contratação prorrogar o prazo acima estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

**7. DA HABILITAÇÃO**

**7.1. DAS CONDIÇÕES PARA PESSOAS JURÍDICAS:**

7.1.1. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato *pdf, (na sua forma pesquisável) via sistema, no prazo de 02 (duas) horas, sob pena de inabilitação.
7.1.2. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.
7.1.3. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.
7.1.4. Serão aceitos registros de CNPJ de licitante matriz e filial com diferenças de números de documentos pertinentes ao CND Federal e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.
7.1.5. Os licitantes deverão encaminhar, nos termos deste Edital, a documentação relacionada nos itens a seguir, para fins de habilitação:

**7.2. REGULARIDADE FISCAL E TRABALHISTA:**

7.2.1. Prova de inscrição no Cadastro Nacional de Pessoa Jurídica – CNPJ;
7.2.2. Prova de Regularidade de Débitos Relativos a Tributos Federais, Dívida Ativa da União e Seguridade Social (INSS);
7.2.3. Prova de regularidade para com a Fazenda Estadual sede do licitante;
7.2.4. Prova de regularidade para com a Fazenda Municipal da sede do licitante;
7.2.5. Prova de regularidade relativa ao Fundo de Garantia por Tempo de Serviço (FGTS), mediante apresentação de Certificado de Regularidade do FGTS – CRF;
7.2.6. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de Certidão Negativa de Débitos Trabalhistas – CNDT;
7.2.7. Prova de Inscrição no Cadastro de Contribuintes Estadual e/ou Municipal, se houver, relativo à sede do LICITANTE, pertinente ao seu ramo de atividade e compatível com o objeto deste Edital
7.2.8. As Microempresas ou Empresas de Pequeno Porte participantes do certame deverão declarar sua condição conforme Anexo X do presente edital, ou Termo de Enquadramento emitido pela Junta Comercial no exercício corrente.
7.2.9. Às Microempresas e Empresas de Pequeno Porte que apresentarem restrição na comprovação de regularidade fiscal será assegurado o prazo de 05 (cinco) dias úteis para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventual Certidão Negativa ou Positiva com Efeito de Negativa.
7.2.10. O prazo assegurado no subitem 7.2.1 terá como termo inicial o momento em que o proponente for declarado vencedor do certame, podendo ser prorrogado por igual período, a critério da Administração.
7.2.11. A não regularização da documentação no prazo previsto no subitem acima implicará decadência do direito à contratação, sem prejuízo das sanções administrativas previstas no artigo 90, § 5º, da Lei Federal no 14.133/21, sendo facultado à Administração convocar os licitantes remanescentes, na ordem de classificação, para a assinatura da ata, ou revogar a licitação.

**7.3. <u>HABILITAÇÃO JURÍDICA</u>**

7.3.1. Registro comercial, no caso de empresa individual; ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores; inscrição do ato constitutivo, no caso de sociedades civis.
7.3.2. Documentos de identificação de todos sócios ou da diretoria em exercício.

**7.4. <u>QUALIFICAÇÃO TÉCNICA</u>:**

A contratada deverá disponibilizar equipe técnica qualificada, em quantitativo e estrutura compatíveis com as exigências deste Termo de Referência, garantindo a execução integral dos serviços contratados, em regime de atendimento contínuo, com cobertura em horários comerciais, plantões e regime 24x7, conforme definido neste instrumento.

A composição mínima da equipe deverá contemplar, obrigatoriamente:

- 1 (um) Gerente Técnico do Contrato;
- 1 (um) Líder Técnico de Suporte Nível 1 e Nível 2;
- 1 (um) Líder Técnico de Suporte Nível 3;
- 2 (dois) Profissional de Suporte Nível 1 (N1);
- 1 (um) Profissional de Suporte Nível 2 (N2);
- 1 (um) Profissional de Suporte Nível 3 (N3);
- 1 (um) Especialista em Segurança da Informação.

**Observação:** A definição do quantitativo total de profissionais por nível é de responsabilidade da contratada, que deverá dimensionar sua equipe conforme a complexidade do contrato e a necessidade de cumprimento integral dos SLAs e quantitativo de atendimentos a serem solicitados. No entanto, será obrigatória a apresentação de profissionais distintos para cada um dos perfis mínimos definidos acima.

**Perfis Profissionais e Requisitos Mínimos**

As exigências de formação, experiência e conhecimentos abaixo descritas devem ser entendidas como requisitos mínimos para aceitação dos profissionais, complementando as atribuições técnicas já descritas noTermo de Referência.

**Gerente Técnico do Contrato**

- Ensino superior completo em TI ou áreas afins;
- Experiência mínima de 10 anos em ambientes de porte semelhante;
- Desejável certificação ITIL ou equivalente;
- Conhecimento comprovado em gestão de contratos de serviços de TI, metodologias de governança, SLAs, relatórios e coordenação de equipes multidisciplinares;
- Conhecimento geral das soluções técnicas previstas neste contrato.

**Líder Técnico de Suporte Nível 1 e Nível 2**

- Ensino superior em andamento ou completo na área de TI;
- Experiência mínima de 5 anos em suporte técnico e liderança de equipes operacionais;
- Domínio de ferramentas ITSM, gestão de escalonamento e priorização;
- Conhecimento técnico em redes, Windows, antivírus, acesso remoto e atendimento a usuários.

13.1.1 **5.15.1.3. Líder Técnico de Suporte Nível 3**

- Ensino superior completo em TI ou áreas correlatas;
- Experiência mínima de 5 anos em administração de servidores e infraestrutura crítica;
- Vivência em coordenação de equipes técnicas, gestão de problemas e implantação de soluções de infraestrutura;
- Conhecimento avançado em sistemas operacionais (Linux e Windows), virtualização, storage, firewall, Active Directory e monitoramento;
- Conhecimento técnico das soluções contratadas.

**Profissionais de Suporte Nível 1 (N1)**

- Ensino médio técnico completo em informática ou área correlata;
- Experiência mínima de 2 anos em atendimento técnico e registro de chamados;
- Conhecimentos obrigatórios:
  - ITSM, Windows, softwares corporativos, antivírus;
  - Atendimento remoto, triagem e comunicação clara com o usuário.

**Profissionais de Suporte Nível 2 (N2)**

- Ensino médio técnico completo;
- Experiência mínima de 3 anos em suporte técnico intermediário;
- Conhecimentos obrigatórios:
  - Diagnóstico e correção de falhas, impressoras, permissões;
  - Apoio a sistemas, antivírus, scripts e testes.

**Profissionais de Suporte Nível 3 (N3)**

- Ensino superior completo em TI;
- Experiência mínima de 5 anos em administração de servidores e redes;

- Conhecimentos obrigatórios:
  - Linux, Windows Server, AD, File Server, DNS, DHCP;
  - Virtualização (KVM, Hyper-V, VMware), Zabbix, backup, firewall, VPNs;
  - PostgreSQL, MySQL, tuning e segurança de infraestrutura.

**Especialistas em Segurança da Informação**

- Ensino superior completo em TI ou áreas correlatas;
- Experiência mínima de 10 anos em projetos de segurança da informação;
- Conhecimentos obrigatórios:
  - Políticas de segurança, ISO/IEC 27001, avaliação de riscos, controles técnicos;
  - Due diligence, auditoria, apoio a contratações com foco em SI;
- Desejáveis certificações: ISO 27001 Lead Implementer, CISSP, CompTIA Security+, CISM, entre outras.

**Documentos para Comprovação de Qualificação Profissional**

A qualificação e experiência dos profissionais deverão ser comprovadas por meio de um ou mais dos seguintes documentos:

- Currículo atualizado com funções exercidas e períodos de atuação;
- Cópias de certificados, diplomas ou documentos acadêmicos;
- Atestados de capacidade técnica emitidos por empresas públicas ou privadas;
- Declarações assinadas por responsáveis técnicos de projetos anteriores;
- Carteira de trabalho (CLT), contratos ou outros documentos que evidenciem a atuação.

A fiscalização poderá solicitar documentos complementares a qualquer tempo. A apresentação de documentos falsos ou informações inverídicas poderá ensejar reprovação do profissional e aplicação das penalidades previstas na legislação e no contrato.

**7.5. QUALIFICAÇÃO ECONÔMICO FINANCEIRA:**

7.5.1. Apresentar balanço patrimonial e demonstrações contábeis dos 02 (dois) últimos exercício financeiro, apresentados na forma da lei (art. 69, Inciso I da Lei 14.133/2021), que comprove a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados quando encerrados há mais de 03 (três) meses da data de apresentação das propostas, tomando como base a variação do IGP-DI ocorrida no período.

7.5.2. Demonstrativo da boa situação econômico-financeira da LICITANTE, consubstanciada nos seguintes índices, de que possui os índices financeiros solicitados a seguir:

ILC = Índice de Liquidez Corrente maior ou igual a **1,00**, calculado pela seguinte fórmula:

$$\underline{\textbf{ILC = Ativo Circulante (AC)}}$$
$$\textbf{Passivo Circulante (PC)}$$

ILG = Índice de Liquidez Geral maior ou igual a **1,00**, calculado pela seguinte formula:

$$\underline{\textbf{ILG = Ativo Circulante + Realizável a Longo Prazo}}$$
$$\textbf{Passivo Circulante + Exigível a Longo Prazo}$$

IEG = Índice de Endividamento Geral, menor ou igual a **0,85**, calculado pela seguinte formula:

$$\underline{\textbf{IEG = Passivo Circulante (PC) + Exigível a Longo Prazo (ELP)}}$$
$$\textbf{Ativo Total (AT).}$$

7.5.3. Os índices de que trata os subitens acima serão calculados pela LICITANTE e confirmados pelo responsável por sua contabilidade, mediante sua assinatura e a identificação do seu nome e do número de registro no Conselho Regional de Contabilidade, constantes no documento de apresentação dos cálculos.

7.5.4. Os valores financeiros acima referidos poderão ser atualizados para a data da licitação pelo índice oficial (IGP-DI), devendo, neste caso ser apresentada a respectiva memória de cálculo;

7.5.5. As empresas que deixarem de atender o subitem 7.7.2 deste Edital, deverão comprovar, considerados os riscos para a Administração, o patrimônio líquido mínimo de 10% (dez por cento) do valor da proposta final apresentada.

7.5.6. Certidão negativa de falência ou concordata expedida pelo distribuidor da sede do licitante válida na data da entrega das propostas e de início da abertura dos envelopes. Caso o documento não consigne prazo de validade, será considerada válida a certidão com data de expedição ou revalidação dos últimos 60 (sessenta) dias anteriores à data da realização da licitação.

**7.6. DECLARAÇÕES**

7.6.1. **CUMPRIMENTO DO DISPOSITIVO CONSTITUCIONAL:** Declaração do licitante de que não possui em seu quadro de pessoal, empregado (s) com menos de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e de 16 (dezesseis) anos em qualquer trabalho, salvo na condição de aprendiz, nos termos do inciso XXXIII do art. 7° da constituição Federal de 1998 (Modelo Anexo II).
7.6.2. Declaração de que não foi declarado inidôneo. (Modelo Anexo XI).
7.6.3. Declaração de Fatos Impeditivos. (Modelo Anexo XII).
7.6.4. Os documentos apresentados deverão ser obrigatoriamente da mesma sede, ou seja, se da matriz, todos da matriz, se de alguma filial, todos da mesma filial, com exceção dos documentos que são válidos para matriz e todas as filiais.
7.6.5 Toda a documentação de habilitação deverá referir-se à data e horário anterior ou igual a data determinada para a abertura das propostas de preços.
7.6.6. **Caso a empresa arrematante não comprove sua habilitação será convocado o próximo licitante na ordem de classificação, sendo este notificado pelo sistema** www.bnc.org.br **para que manifeste seu interesse em 02 (duas) horas. Após a confirmação do interesse, serão concedidos os mesmos prazos do item 8.1 para entrega da proposta e documentação de habilitação. Se o licitante não se manifestar dentro do prazo fixado, entender-se-á seu não interesse em fornecer.**
7.6.7. Constatando o atendimento das exigências previstas no Edital e transcorrida a fase de análise da documentação, o licitante será declarado vencedor, sendo homologado o procedimento e adjudicado o objeto da licitação pela autoridade competente.
7.6.8. Após a habilitação, poderá a licitante ser desqualificada por motivo relacionado com a capacidade jurídica, regularidade fiscal, qualificação econômico-financeira, qualificação técnica e/ou inidoneidade, em razão de fatos supervenientes ou somente conhecidos após o julgamento.
7.6.9. As certidões deverão ser apresentadas dentro do respectivo prazo de validade. Caso não conste prazo de validade no corpo da certidão, considerar-se-á o prazo de 60 (sessenta) dias da data de emissão.
7.6.10. Os documentos apresentados para habilitação são definitivos, não sendo admissível substituição ou posterior inclusão de documentos, com exceção do disposto no subitem 7.4.1.
7.6.11. O licitante vencedor que deixar de apresentar qualquer dos documentos exigidos ou apresentar documento com prazo expirado, será julgado inabilitado.

### 7.7. CRITÉRIO DE PONTUAÇÃO DA LICITANTE

7.7.1. Em razão da natureza especializada dos serviços de tecnologia da informação e segurança da informação, da complexidade técnica do objeto e da necessidade de assegurar o mais elevado padrão de qualidade na execução contratual, o julgamento das propostas deverá ocorrer segundo o critério de Técnica e Preço, nos termos do art. 36 da Lei nº 14.133/2021.
7.7.2. Esse critério garante a escolha da proposta mais vantajosa para a Administração com base em dois fatores: a qualidade técnica da proposta (experiência e certificações) e a competitividade econômica do preço ofertado.

A ponderação entre os fatores será a seguinte:

- 60% (sessenta por cento) para a Proposta Técnica;
- 40% (quarenta por cento) para a Proposta de Preços.

A Nota Final (NF) será calculada com base na média ponderada entre o Índice Técnico (IT) e o Índice de Preço (IP), segundo a fórmula:

NF = (IT × 60 + IP × 40) / 10
Onde:

- IT = Índice Técnico, obtido conforme detalhamento no item 10.1;
- IP = Índice de Preço, proporcional ao menor preço apresentado.

Será exigido, como condição mínima de classificação, que a licitante atinja nota técnica **igual ou superior a 60 pontos**, a fim de que participe da etapa de análise de preços. Essa exigência visa assegurar que somente fornecedores com qualificação técnica compatível possam ser habilitados à fase final de julgamento.

#### 7.7.3. Avaliação Técnica: Composição e Pontuação

7.7.3.1. A pontuação máxima da Proposta Técnica será de 100 pontos, distribuída da seguinte forma:

- Experiência Técnica – até 60 pontos

Apurada por meio de atestados de capacidade técnica emitidos por pessoas jurídicas de direito público ou privado, comprovando a execução de serviços compatíveis com os critérios estabelecidos neste TR.

- Fator Qualidade (Certificações Técnicas) – até 40 pontos

Aferida com base na apresentação de certificações ISO/IEC 27001 (Segurança da Informação) e ISO/IEC 27701 (Privacidade da Informação), em nome da licitante e com escopo aderente ao objeto do contrato.

**7.7.4. Experiência Técnica (Atestados de Capacidade Técnica) – 60 pontos**

7.7.4.1. A pontuação referente à experiência técnica da licitante será apurada com base na apresentação de atestados de capacidade técnica emitidos por pessoas jurídicas de direito público ou privado, que comprovem a execução anterior de serviços com escopo compatível aos exigidos nesta contratação.

7.7.4.2. Cada atestado que atenda aos requisitos técnicos descritos a seguir atribuirá até 6 (seis) pontos, totalizando até o limite máximo de 60 (sessenta) pontos.

| ***Critérios de Pontuação Técnica*** | ***7.7.4.2. Pontuação*** |
|---|---|
| ***1. Implantação de Sistema de Gestão de Segurança da Informação (SGSI) com base na ISO/IEC 27001 ou equivalente -*** *Atestado que comprove que a empresa executou projeto de implantação de SGSI conforme os princípios e controles definidos na norma ISO/IEC 27001 ou padrão equivalente, preferencialmente com posterior certificação da organização contratante.* | 6 pontos |
| **2. Elaboração de Políticas e Procedimentos de Segurança da Informação -** Atestado que comprove a execução de serviços voltados à elaboração de políticas, normas, procedimentos e planos de segurança, incluindo, entre outros: Política de Segurança da Informação, Política de Senhas, Política de Controle de Acesso, Plano de Continuidade, Plano de Resposta a Incidentes, Plano de Backup, Plano de Recuperação de Desastres. | 6 pontos |
| **3. Execução de Avaliação de Riscos ou Análise de Gaps em Segurança da Informação -** Atestado que comprove a realização de avaliação de riscos, análise de vulnerabilidades, ou gap analysis com base nos requisitos da norma ISO/IEC 27001, ISO 31000 ou frameworks reconhecidos. | 6 pontos |
| **4. Implantação de Solução ITSM (Sistema de Gestão de Chamados e Ativos de TI) -** Atestado que comprove a implantação de plataforma de ITSM com funcionalidades de abertura e gestão de chamados, controle de ativos, catálogo de serviços, base de conhecimento, escalonamento técnico e emissão de relatórios gerenciais. A solução deverá contemplar a gestão dos níveis de atendimento (N1, N2, N3) e integração com ferramentas de monitoramento. | 6 pontos |
| **5. Execução de Suporte Técnico Nível 1 e Nível 2 -** Atestado que comprove a prestação de serviços de atendimento técnico remoto e/ou presencial nos níveis 1 e 2, com classificação de chamados, atendimento por tipo de incidente, categorização e registro em ferramenta de service desk. Deve conter período de execução e escopo atendido. | 6 pontos |
| **6. Execução de Suporte Técnico Nível 3 -** Atestado que comprove a atuação técnica especializada para resolução de demandas complexas em ambientes de servidores, rede, segurança ou infraestrutura crítica, classificada como Suporte Nível 3. O atestado deve mencionar atuação corretiva, preventiva e/ou de melhoria contínua em ambiente corporativo. Deve conter período de execução e escopo atendido. | 6 pontos |
| **7. Implantação e Gerenciamento de Active Directory (AD) com redundância para Controle de Acesso -** Atestado que comprove a implantação e administração de ambientes com Active Directory, incluindo a criação e gestão de grupos, políticas de GPO, unidades organizacionais (OUs), autenticação integrada e estrutura de permissões por perfil. Inclui integração com serviços de diretório e autenticação. | 6 pontos |
| **8. Implantação e Gestão de Solução de Backup com Armazenamento em Nuvem -** Atestado que comprove o fornecimento, implantação, monitoramento e gestão de solução de backup com armazenamento em nuvem, incluindo políticas de retenção, versionamento, criptografia, e execução de testes de restauração. | 6 pontos |

| | |
|---|---|
| **9. Implantação de Solução de Gestão de Logs (SIEM) -** Atestado que comprove a implantação de solução de gestão e correlação de logs (SIEM), com coleta de eventos de segurança, análise em tempo real, criação de regras de alerta, dashboards operacionais e trilha de auditoria. Preferencialmente com integração a ativos diversos (servidores, firewalls, endpoints). | 6 pontos |
| **10. Implantação de Solução de Monitoramento Remoto e Disponibilidade de Ativos -** Atestado que comprove a implantação de ferramenta de monitoramento de ativos, recursos de rede, servidores e disponibilidade de sistemas, com geração de alertas, dashboards, acompanhamento de incidentes e relatórios de disponibilidade. | 6 pontos |

**7.7.5. Requisitos Obrigatórios dos Atestados:**

Todos os atestados apresentados deverão:

- Ser emitidos por pessoa jurídica de direito público ou privado;
- Estar em papel timbrado da entidade emitente, devidamente assinado por responsável legal;
- Conter descrição clara e objetiva dos serviços executados, alinhada com os critérios acima;
- Informar:
  - Nome da instituição contratante;
  - Período de execução;
  - Quantitativo ou abrangência do serviço;
  - Nome, cargo, telefone e e-mail do responsável pela emissão (para eventual diligência).

No caso de atestados emitidos por empresas privadas, poderão ser exigidos, em fase de análise técnica ou diligência, os seguintes documentos complementares:

- Cópia do contrato ou instrumento jurídico correspondente;
- Três últimas notas fiscais emitidas antes da publicação do edital;
- Reconhecimento de firma do signatário do atestado;
- Procuração ou comprovação dos poderes de representação do signatário, se aplicável.

Importante: Não serão aceitos atestados emitidos por empresas do mesmo grupo econômico, com sócios em comum, ou com vínculos societários entre emitente e licitante.

Regras de Pontuação:

- Cada atestado que comprove um dos critérios técnicos: 6 pontos;
- Não serão aceitos atestados compostos (que atendam mais de um critério em um único atestado sem clareza objetiva);
- Pontuação máxima total permitida: 60 pontos.

**7.7.6. Fator de Qualidade – Certificações Técnicas (até 40 pontos)**

7.7.6.1. A pontuação atribuída ao fator de qualidade técnica será aferida com base na apresentação de certificações formais emitidas por organismos acreditados, em nome da licitante (matriz ou filial), que demonstrem, de forma inequívoca, que a empresa possui sistemas de gestão implementados e operacionais, diretamente relacionados ao escopo desta contratação.

7.7.6.2. Tais certificações deverão atestar a conformidade da organização com normas internacionais amplamente reconhecidas, voltadas à segurança da informação e à proteção de dados pessoais, elementos centrais deste contrato, considerando o grau de criticidade dos serviços prestados.

7.7.6.3. Serão admitidas para fins de pontuação técnica as seguintes certificações:

- Certificação ISO/IEC 27001 – até 25 (vinte e cinco) pontos: válida para empresas que possuam sistema de gestão da segurança da informação implementado, com escopo compatível com atividades de operação de infraestrutura de TIC, consultoria em segurança da informação, suporte técnico especializado em tecnologia da informação. O escopo técnico deverá estar claramente vinculado às obrigações contratuais previstas neste Termo de Referência.
- Certificação ISO/IEC 27701:2019 – até 15 (quinze) pontos: válida para empresas certificadas em sistema de gestão da privacidade da informação, com escopo compatível com atividades de operação de infraestrutura de TIC, consultoria em segurança da informação, suporte técnico especializado em tecnologia da informação. O escopo técnico deverá estar claramente vinculado às obrigações contratuais previstas neste Termo de Referência.

As certificações apresentadas deverão obrigatoriamente atender aos seguintes requisitos formais:

- Estar válidas na data de abertura da licitação, conforme indicado no documento oficial emitido pelo organismo certificador;
- Ser apresentadas em cópia simples ou autenticada, em idioma original;
- Conter a identificação expressa da unidade certificada, seja matriz ou filial, que participará da execução contratual;
- Apresentar o escopo técnico certificado de forma clara e objetiva, seja diretamente no certificado ou em declaração complementar do organismo certificador, demonstrando a compatibilidade com as exigências deste edital.

7.7.6.4. A ausência das certificações referidas não configura fator impeditivo à habilitação da licitante, todavia, sua apresentação conferirá pontuação técnica adicional e objetiva, representando diferencial competitivo para empresas que atuem com nível de maturidade institucional de segurança da informação e privacidade alinhado às boas práticas de mercado e à normativa técnica vigente.

7.7.6.5. O objetivo desta avaliação é fomentar a seleção de empresas com capacidade organizacional comprovada, estruturalmente aderentes ao modelo de governança e segurança requerido pela Administração Pública, sobretudo no que tange à integridade, disponibilidade, confidencialidade e privacidade das informações tratadas.

**7.7.7. Cálculo da Nota Final da Proposta**

7.7.7.1.Para a definição da proposta mais vantajosa à Administração, será adotada metodologia de julgamento pelo critério de Técnica e Preço, conforme disposto no art. 36 da Lei nº 14.133/2021 e conforme detalhamento constante do item 10 deste Termo de Referência. A avaliação das propostas seguirá uma abordagem objetiva e proporcional, que considera a qualificação técnica da licitante e a vantajosidade econômica de sua proposta.

**7.7.8. Etapas de Avaliação e Fórmulas Aplicadas**

**a) Cálculo da Nota Técnica (NT)**

A Nota Técnica será composta pela soma dos pontos obtidos nos seguintes componentes:

- Experiência Técnica (até 60 pontos) – conforme descrito no subitem 10.1.1;
- Fator de Qualidade – Certificações Técnicas (até 40 pontos) – conforme descrito no subitem 10.1.2.

A pontuação máxima da NT será, portanto, de 100 (cem) pontos.

**b) Cálculo do Índice Técnico (IT)**

A nota técnica atribuída a cada licitante será convertida em um índice padronizado, proporcional à melhor nota técnica recebida entre todas as concorrentes, mediante a seguinte fórmula:

$$IT = (NPTp / NPTa) \times 10$$

Onde:

- IT = Índice Técnico da licitante avaliada;
- $NPT_p$ = Nota da Proposta Técnica da licitante avaliada;
- $NPT_a$ = Maior Nota Técnica entre todas as propostas apresentadas.

Esse método garante que a proposta tecnicamente mais bem pontuada receba índice igual a 10, servindo de base para a proporcionalidade das demais.

**c) Cálculo do Índice de Preço (IP)**

A pontuação referente ao preço será igualmente convertida em índice, com base no menor preço global apresentado entre todos os licitantes, conforme fórmula:

$$IP = (MP / VPP) \times 10$$

Onde:

- IP = Índice de Preço da licitante;
- MP = Menor Preço Global apresentado entre todas as propostas;
- VPP = Valor da Proposta de Preço da licitante avaliada.

Dessa forma, o menor preço apresentado receberá índice 10, e os demais serão ajustados proporcionalmente.

**d) Cálculo da Nota Final (NF)**

A Nota Final será obtida mediante ponderação entre o Índice Técnico (IT) e o Índice de Preço (IP), segundo os pesos previamente estabelecidos:

- 60% para o componente técnico;
- 40% para o componente preço.

A fórmula de cálculo da NF será:

$$NF = (IT \times 60 + IP \times 40) / 100$$

Onde:

- **NF** = Nota Final da licitante;
- **IT** = Índice Técnico;
- **IP** = Índice de Preço.
-

**e) Classificação Final**

A licitante que obtiver a **maior Nota Final (NF)** será classificada em **primeiro lugar**, observadas as demais condições de habilitação jurídica, regularidade fiscal e trabalhista, qualificação econômico-financeira e ausência de impedimentos legais. Em caso de empate na Nota Final, aplicar-se-á o disposto nos art. 60 da Lei nº 14.133/2021.

**8. DO ENVIO DOS DOCUMENTOS ORIGINAIS OU ATENTICADOS**

8.1. Após o comunicado da Comissão de Contratação, o licitante deverá encaminhar os ORIGINAIS OU CÓPIAS AUTENTICADAS, VIA SEDEX ou outro meio que lhe for conveniente, no prazo máximo de 02 (dois) dias, sob pena de decair do direito do licitante de ser contratado, sem prejuízo das sanções previstas neste Edital.

8.1.1. Os Documentos poderão ser apresentados em original, por qualquer processo de cópia autenticada por cartório competente ou por servidor da Administração ou publicação em órgão da imprensa oficial.

8.2. Também deverá ser enviada o original da proposta impressa assinada, com o último lance ofertado no certame, conforme disposições do item 6, respeitados os limites de preços máximos estabelecidos para cada item contido nas planilhas do Anexo III.

8.3. No prazo máximo de 02 (dois) dia úteis o licitante deverá comprovar a postagem dos documentos com o ENCAMINHAMENTO DO CÓDIGO RASTREADOR OU OUTRO DOCUMENTO COMPROBATÓRIO da sua postagem, para o e-mail: **licitacao@morrodochapeu.ba.gov.br**

8.3.1. Os documentos deverão ser encaminhados aos cuidados do AGENTE DE CONTRATAÇÃO para o seguinte endereço:

**PREFEITURA MUNICIPAL DE MORRO DO CHAPÉU-BAHIA**
**DEPARTAMENTO DE LICITAÇÕES E CONTRATOS ADMINISTRATIVOS**
**RUA CORONEL DIAS COELHO, Nº 188, CENTRO**
**MORRO DO CHAPÉU-BAHIA**
**CEP: 44.850-000**

8.4. Se os documentos forem assinados com certificado digital de acordo com a MP 2.200-2/2001 (Chave ICP Brasil), ou ainda autenticados de forma digital por instituição aceita e reconhecida pela legislação, fica a empresa desobrigada a encaminhar a documentação referida acima.

**9. DO VALOR MÁXIMO DA LICITAÇÃO**

9.1. O valor estimado ou o valor máximo aceitável para a contratação está devidamente descrito no anexo I (Termo de Referência) deste edital.

**10. DA IMPUGNAÇÃO AO EDITAL E RECURSOS**

10.1. Impugnações e pedidos de esclarecimentos ao ato convocatório do Concorrência serão recebidos até 03 (três) dias úteis anteriores a data fixada para abertura da licitação, por meio do e-mail indicado no preambulo deste edital.

10.1.1. Caberá à Comissão de Contratação decidir sobre a impugnação, no prazo de 02 (dois) dias úteis.

10.1.2. Deferida a impugnação do ato convocatório, será designada nova data para realização do certame.

10.2. Ao final da sessão pública e declarado o vencedor, o proponente que desejar recorrer contra decisões da Comissão de Contratação poderá fazê-lo, manifestando sua intenção imediatamente em até 30 (trinta) minutos, no campo próprio do sistema (opção recurso), sendo-lhe facultado juntar memoriais no prazo de 3 (três) dias úteis. Os interessados ficam, desde logo, intimados a apresentar contrarrazões em igual prazo, que começará a correr do término do prazo do recorrente.

10.2.1. A falta de manifestação imediata do licitante importará a decadência do direito de recorrer e a adjudicação ao vencedor do certame.

10.2.2. As razões recursais deverão ser encaminhadas devidamente instruídas para o e-mail da Comissão de Contratação, indicado no preambulo deste edital, ou protocolado no setor de licitações também indicados no preambulo.

10.3. Os recursos contra decisões da Comissão de Contratação referente à habilitação ou inabilitação do licitante e julgamento das propostas terão efeito suspensivo e deverão respeitar os ditames legais previstos no artigo 168, da Lei Federal nº. 14.133/21.

10.4. O acolhimento de recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento.
10.5. Havendo recurso, da Comissão de Contratação apreciará os mesmos e, caso não reconsidere sua posição, caberá à autoridade máxima competente, a Prefeita Municipal, a decisão em grau final.
10.5.1. A decisão em grau de recurso será definitiva e dela dar-se-á conhecimento mediante publicação na imprensa oficial.
10.6. Não serão conhecidas as impugnações e recursos apresentados fora do prazo legal, subscrito por representante não habilitado legalmente, ou não identificado no processo para responder pelo proponente.

**11. DA HOMOLOGAÇÃO E ADJUDICAÇÃO**
11.1. Decididos os recursos e constatada a regularidade dos atos procedimentais, a autoridade competente homologará e adjudicará o objeto ao vencedor, podendo revogar a licitação nos termos do artigo 71 da Lei Federal n º 14.133/21.

**12. DA CONTRATAÇÃO**
12.1. Terá o adjudicatário o prazo de 05 (cinco) dias, contados a partir da data de sua convocação, para assinar o contrato sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.
12.2. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Contrato, a Administração poderá encaminhá-la para assinatura, mediante meio eletrônico, para que seja assinada e devolvida para o endereço indicado no item 8.3, no prazo de 05 (cinco) dia, a contar da data do envio do e-mail.
12.3. Para celebração do contrato o licitante deverá manter todas as condições de habilitação, reapresentando todas as certidões de regularidade exigidas por ocasião da licitação.
12.4. Farão parte integrante do contrato todos os elementos apresentados pelo licitante vencedor, que tenham servido de base à Licitação, bem como as condições estabelecidas neste Edital e seus anexos.
12.5. A empresa convocada deverá apresentar na data da assinatura do contrato, documentação comprobatória da capacidade operacional que poderá ser fornecida da seguinte forma:
a) Relação dos profissionais e comprovação do vinculo de subordinação entre a empresa e os profissionais colocados a disposição da administração.
12.6. A empresa deverá, ainda, apresentar planilha discriminando, de forma individualizada, o item, a descrição, os valores e percentuais dos insumos e da mão de obra.

**13. DO PAGAMENTO**
13.1. Os pagamentos serão efetuados mediante crédito em conta corrente devendo o fornecedor informar o número do banco, da agência e conta bancária, ou através de banco credenciado, a critério da Administração.
13.2. O pagamento devido pelo Município será efetuado, conforme estipulado nos termo da Minuta do Contrato.

**14. DA DOTAÇÃO ORÇAMENTÁRIA**
14.1. Os recursos necessários ao pagamento das despesas inerentes a este contrato correrão por conta das dotações orçamentárias e elementos de despesa indicados na Minuta do Contrato.

**15. DAS PENALIDADES E SANÇÕES AOS LICITANTES**
15.1. A empresa adjudicatária deverá observar rigorosamente as condições estabelecidas para fornecimento do objeto adjudicado, sujeitando-se as penalidades constantes nos artigos 156 e 162 da Lei 14.133/21, dentre elas a suspensão do direito de licitar pelo período de 3 (três) anos.
15.1.2 Para os efeitos do art. 162 da Lei 14.133/21, fica estabelecida a multa cominatória de 2% (dois por cento) sob o valor global da proposta apresentada, a ser aplicada em caso de infringência de qualquer das cláusulas contratuais celebradas, no presente instrumento e/ou da proposta apresentada;
15.1.3 Pelo não fornecimento do objeto licitado após assinatura do contrato, multa de 2% (dois por cento) do valor do contrato, e nessa hipótese, poderá ainda o Município de Morro do Chapéu revogar a licitação (ou rescindir o contrato) ou convocar os licitantes remanescentes, na ordem de classificação, para fazer o fornecimento do objeto, nas mesmas condições propostas pelo primeiro classificado.
15.2. Multa de 0,1% (um décimo por cento) por dia de atraso na entrega programada, incidente sobre o valor da quantidade que deveria ser entregue. A partir do 16º décimo sexto dia de atraso será considerado como inexecução parcial e a partir do 31º (trigésimo primeiro) dia inexecução total do ajuste, incidindo sobre estas as multas estabelecidas nos subitens a seguir:

15.2.1. Multa de 2% (dois por cento) por inexecução parcial do ajuste, calculada sobre o valor da parcela inexecutada, inclusive por entregar o produto em desconformidade com o exigido no Edital e seus respectivos anexos.
15.2.1.1. Quando o tipo de embalagem e/ou rotulagem do produto estiver em desacordo com o solicitado, além da troca do produto pela licitante, que será aceita uma única vez, no prazo de 10 (dez) dias corridos, a contar da data da intimação/notificação, sem qualquer ônus para o Município.
15.2.2. Multa de 5% (cinco por cento) por inexecução total do ajuste, calculada sobre o valor do contrato ou Ordem de Fornecimento respectiva.
15.3. Multa de 10% (dez por cento) calculada sobre o valor do produto entregue, que será aplicada após regular processo, nos seguintes casos:
15.3.1. Quando na análise sensorial, o produto apresentar características alteradas e/ou quando na reanálise técnica, o produto apresentar distorções em relação ao estabelecido na ficha técnica, além da troca do produto pela licitante, no prazo máximo de 10 (dez) dias corridos, contados da data da notificação/intimação, sem qualquer ônus para o Município.
15.3.2. Quando apurado por laudo, o produto apresentar alguma diferença em suas características físico-químicas, além da troca da mercadoria pela licitante, no prazo máximo de 10 (dez) dias, a contar da data da intimação/notificação, sem qualquer ônus para o Município.
15.3.3. Quando apurado por laudo, a análise microscópica e/ou toxicológica do produto comprovar a presença de sujidades, parasitas e larvas ou substâncias estranhas à sua composição, além da troca da mercadoria, no prazo máximo de 10 (dez) dias, a contar da data da notificação/intimação, sem qualquer ônus para o Município.
15.3.4. Quando apurado por laudo, a análise microbiológica e/ou toxicológica do produto comprovar a presença de substâncias nocivas à saúde, contaminação e/ou deterioração, sem prejuízo da apuração da responsabilidade civil e criminal, perante os Órgãos de Defesa do Consumidor.
15.3.5. Nesta hipótese, o produto será posto à disposição do Órgão de Fiscalização Federal, Estadual ou Municipal competente, para que o mesmo disponha sobre sua retirada e destinação, devendo a licitante providenciar a sua substituição, responsabilizando-se por todas as despesas relativas ao transporte e armazenamento do produto.
15.4. Nos casos acima descritos, se a licitante efetuar a troca do produto, sem nele perdurar as irregularidades anteriormente constatadas, pode a Administração, mediante justificativa expressa, dispensar a aplicação das referidas penalidades.
15.5. Se a infração cometida se caracterizar de má-fé ou causar prejuízos ao abastecimento efetuado pela Prefeitura Municipal de Morro do Chapéu, poderá esta impor àquela a pena de suspensão temporária do direito de licitar e contratar com o Poder Público ou propor à autoridade competente, a declaração de inidoneidade, pelo período de até 03 (três) anos.
15.6. No caso de troca do produto na forma estabelecida nos subitens anteriores, a licitante assumirá a responsabilidade pelos custos de armazenagem, que incluem: transporte, carga, descarga, estocagem e movimentação, relativos ao período em exame, que deverão ser pagos pela licitante através da Guia de Arrecadação própria, emitida pela Prefeitura Municipal de Morro do Chapéu. Nenhum pagamento será efetuado à Contratada até que seja atestado o novo recebimento do produto.
15.7. As multas são independentes entre si e a aplicação de uma não exclui a das outras, sendo descontadas do respectivo pagamento, através da retenção dos créditos decorrentes do contrato, até o limite dos valores apurados.

**16. DAS DISPOSIÇÕES FINAIS**

16.1. O proponente vencedor será responsável pelos danos causados diretamente à Administração ou a terceiros, decorrentes de sua culpa ou dolo, na execução da obrigação, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo órgão interessado.
16.2. As normas disciplinadoras deste Concorrência serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, a finalidade e a segurança da contratação.
16.3. É facultado a Comissão de Contratação ou à autoridade superior, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou complementar a instrução do processo, vedada a inclusão posterior de documento ou informação que deveria constar no ato da sessão pública.
16.4. A Administração reserva-se o direito de transferir o prazo para o recebimento e abertura das propostas descabendo, em tais casos, direito à indenização pelos licitantes.
16.5. A participação na presente licitação implica em concordância tácita, por parte do licitante, com todos os termos e condições deste Edital e das cláusulas contratuais já estabelecidas.

16.6. A autoridade competente, para determinar a contratação, poderá revogar a licitação em face de razões de interesse público derivadas de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta, devendo anulá-la por ilegalidade, de ofício ou por provocação de qualquer pessoa, mediante ato escrito e fundamentado.
16.7. Fica eleito o Foro da Comarca de MORRO DO CHAPÉU - BA, excluindo qualquer outro, por mais privilegiado que seja ou venha a se tornar, para dirimirem-se eventuais litígios oriundos do presente Edital.

**17. ANEXOS DESTE EDITAL:**
Anexo I - Termo de Referência;
Anexo II - Modelo de Declaração de Cumprimento a Disposto Constitucional (Declaração de menor);
Anexo III - Modelo Carta de Apresentação da Proposta;
Anexo IV – Modelo de Pleno Conhecimento;
Anexo V – Minuta do Contrato;
Anexo VI – Modelo de Procuração;
Anexo VII – Modelo de Declaração de Micro Empresa ou Empresa de Pequeno Porte;
Anexo VIII – Modelo de Declaração de Inidoneidade;
Anexo IX – Modelo de Declaração de Fatos Impeditivos;
Anexo X – Modelo de Declaração de Autenticidade dos Documentos;

**Morro do Chapéu-Bahia, 06 de novembro de 2025.**

_____
**VANESSA DE FREITAS PEREIRA**
**SECRETÁRIA DE ADMINISTRAÇÃO E FINANÇAS**

**ANEXO I**

## TERMO DE REFERÊNCIA

| | |
|---|---|
| **SECRETARIA DEMANDANTE:** | Secretaria Municipal de Administração e Finanças |
| **Nº DFD:** | 026/2025 |

## 1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

**1.1.** Contratação de empresa para prestação de serviço especializado em tecnologia da informação e segurança da informação, incluindo suporte técnico em múltiplos níveis (N1, N2 e N3), implantação e operação de soluções de segurança (backup, antivírus, SIEM, RMM, ITSM, entre outras), apoio à resposta a incidentes, e estruturação de políticas e normas de segurança, visando garantir a continuidade dos serviços públicos, a estabilidade da infraestrutura de TI do município de Morro do Chapéu/BA**,** nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

| Item | Descrição | Unidade de Medida | QUANT. | MÈDIA MENSAL | MÉDIA ANUAL |
|---|---|---|---|---|---|
| 1 | Gerenciamento Técnico e Operacional do Contrato - Presencial e Remoto | Mês de vigência contratual | 12 | R$ 5.179,97 | R$ 62.159,64 |
| 2 | Serviços Técnicos de Suporte Nível 1 (N1) - 24x7 - Remoto | Mês de vigência contratual com disponibilidade de até 500 chamados no mês corrente. | 12 | R4 17.279,60 | R$ 207.355,20 |
| 3 | Serviços Técnicos de Suporte Nível 2 (N2) - 24x7 - Remoto e Presencial | Mês de vigência contratual com disponibilidade de até 150 chamados no mês corrente. | 12 | R$ 13.418,61 | R$ 161.023,32 |
| 4 | Serviços Técnicos de Suporte Nível 3 (N3) - 24x7 - Remoto e Presencial | Mês de vigência contratual com disponibilidade de até 50 chamados no mês corrente. | 12 | R$ 5.955,55 | R$ 71.466,60 |
| 5 | Serviços Especializados de Segurança da Informação - 24x7 - Remoto e Presencial | UST - Contrato anual com 1200 UST | 1.200 | R$ 233,05 | R$ 279.660,00 |
| 6 | Implantação de Solução de Active Directory Redundante com File Server e DFS | Implantação (setup) | 1 | R$ 34.417,02 | R$ 34.417,02 |
| 7 | Implantação da Solução de ITSM com Módulo de Inventário e CMDB | Implantação (setup) + Mês de vigência contratual | 12 | R$ 5.315,97 | R$ 63.791,64 |

| | | | | | |
|---|---|---|---|---|---|
| 8 | Implantação da Solução de RMM (Remote Monitoring and Management) - Para até 600 máquinas (servidores e desktops) | Implantação (setup) + Mês de vigência contratual | 12 | R$ 6.183,92 | R$ 74.207,04 |
| 9 | Implantação da Solução de Monitoramento de Ativos, Servidores, Redes e Sistemas | Implantação (setup) + Mês de vigência contratual | 12 | R$ 2.978,15 | R$ 35.737,80 |
| 10 | Implantação da Solução de Gestão de Logs e SIEM | Implantação (setup) + Mês de vigência contratual | 12 | R$ 2.517,41 | R$ 30.208,92 |
| 11 | Implantação de Solução de Análise de Vulnerabilidade Técnica - servidores, desktops, sistemas e rede | Implantação (setup) + Mês de vigência contratual | 12 | R$ 2.314,78 | R$ 27.777,36 |
| 12 | Solução de Antivírus com EDR e Filtro de Conteúdo - 580 licenças (servidores e desktops) | Implantação (setup) + Mês de vigência contratual | 12 | R$ 9.158,29 | R$ 109.899,48 |
| 13 | Solução de Backup em Nuvem com Segurança Avançada e Recuperação de Desastres - 10TB de armazenamento em nuvem localizados em Datacenter no Brasil | Implantação (setup) + Mês de vigência contratual | 12 | R$ 10.612,62 | R$ 127.351,44 |
| **Subtotal** | | | | | **R$ 1.285.055,46** |

**Tabela 1 – Descrição dos Serviços, Unidade de Medida e Método de Medição**

| Item | Descrição | Unidade de Medida | Método de Medição |
|---|---|---|---|
| 1 | Gerenciamento Técnico e Operacional do Contrato - Presencial e Remoto | Mês de vigência contratual | **Mês de Vigência Contratual:**<br>* Relatório mensal de desempenho técnico;<br>* Reunião semanal/mensal de acompanhamento com o gestor das atividades e dos projetos; |
| 2 | Serviços Técnicos de Suporte Nível 1 (N1) - 24x7 - Remoto | Mês de vigência contratual com disponibilidade de até | **Mês de Vigência Contratual:**<br>* Registros de chamados na ferramenta de ITSM; |

| | | | |
|---|---|---|---|
| | | 500 chamados no mês corrente. | * Cumprimento de SLAs de atendimento;<br>* Resultado da pesquisa de satisfação; |
| 3 | Serviços Técnicos de Suporte Nível 2 (N2) - 24x7 - Remoto e Presencial | Mês de vigência contratual com disponibilidade de até 150 chamados no mês corrente. | **Mês de Vigência Contratual:**<br>* Registros de chamados na ferramenta de ITSM;<br>* Cumprimento de SLAs de atendimento;<br>* Resultado da pesquisa de satisfação; |
| 4 | Serviços Técnicos de Suporte Nível 3 (N3) - 24x7 - Remoto e Presencial | Mês de vigência contratual com disponibilidade de até 50 chamados no mês corrente. | **Mês de Vigência Contratual:**<br>* Registros de chamados na ferramenta de ITSM;<br>* Cumprimento de SLAs de atendimento;<br>* Resultado da pesquisa de satisfação; |
| 5 | Serviços Especializados de Segurança da Informação - 24x7 - Remoto e Presencial | UST - Contrato anual com 1200 UST | **Banco de Horas (UST):**<br>* Ordem de serviço assinada para execução do serviço;<br>* Relatório de execução das atividades;<br>* Apuração mensal de saldo e uso de USTs; |
| 6 | Implantação de Solução de Active Directory Redundante com File Server e DFS | Implantação (setup) | **Implantação (Setup):**<br>* Entrega técnica validada (checklist de implantação)<br>* Documentação entregue<br>* Ambiente funcionando, testado e totalmente integrado |
| 7 | Implantação da Solução de ITSM com Módulo de Inventário e CMDB | Implantação (setup) + Mês de vigência contratual | **Implantação (Setup):**<br>* Entrega técnica validada (checklist de implantação)<br>* Documentação entregue<br>* Ambiente funcionando, testado e totalmente integrado<br>**Mês de Vigência Contratual:**<br>* SLA de disponibilidade da ferramenta (>= 99%);<br>* Relatórios mensais de chamados registrados;<br>* Relatório mensal dos equipamentos inventariadas; |

| | | | |
|---|---|---|---|
| 8 | Implantação da Solução de RMM (Remote Monitoring and Management - Gerenciamento e monitoramento Remoto) - Para até 600 máquinas (servidores e desktops) | Implantação (setup) + Mês de vigência contratual | **Implantação (Setup):**<br>* Entrega técnica validada (checklist de implantação)<br>* Documentação entregue<br>* Ambiente funcionando, testado e totalmente integrado<br><br>**Mês de Vigência Contratual:**<br>* SLA de disponibilidade da ferramenta (>= 99%);<br>* Relatórios de agents ativos + alertas tratados; |
| 9 | Implantação da Solução de Monitoramento de Ativos, Servidores, Redes e Sistemas | Implantação (setup) + Mês de vigência contratual | **Implantação (Setup):**<br>* Entrega técnica validada (checklist de implantação)<br>* Documentação entregue<br>* Ambiente funcionando, testado e totalmente integrado<br><br>**Mês de Vigência Contratual:**<br>* SLA de disponibilidade da ferramenta (>= 99%);<br>* Painel com todos os ativos monitorados + mapa + relatório com alertas emitidos; |
| 10 | Implantação da Solução de Gestão de Logs e SIEM | Implantação (setup) + Mês de vigência contratual | **Implantação (Setup):**<br>* Entrega técnica validada (checklist de implantação)<br>* Documentação entregue<br>* Ambiente funcionando, testado e totalmente integrado<br><br>**Mês de Vigência Contratual:**<br>* SLA de disponibilidade da ferramenta (>= 99%);<br>* Painel com todos os ativos sendo monitorados + registro de logs durante todo o período; |
| 11 | Implantação de Solução de Análise de Vulnerabilidade Técnica - servidores, desktops, sistemas e rede | Implantação (setup) + Mês de vigência contratual | **Implantação (Setup):**<br>* Entrega técnica validada (checklist de implantação)<br>* Documentação entregue<br>* Ambiente funcionando, testado e totalmente integrado<br><br>**Mês de Vigência Contratual:**<br>* SLA de disponibilidade da ferramenta (>= 99%);<br>* Painel com todos as análises de vulnerabilidades efetuadas no período e a |

| | | | |
|---|---|---|---|
| | | | manutenção do histórico;<br>* Relatório com o status das correções de vulnerabilidades encontradas e a evolução no tratamento das vulnerabilidades; |
| 12 | Solução de Antivírus com EDR e Filtro de Conteúdo - 580 licenças (servidores e desktops) | Implantação (setup) + Mês de vigência contratual | **Implantação (Setup):**<br>* Entrega técnica validada (checklist de implantação)<br>* Documentação entregue<br>* Ambiente funcionando, testado e totalmente integrado<br><br>**Mês de Vigência Contratual:**<br>* SLA de disponibilidade da ferramenta (>= 99%);<br>* Relatório com total de agents instalados + total de alertas gerados pela ferramenta;<br>* Relatório de uso do filtro de conteúdo; |
| 13 | Solução de Backup em Nuvem com Segurança Avançada e Recuperação de Desastres - 10TB de armazenamento em nuvem localizados em Datacenter no Brasil | Implantação (setup) + Mês de vigência contratual | **Implantação (Setup):**<br>* Entrega técnica validada (checklist de implantação)<br>* Documentação entregue<br>* Ambiente funcionando, testado e totalmente integrado<br><br>**Mês de Vigência Contratual:**<br>* SLA de disponibilidade da ferramenta<br>(>= 99%);<br>* Disponibilização de armazenamento em nuvem e em datacenter no Brasil;<br>* Relatório de execução e acompanhamento do processo de backup incluindo checagens, testes, *restores*, uso de armazenamento e problemas/incidentes com o backup no período; |

**1.2.** A presente contratação adotará como regime de execução a Empreitada por Preço Global

**1.3.** O prazo de vigência da contratação é de 12 (doze) meses, contados da assinatura do contrato, na forma do artigo 105, podendo ser prorrogável na forma do art. 106 da Lei n° 14.133/2021.

**1.4** Os serviços a serem contratados enquadram-se nas possibilidades legais para terceirização da administração pública, podendo ser executados de forma indireta.

**1.5** A prestação dos serviços não gera vínculo empregatício entre os empregados da Contratada e a Administração Contratante, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

## 2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

A contratação de empresa especializada em tecnologia da informação e segurança da informação visa atender à necessidade estratégica do Município de Morro do Chapéu/BA de garantir a continuidade dos serviços públicos, a

estabilidade da infraestrutura de TI e a conformidade com a legislação vigente, especialmente no que se refere à proteção de dados e à segurança digital.

A Administração Municipal enfrenta desafios críticos relacionados à ausência de políticas estruturadas de segurança da informação, limitações operacionais da equipe interna e inexistência de soluções técnicas adequadas para suporte, monitoramento, prevenção de incidentes e resposta a falhas. Atualmente, não há estrutura suficiente para gerenciar riscos tecnológicos, proteger os dados institucionais e assegurar a disponibilidade dos sistemas essenciais ao funcionamento da gestão pública.

Nesse contexto, torna-se imprescindível a contratação de serviços especializados que contemplem:

- Suporte técnico em múltiplos níveis (N1, N2 e N3);
- Implantação e operação de soluções integradas de segurança e gestão, como backup em nuvem, antivírus com EDR, RMM (monitoramento remoto), ITSM (gestão de serviços), SIEM (gerenciamento de eventos e incidentes de segurança), entre outras;
- Apoio à resposta a incidentes de segurança;
- Estruturação e implementação de políticas, normas e procedimentos de segurança da informação, alinhados à LGPD e às melhores práticas internacionais (como ISO 27001 e NIST).

Esses serviços deverão ser prestados por equipe técnica multidisciplinar, com capacidade de atendimento em regime contínuo (24x7), conforme níveis de criticidade definidos, garantindo rapidez na resposta a falhas, mitigação de riscos e suporte qualificado para as demandas da Administração.

Além de fortalecer a infraestrutura tecnológica municipal, a contratação visa atender aos princípios da eficiência, economicidade, continuidade do serviço público, segurança jurídica e conformidade regulatória, conforme previsto na Lei nº 14.133/2021, especialmente em seus artigos 6º, 11 e 18, bem como na Lei nº 13.709/2018 (LGPD), Lei nº 12.527/2011 (LAI) e no Marco Civil da Internet (Lei nº 12.965/2014).

Portanto, a contratação ora proposta representa uma medida essencial para modernizar e proteger o ambiente digital da Administração Municipal, assegurando a prestação de serviços públicos com confiabilidade, segurança e qualidade.

## 3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO

**3.1.** A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares.

## 4. REQUISITOS DA CONTRATAÇÃO:

**4.1.** São requisitos da contratação:
a) Atendimento técnico em múltiplos níveis (N1, N2 e N3), com atuação remota e presencial, conforme a criticidade da demanda.
b) Apoio contínuo à gestão de infraestrutura de TI da Prefeitura Municipal, com foco na prevenção de incidentes, resposta rápida e manutenção da estabilidade dos serviços.
c) Implantação e operação de sistemas de backup corporativo automatizado, com retenção e versionamento seguro.
d) Gerenciamento de soluções de antivírus corporativo com console centralizada.
e) Operação de sistemas de SIEM (Security Information and Event Management) e RMM (Remote Monitoring and Management).
f) Implantação e/ou manutenção de plataforma ITSM (Information Technology Service Management).
g) Monitoramento contínuo de ativos, rede e serviços, com geração de alertas em tempo real.
h) Elaboração e/ou atualização de políticas, planos, diretrizes e normas de segurança da informação em conformidade com a LGPD (Lei Geral de Proteção de Dados) e melhores práticas.
i) Apoio à estruturação de planos de continuidade de negócios (PCN) e de recuperação de desastres (DRP).
j) Realização de treinamentos e orientações à equipe interna sobre boas práticas de cibersegurança.

l) A prestação dos serviços deverá prever a continuidade das operações de TI, com suporte em regime de prontidão para incidentes críticos.
m) Comprovação de experiência anterior em prestação de serviços similares em órgãos públicos ou entes de médio ou grande porte.
n) Disponibilização de relatórios periódicos sobre o desempenho dos serviços, incluindo tempo médio de atendimento, número de chamados resolvidos por nível, incidentes de segurança registrados e mitigados, entre outros.
o) Apresentação de indicadores de desempenho (KPIs) que permitam a avaliação contínua da efetividade dos serviços prestados.

## 5. MODELO DE EXECUÇÃO DO OBJETO

**Condições de execução**
5.1. A execução do objeto seguirá a seguinte dinâmica:
a) O início da execução do objeto será a partir da assinatura do Contrato de Prestação de Serviços;
b) Os serviços devem ser prestados no Município de Morro do Chapéu, nas suas unidades administrativas.

**Materiais a serem disponibilizados**
5.2. Para perfeita execução dos serviços, a Contratada deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, na quantidade e qualidade para a perfeita execução da prestação de serviço, promovendo sua substituição quando necessário.

**5.3. Informações relevantes para o dimensionamento da proposta**

A execução dos serviços objeto desta contratação tem como finalidade assegurar a estabilidade, disponibilidade, segurança e continuidade das operações tecnológicas da Prefeitura Municipal, mediante a prestação de serviços técnicos especializados em tecnologia da informação e segurança da informação. A atuação da contratada envolverá suporte técnico operacional em múltiplos níveis (N1, N2 e N3), bem como a implantação e operação de soluções essenciais de infraestrutura, segurança e governança de TI, voltadas à modernização do ambiente computacional da Administração.

Atualmente, o parque tecnológico da Prefeitura é composto por aproximadamente 386 equipamentos em operação, entre desktops e notebooks, além de 111 impressoras. Há também 49 desktops, 8 notebooks e 23 impressoras fora de uso, por motivos técnicos. Com a contratação paralela de novos equipamentos por meio de locação, o parque será ampliado para 526 estações ativas (sendo 387 desktops e 139 notebooks), além de 155 impressoras, considerando ainda uma margem de crescimento de até 10%, em razão da posse de novos servidores públicos aprovados em concurso.

Com a modernização proposta, serão implantadas soluções estratégicas, como controladores de domínio (Active Directory) com redundância, servidores de arquivos com alta disponibilidade, antivírus corporativo, backup em nuvem, gestão de acessos, análise de vulnerabilidades, gestão de logs, monitoramento, sistema ITSM, inventário automatizado, entre outras medidas alinhadas às boas práticas de segurança da informação.

Para suportar essa estrutura, a contratada deverá dispor de uma equipe técnica multidisciplinar estruturada em três níveis de atendimento:

- **Nível 1 (N1):** atendimento inicial, triagem, resolução de demandas comuns e contato direto com o usuário final;
- **Nível 2 (N2):** atendimento técnico intermediário, voltado à resolução de incidentes e solicitações não solucionadas pelo N1;
- **Nível 3 (N3):** atendimento especializado, voltado à infraestrutura crítica, ambientes complexos e soluções de segurança da informação.

Considerando o porte da operação e o número de usuários atendidos, aproximadamente 1600 servidores entre estatutários, comissionados e temporários os atendimentos deverão observar os seguintes regimes:

- **N1 e N2 – Atendimento Regular:** segunda a sexta-feira, das 7h às 19h; e aos sábados, das 7h às 13h;
- **N1 e N2 – Atendimento Extraordinário 24x7x365:** para serviços críticos, unidades com funcionamento ininterrupto (ex: saúde), e atendimento a autoridades administrativas sempre que houver demanda;
- **N3 e Serviços Especializados de Segurança – Atendimento 24x7x365:** com foco na integridade, disponibilidade e estabilidade dos serviços estratégicos, incluindo domínios, backups, antivírus, SIEM, análise de vulnerabilidades e outros.

Todas as soluções contratadas deverão contar com suporte técnico integral, de forma a assegurar o pleno funcionamento da estrutura de TI da Prefeitura, a resiliência da infraestrutura crítica e a conformidade com as normas legais aplicáveis, especialmente quanto à proteção de dados, continuidade dos serviços públicos e segurança da informação.

**Processo de Atendimento Técnico**
Todo o processo de atendimento será executado por meio da Central de Serviços de TI da contratada, que atuará como ponto único de contato (SPoC – Single Point of Contact) para os usuários da Administração Pública. Essa Central será responsável por garantir o funcionamento contínuo do parque tecnológico da Prefeitura, bem como a manutenção dos serviços de tecnologia implantados. O atendimento será estruturado em múltiplos níveis, com escalonamento técnico conforme a natureza e a complexidade das demandas.

**Atendimento Nível 1 (N1)**
A equipe de suporte N1 será responsável por recepcionar, registrar, classificar e, quando aplicável, solucionar as solicitações iniciais recebidas pelos canais disponíveis: WhatsApp corporativo, telefone institucional, e-mail institucional ou outros definidos no ITSM. Caberá à equipe o tratamento de demandas de baixa complexidade, bem como o encaminhamento adequado ao N2 ou a fornecedores externos. Todos os chamados deverão ser registrados na ferramenta ITSM homologada, garantindo rastreabilidade e auditoria, inclusive para atendimentos realizados por telefone ou aplicativo de mensagens.

**Atendimento Nível 2 (N2)**
A equipe de N2 atuará nas demandas não solucionadas no N1 ou que exijam maior profundidade técnica. Isso inclui erros sistêmicos, suporte a softwares corporativos, permissões e configurações intermediárias, integração de sistemas e apoio técnico a redes e domínios. O atendimento será prestado preferencialmente de forma remota, com obrigação de deslocamento presencial sem custo adicional em casos de não resolução remota, respeitando os prazos pactuados nos SLAs.

**Atendimento Nível 3 (N3)**
O Nível 3 será composto por especialistas técnicos, com responsabilidade sobre incidentes críticos, infraestrutura, ambientes virtualizados e sistemas complexos. Atuarão em reconfigurações de firewall, Active Directory, VPN, políticas de segurança e incidentes de maior impacto. Também realizarão suporte avançado à infraestrutura e às soluções contratadas, além de coordenar ações de investigação, mudança e resolução de problemas sistêmicos. O primeiro atendimento será remoto, com deslocamento presencial quando necessário, sem ônus para a contratante.

**Serviços Especializados em Segurança da Informação**
Os serviços especializados em segurança da informação deverão ser executados por equipe técnica com experiência comprovada em cibersegurança e gestão de riscos. Estão incluídas atividades como elaboração de políticas e procedimentos de segurança, resposta a incidentes, configuração de ferramentas como antivírus, backup, SIEM, controle de acesso, gestão de vulnerabilidades e suporte às soluções de segurança implantadas. Esta equipe operará em regime 24x7x365, com responsabilidade plena pela integridade e continuidade das soluções de segurança contratadas.

**Governança de Serviços e Processos ITIL**
O processo de atendimento deverá seguir as boas práticas de governança de TI, com base nos princípios do ITIL. Deverão ser implantados e mantidos os processos de Gerenciamento de Incidentes, Requisições, Problemas e Mudanças, com apoio de uma CMDB (base de dados de configuração) e um Catálogo de Serviços atualizado, definindo o escopo, SLAs, prioridades e padrões operacionais.

A contratada deverá implementar mecanismos automatizados de pesquisa de satisfação, aplicados ao final de cada chamado, com exigência contratual de cumprimento de índices mínimos de avaliação. Todos os níveis de suporte (N1, N2, N3 e Especialistas em Segurança) deverão atuar conforme os SLAs definidos no TR, com prazos de atendimento (TA) e solução (TS) por criticidade.

Cabe à contratada realizar o planejamento, o dimensionamento e a precificação adequados da equipe técnica, dos processos e das ferramentas utilizadas, considerando o regime de operação contínua 24x7x365, a criticidade das áreas atendidas e a responsabilidade sobre todo o fluxo técnico descrito neste item.

**Serviços Técnicos de Suporte – Nível 1 e Nível 2**

Os serviços de atendimento técnico nos níveis 1 e 2 compreendem um conjunto de atividades executadas no âmbito da Central de Serviços de TI da contratada, com o objetivo de atender integralmente às demandas dos usuários da Prefeitura Municipal. A execução se dará por equipe técnica qualificada, com uso de ferramenta ITSM para registro e rastreamento dos chamados, observando os prazos estabelecidos nos Acordos de Nível de Serviço (SLA) contratados. O atendimento será realizado predominantemente de forma remota, com deslocamento presencial sempre que necessário, sem ônus adicional para a contratante. A contratada será responsável por manter equipe compatível com o volume de chamados, a criticidade dos serviços e a complexidade dos atendimentos previstos neste Termo de Referência.

**Serviços Técnicos de Suporte – Nível 1 (N1)**

A equipe N1 será responsável por atender a todas as solicitações iniciais dos usuários, realizando triagem, classificação, atendimento direto ou encaminhamento, de acordo com o tipo e a complexidade da demanda. O atendimento será realizado de forma remota por meio da Central de Serviços da contratada, com possibilidade de encaminhamento a fornecedores, escalonamento ao N2, N3 ou encerramento com resolução. As seguintes atividades deverão ser executadas pela equipe de Nível 1:

| |
|---|
| Atendimento multicanal (telefone, WhatsApp, e-mail), com registro obrigatório de todos os chamados na ferramenta ITSM; |
| Tipificação e priorização dos chamados (incidente, requisição, criticidade, urgência e impacto); |
| Encaminhamento e acompanhamento de chamados junto a fornecedores externos, como operadoras de internet, fornecedores de equipamentos e prestadores de software; |
| Acompanhamento de status, SLA e encerramento dos chamados; |
| Aplicação de procedimentos padrão para coleta de informações e validação inicial do problema reportado. |
| Instalação, reinstalação e atualização de sistemas operacionais Windows e Linux Desktop; |
| Instalação e configuração de pacote Microsoft Office, navegadores, Adobe Reader, Java, WinRAR, antivírus e demais aplicativos homologados pela Prefeitura; |
| Configuração de softwares e ferramentas específicas utilizadas pelos órgãos municipais (ex: sistemas administrativos, tributários, educacionais ou saúde); |
| Apoio remoto para instalação e reinstalação de ferramentas do dia a dia dos usuários. |
| Criação e manutenção de contas de usuários na rede, em diretório ativo (AD); |
| Configuração de e-mails institucionais, acesso à internet, mapeamento de pastas, drives e impressoras de rede; |
| Suporte à alteração de senhas, desbloqueio de contas e problemas de login; |
| Liberação de cotas de impressão, armazenamento e controle básico de permissões. |
| Instalação e configuração de impressoras locais e de rede (inclusive multifuncionais); |
| Resolução de falhas de impressão, substituição de drivers, limpezas lógicas (spooler, fila, buffer); |
| Diagnóstico e limpeza lógica de estações de trabalho: remoção de arquivos temporários, verificação de inicialização lenta, verificação de integridade básica do sistema; |
| Execução de análises iniciais de desempenho, uso de CPU, memória e disco; |
| Encerramento forçado de processos ou serviços travados; |
| Atualização manual ou automatizada de drivers. |
| Apoio à instalação e atualização de ferramentas de gerenciamento de desktop e antivírus; |
| Aplicação de patches e atualizações do sistema operacional e softwares de uso comum; |
| Execução de scripts de login, automações de inicialização, scripts de limpeza, mapeamento de unidades; |

| |
|---|
| Execução de procedimentos padronizados de correção e manutenção. |
| Identificação de falhas ou incidentes que demandem atuação de Nível 2 (N2) ou Nível 3 (N3), com encaminhamento e escalonamento correto via ITSM; |
| Apoio à coleta de informações para subsidiar o N2/N3, incluindo logs, prints, arquivos de erro e histórico do problema. |
| Atendimento a requisições de TI consideradas simples, como: |
| Suporte a videoconferência e apresentação; |
| Orientações básicas de uso de sistemas; |
| Acompanhamento remoto com o usuário para instruções e validações; |
| Registro completo de todas as atividades e feedback do usuário no fechamento do chamado. |

Ao final de cada atendimento, será obrigatório o registro completo da atividade no sistema ITSM, com rastreabilidade, SLA e evidências associadas. Todos os atendimentos, independentemente do canal utilizado, deverão seguir esse procedimento para fins de medição contratual e controle da execução.

**Serviços Técnicos de Suporte – Nível 2 (N2)**
A equipe N2 será acionada sempre que a equipe N1 não for capaz de resolver a demanda, seja pela complexidade técnica ou por limitações operacionais. O Nível 2 será responsável por atuar em solicitações que exijam maior profundidade técnica, configurando, ajustando ou diagnosticando componentes de infraestrutura, sistemas, redes e dispositivos com maior criticidade ou personalização. As seguintes atividades deverão ser executadas pela equipe de Nível 2:

| |
|---|
| Recebimento de chamados escalonados pelo N1, com reclassificação, categorização e aprofundamento técnico do problema; |
| Atendimento remoto com possibilidade de deslocamento presencial para resolução de chamados em locais críticos ou isolados; |
| Apoio à identificação de falhas mais complexas que exigem acesso administrativo ao sistema operacional ou serviços de rede. |
| Instalação, configuração e manutenção básica de servidores locais ou unidades remotas da Prefeitura; |
| Configuração de serviços como DHCP, DNS, compartilhamentos de rede e autenticação local; |
| Aplicação de boas práticas de segurança e controle de permissões; |
| Apoio em atualizações de sistemas operacionais e aplicação de patches críticos em servidores de pequeno porte; |
| Suporte à instalação de serviços locais em ambientes remotos (ex: impressoras de rede, pastas compartilhadas, scanners, entre outros). |
| Apoio à instalação, configuração e troubleshooting de sistemas corporativos de média complexidade, como ERPs, sistemas administrativos, educacionais, financeiros e outros; |
| Suporte técnico a sistemas legados, aplicativos específicos de secretarias e sistemas com dependências locais; |
| Intervenções em serviços em segundo plano, serviços travados, banco de dados locais e logs de erro. |
| Intervenções em rede local (LAN): teste e substituição de cabos, porta de switch, ponto de rede; |
| Análise de conectividade básica: gateway, IP fixo/dinâmico, testes de ping, DNS, latência e rota; |
| Verificação de conflitos de IP e degradação de link interno; |
| Configuração de impressoras em rede, IPs fixos, reservas no DHCP e compartilhamento. |
| Suporte avançado a estações com problemas persistentes; |
| Restauração de imagem de sistema, recuperação de perfil corrompido, reinstalação de drivers; |
| Avaliação e resolução de problemas de desempenho e falhas recorrentes; |
| Execução de limpeza avançada do sistema (desfragmentação, verificação de disco, remoção de conflitos de drivers). |
| Realização de inventário completo de hardware e software com atualização do CMDB; |
| Auditoria de estações, configurações, uso de software não homologado e controle de compliance; |
| Reinstalação ou atualização de ferramentas de segurança (antivírus, EDR, filtro de conteúdo); |
| Apoio à verificação de incidentes de segurança de menor complexidade, como infecções isoladas ou suspeitas de acesso indevido. |

| |
|---|
| Apoio direto ao N1 na execução de atividades técnicas mais delicadas (ex: alterações no registro do Windows, configuração de políticas locais); |
| Diagnóstico aprofundado de falhas críticas que exigem documentação e preparo técnico para escalonamento ao N3; |
| Encaminhamento adequado ao N3, com registro estruturado do problema, logs e histórico de tentativas de resolução. |
| Encaminhamento adequado a fornecedores do ecossistema de TI da Prefeitura, com registro estruturado do problema, logs e histórico de tentativas de resolução. |

Assim como no Nível 1, todas as ações realizadas pela equipe de N2 deverão ser registradas integralmente no sistema ITSM, vinculadas ao chamado correspondente, com detalhamento técnico da execução, cumprimento dos prazos estabelecidos em SLA e evidências de atendimento para fins de auditoria e validação contratual.

**Serviços Técnicos de Suporte – Nível 3 (N3)**
A equipe de Suporte Técnico Nível 3 será responsável por atividades operacionais e táticas de alta complexidade, com foco na sustentação e evolução da infraestrutura crítica de tecnologia da Prefeitura Municipal. Sua atuação tem caráter preventivo e corretivo, abrangendo servidores, redes, bancos de dados, virtualização, segurança da informação e ambientes híbridos, com o objetivo de garantir a disponibilidade, integridade e desempenho contínuo dos serviços de TI essenciais à Administração Pública.

Essa equipe será composta por especialistas técnicos com experiência comprovada em ambientes de missão crítica, devendo atuar de forma integrada com as equipes de N1 e N2 e assumir total responsabilidade técnica sobre os ambientes sensíveis e estratégicos da contratante. As seguintes atividades deverão ser executadas pela equipe de Nível 3:

| |
|---|
| **Administração de Servidores e Ambientes Virtuais** |
| Instalação, configuração e suporte a servidores físicos e virtuais (Windows, Linux, Hypervisores); |
| Gestão de recursos computacionais: memória, CPU, disco, rede; |
| Apoio à administração de ambientes de virtualização e storages; |
| Atualizações e manutenção de sistemas operacionais em produção e homologação (feito mensalmente). |
| **Gestão de Redes e Conectividade** |
| Administração de redes locais (LAN), redes de longa distância (WAN), sub-redes e VLANs; |
| Configuração e gerenciamento de ativos de rede: switches, firewalls, roteadores; |
| Suporte à configuração de protocolos como OSPF, BGP, NAT, VPNs e ACLs; |
| Monitoramento da disponibilidade de circuitos e links de comunicação. |
| **Administração de Bancos de Dados** |
| Apoio à administração de bancos como MySQL e PostgreSQL; |
| Configuração de replicação, tuning de desempenho e monitoramento de crescimento; |
| Gestão de rotinas de backup e restauração de bases de dados. |
| **Segurança da Informação** |
| Aplicação das políticas de segurança da contratante; |
| Execução de análise de vulnerabilidades nos servidores e estações (no mínimo trimestral) |
| Detecção, resposta e correções a vulnerabilidades encontradas, falhas e ataques; |
| Configuração e suporte para solução de antivírus e EDR; |
| Monitoramento de logs, geração de alertas e automação de respostas; |
| Criação de *jobs* de verificação, correção e geração de evidências de conformidade; |
| Execução de inteligência de ameaças através da análise de logs correlacionados com a ferramenta de SIEM. |
| Definição e aplicação de baselines mínimas de segurança para servidores e estações; |
| **Gestão de Monitoramento e Saúde do Ambiente** |
| Coleta de indicadores de disponibilidade e performance por meio de ferramentas de monitoramento e SIEM; |
| Monitoramento contínuo de alarmes e eventos gerados por sistemas, servidores e ativos; |
| Execução de rotinas diárias e semanais para manutenção da “saúde do ambiente”: patches, hotfixes, limpeza de logs, verificação de integridade de backups e conectividade; |
| Acompanhamento e garantia da execução das políticas de backup e recuperação de desastres da contratante. |

| |
|---|
| **Inventário e CMDB** |
| Inventário e auditoria de ativos de infraestrutura (servidores, redes, storages, etc.); |
| Registro, atualização e relacionamento dos componentes críticos no banco de dados de configuração (CMDB). |
| **Documentação, Suporte Estratégico e Integração** |
| Apoio técnico contínuo às equipes de N1 e N2, prestando consultoria, tirando dúvidas e participando de resoluções conjuntas; |
| Elaboração de procedimentos operacionais padrão (POPs), guias técnicos, fluxos e manuais de atendimento; |
| Apoio na definição e atualização do Catálogo de Serviços da TI da Prefeitura; |
| Participação ativa em processos de melhoria contínua e controle de mudanças e contribuição com o planejamento de capacidade e disponibilidade dos serviços de TI (mensal). |

Todas as ações da equipe N3 deverão ser registradas no sistema ITSM utilizado na Central de Serviços, com histórico completo da execução, vinculação ao chamado original, evidências técnicas e cumprimento dos Acordos de Nível de Serviço (SLA). A equipe deverá operar sob regime 24x7x365, garantindo cobertura contínua dos ambientes críticos e suporte especializado à infraestrutura da Prefeitura, sem ônus adicional para a contratante em caso de necessidade de atendimento presencial.

**Serviços Especializados em Segurança da Informação**
A execução dos serviços especializados em segurança da informação será de responsabilidade de uma equipe técnica altamente qualificada, com competências para atuar nos níveis estratégico, tático e operacional, com foco na preservação da confidencialidade, integridade e disponibilidade dos ativos e informações da Prefeitura Municipal. Essa equipe atuará como camada transversal de suporte a toda a operação de TI, sendo responsável por planejar, implementar, monitorar e aperfeiçoar continuamente os controles de segurança da informação, conforme as boas práticas das normas ISO/IEC 27001, NIST CSF, CIS Controls e legislação vigente, como a LGPD.

As seguintes atividades deverão ser executadas pela equipe de serviços especializados em segurança da informação:

| |
|---|
| **Governança, Políticas e Conformidade** |
| Elaboração e revisão de políticas, normas e procedimentos de segurança da informação, incluindo: |
| Política de Backup Corporativa; |
| Plano de Continuidade de Negócios e Recuperação de Desastres (BCP/DRP); |
| Política de Gestão de Incidentes de Segurança; |
| Política de Uso Aceitável de Recursos de TI; |
| Política de Controle e Gestão de Acessos; |
| Política de Segurança para Acesso à Internet e Conteúdo; |
| Política de Senhas; |
| E outras; |
| Condução de gap analysis com base na ISO/IEC 27001 e outros frameworks aplicáveis; |
| Produção de relatórios de conformidade e riscos de segurança, com recomendações práticas para adequação do ambiente; |
| Acompanhamento de indicadores e geração de relatórios periódicos de maturidade em segurança. |
| **Apoio à Contratações e Due Diligence** |
| Apoio técnico na elaboração, revisão e análise de termos de referência e editais de soluções de TI, com foco em requisitos de segurança da informação; |
| Avaliação de fornecedores de soluções de TI sob a ótica da segurança, incluindo análise de risco, cláusulas contratuais, níveis de serviço e conformidade; |
| Condução de due diligence técnica e contratual em fornecedores de soluções críticas (cloud, SaaS, software embarcado, serviços gerenciados); |
| Avaliação da segurança de ambientes em nuvem, com foco em responsabilidade compartilhada e integridade da prestação do serviço. |
| **Segurança Técnica, Projetos e Automação** |
| Implantação, gestão e sustentação de novas tecnologias de segurança da informação, priorizando soluções baseadas em software livre; |
| Execução de projetos técnicos e consultoria especializada na área de segurança cibernética; |

| |
|---|
| Integração de soluções com Active Directory / LDAP, garantindo centralização de autenticação, aplicação de políticas e rastreabilidade; |
| Criação de scripts e automações para controle, correção e reforço da segurança da infraestrutura; |
| Apoio na implementação de soluções como: |
| Single Sign-On (SSO); |
| Gestão segura de senhas e cofres digitais; |
| Ferramentas de controle de conteúdo web e DLP; |
| Correlação de logs e análise comportamental. |
| E outras |
| **Suporte Avançado e Resolução de Incidentes** |
| Resolução de incidentes críticos de segurança da informação, com atuação coordenada com as equipes N3 e com fornecedores estratégicos; |
| Suporte direto a soluções que exijam análise profunda e multidisciplinar, não solucionadas por outras equipes; |
| Apoio e orientação técnica às equipes de N1, N2 e N3 quanto a diretrizes de segurança, procedimentos de resposta e recomendações de hardening; |
| Participação em reuniões de crise e resposta a incidentes que envolvam vazamentos, ataques ou falhas estruturais; |
| Geração de relatórios técnicos e gerenciais após incidentes, com lições aprendidas e planos de mitigação. |
| **Inovação e Melhoria Contínua** |
| Pesquisa, prospecção e recomendação de novas tecnologias, ferramentas e controles de segurança da informação; |
| Estudo de viabilidade e acompanhamento de tendências de mercado, incluindo LGPD, Zero Trust, autenticação multifator e proteção de endpoints; |
| Implantação de programas contínuos de melhoria, com foco na evolução da maturidade de segurança institucional. |

A equipe de segurança deverá atuar de forma integrada com as demais equipes técnicas da contratada, prestando apoio à governança institucional de TI e garantindo a conformidade com os princípios de segurança, gestão de riscos, continuidade de negócios e proteção de dados. Todas as atividades deverão ser devidamente registradas no sistema ITSM, com rastreabilidade, controle de SLA e geração de relatórios para validação técnica e acompanhamento contratual. O atendimento deverá ocorrer em regime 24x7x365, com capacidade de resposta a incidentes de alta complexidade, ações corretivas e apoio à gestão estratégica da segurança da informação da Administração.

**Gerenciamento Técnico e Operacional do Contrato**
A contratada deverá designar formalmente um(a) profissional de perfil técnico-sênior para atuar como Gerente Técnico do Contrato, sendo este o responsável por assegurar a execução plena dos serviços contratados, garantir o cumprimento do objeto contratual e atuar como interlocutor direto junto à equipe técnica da Prefeitura Municipal.

Esse profissional será o ponto focal da contratada para todas as tratativas operacionais, devendo coordenar as equipes de N1, N2, N3 e de Serviços Especializados de Segurança da Informação, bem como acompanhar o desempenho técnico, a gestão dos projetos e a entrega dos serviços conforme prazos, escopos e indicadores acordados.

Suas responsabilidades incluem:
- Acompanhamento da execução dos serviços, observância dos SLAs e tratamento de exceções;
- Consolidação e envio dos relatórios operacionais e técnicos com a periodicidade estabelecida – mensal e semanal;
- Participação ativa em auditorias técnicas, reuniões periódicas de acompanhamento e eventos de transição contratual;
- Apoio à implantação de novos processos e ferramentas de atendimento, quando aplicável;
- Coordenação das ações de melhoria contínua com base em indicadores e feedbacks dos usuários.

O Gerente Técnico deverá estar permanentemente disponível para contato com a fiscalização do contrato, presencialmente ou remotamente, conforme definido pela Prefeitura. É obrigatória a participação em reuniões

semanais e mensais de acompanhamento, com apresentação dos relatórios de atendimento e avaliação dos níveis de serviço, podendo ser requisitada a presença física, na sede da Contratante, mediante aviso prévio de até 72 horas.

Em caso de encerramento contratual, esse profissional deverá liderar o processo de transição técnica, garantindo a entrega organizada da base de conhecimento, documentos operacionais e relatórios necessários para continuidade dos serviços.

O descumprimento das obrigações associadas ao Gerente Técnico ou a ausência desse profissional sem justificativa poderá ser caracterizado como falha na execução contratual, com os devidos registros pela fiscalização.

**Modelo de Precificação e Forma de Execução dos Serviços**
A execução dos serviços contratados será realizada por meio de dois modelos complementares, conforme a natureza e o perfil da demanda:

**Serviços Continuados**
Os serviços de suporte técnico classificados como Nível 1 (N1), Nível 2 (N2), Nível 3 (N3) e o Gerenciamento Técnico do Contrato serão executados de forma continuada e ininterrupta, com faturamento mensal fixo. A execução ocorrerá em regime remoto e presencial, conforme as necessidades operacionais e os níveis de criticidade, obedecendo às escalas e coberturas definidas neste Termo de Referência. Esses serviços serão prestados com equipe dedicada, estrutura de atendimento supervisionado, SLAs pactuados e rastreabilidade integral via sistema ITSM.

**Serviços Especializados de Segurança da Informação**
Devido à sua natureza estratégica, consultiva e sob demanda, estes serviços serão prestados por meio de banco de horas técnicas previamente contratadas (UST). A execução será condicionada à autorização formal da contratante e à apresentação de planos de trabalho, conforme os casos de uso descritos neste Termo. O consumo será controlado por registros formais no sistema ITSM e relatórios de execução, com cobrança proporcional ao uso, sem obrigatoriedade de consumo mensal fixo.

A seguir, apresenta-se o quadro-resumo com as principais características dos serviços por nível de suporte, forma de execução e modelo de precificação:

| Nível de Serviço | Descrição Geral | Forma de Execução | Abrangência Técnica | Modelo de Precificação |
|---|---|---|---|---|
| **Gerenciamento Técnico do Contrato** | Coordenação geral das equipes e do contrato, gestão de SLAs, projetos, relatórios e reuniões com a Prefeitura. | Presencial e remoto, conforme necessidade | Governança, relatórios, reuniões mensais, transição de conhecimento, gestão da execução contratual. | Faturamento mensal fixo (serviço contínuo) |
| **Nível 1 (N1)** | Atendimento inicial ao usuário, triagem, resolução de chamados simples, registro e encaminhamento. | Remoto, modalidade 24x7 | Estações de trabalho, sistemas básicos, antivírus, requisições e incidentes de baixo impacto. | Faturamento mensal fixo (serviço contínuo) |
| **Nível 2 (N2)** | Atendimento técnico intermediário, resolução de | Remoto e Presencial, modalidade 24x7 | Suporte técnico mais profundo, configuração de sistemas, | Faturamento mensal fixo (serviço contínuo) |

| Nível de Serviço | Descrição Geral | Forma de Execução | Abrangência Técnica | Modelo de Precificação |
|---|---|---|---|---|
| | chamados não solucionados pelo N1. | | servidores remotos, inventário, atualizações. | |
| **Nível 3 (N3)** | Suporte técnico especializado para infraestrutura crítica e resolução de incidentes complexos. | Remoto e Presencial, modalidade 24x7 | Servidores, redes, banco de dados, virtualização, backup, segurança, monitoramento e continuidade de negócios. | Faturamento mensal fixo (serviço contínuo) |
| **Serviços Especializados de Segurança** | Atuação estratégica, tática e operacional em segurança da informação, com foco em governança e conformidade. | Sob demanda, via banco de horas. Remoto ou presencial | Políticas, ISO 27001, due diligence, projetos, auditorias, gap analysis, automação, suporte técnico especializado. | Banco de horas técnicas sob demanda |

**Meios de Contato com a Central de Serviços**

A contratada deverá disponibilizar, de forma ininterrupta (24x7x365), pelo menos quatro canais distintos de contato para que qualquer servidor da Prefeitura possa abrir chamados técnicos junto à Central de Serviços. Os meios mínimos obrigatórios incluem:

- WhatsApp corporativo;
- Telefone institucional;
- E-mail institucional;
- Portal da ferramenta de ITSM;
- Outros meios adicionais poderão ser acordados entre as partes durante a vigência contratual.

Todos os canais deverão estar permanentemente operacionais, com acesso direto a profissionais capacitados da equipe técnica, assegurando o cumprimento dos prazos de primeiro atendimento (TA) definidos nos Acordos de Nível de Serviço.

Os atendimentos realizados por qualquer canal deverão ser integralmente auditáveis, com os seguintes requisitos obrigatórios:

- Registro automático ou manual da data e hora de início do atendimento, tempo de resposta do primeiro atendente e histórico completo da tratativa;
- Gravação e armazenamento de chamadas telefônicas, com acesso disponível para fins de auditoria;
- Preservação integral, rastreável e não editável de conversas realizadas via WhatsApp, sendo vedada qualquer exclusão de mensagens;
- Registro encadeado e completo de e-mails trocados, devidamente integrados à ferramenta ITSM.

Em atendimentos iniciados por meios não automatizados (como telefone ou WhatsApp), o registro no sistema ITSM deverá ser realizado antes de qualquer ação técnica, garantindo rastreabilidade desde o primeiro contato.

O descumprimento dessas exigências poderá ser considerado não conformidade contratual, com impactos na apuração de indicadores de desempenho e na fiscalização da execução do contrato.

**Acionamento de Prestadores Externos**

Sempre que, no curso do atendimento técnico, for identificado que a origem ou a solução de uma demanda está vinculada a fornecedores externos da Prefeitura, caberá à contratada realizar o acionamento imediato e acompanhar integralmente a tratativa até sua conclusão, independentemente do nível de suporte envolvido (N1, N2, N3 ou Serviços Especializados em Segurança da Informação).

Entre os fornecedores que poderão ser acionados, incluem-se, entre outros:

- Provedores de link de internet;
- Empresas responsáveis pela interconexão entre unidades da Prefeitura;
- Fornecedores de locação de equipamentos de TI;
- Fornecedores de sistemas, aplicações em nuvem e plataformas SaaS;
- Parceiros tecnológicos definidos contratualmente pela Prefeitura.

O acionamento deverá seguir os canais e procedimentos definidos no Termo de Referência e/ou contrato de cada fornecedor. Caso o fornecedor utilize uma ferramenta própria de gestão de tickets, a contratada deverá registrar a solicitação diretamente nessa plataforma, obedecendo aos fluxos estabelecidos.

A partir da abertura do chamado, a Central de Serviços da contratada será a responsável exclusiva por seu acompanhamento, devendo monitorar prazos, interagir tecnicamente com o fornecedor, cobrar retorno e manter o usuário da Prefeitura informado quanto à evolução da tratativa.

Toda a gestão desse atendimento externo, incluindo prazos, status, interações e conclusão, deverá ser documentada no sistema ITSM da Prefeitura, garantindo a rastreabilidade completa da ocorrência.

Nos casos em que o fornecedor ultrapassar os prazos estabelecidos em seu contrato, a contratada deverá registrar o fato nos relatórios periódicos, informando os impactos operacionais causados e as medidas tomadas. É de responsabilidade da contratada conhecer previamente os canais, SLAs, procedimentos e condições contratuais dos fornecedores, atuando como facilitadora e integradora na gestão técnica e operacional da infraestrutura de TI da Prefeitura.

**Equipamentos, Ferramentas e Infraestrutura Operacional da Contratada**

É de responsabilidade exclusiva da contratada prover, manter e garantir o pleno funcionamento de todos os equipamentos, softwares, ferramentas, acessos e demais recursos técnicos necessários à execução dos serviços contratados, conforme os requisitos definidos neste Termo de Referência.

Todos os profissionais envolvidos na prestação dos serviços deverão dispor de recursos adequados e compatíveis com suas funções, sendo obrigatória a disponibilização, pela contratada, de:

- Notebooks, desktops, dispositivos móveis e acessórios em conformidade com as demandas técnicas;
- Licenciamento regular de todos os softwares utilizados, com comprovação de conformidade legal;
- Ferramentas de acesso remoto seguras, homologadas e com autenticação forte;
- Conectividade de internet com banda adequada, estabilidade e alta disponibilidade;
- Ferramentas de colaboração, comunicação e gestão compatíveis com os níveis de suporte e os padrões operacionais adotados.

Nos casos de atendimento sob regime de plantão ou operação contínua (24x7), inclusive com deslocamento presencial de profissionais às unidades da Prefeitura, a contratada deverá garantir:

- Internet móvel de qualidade para execução de atividades em campo;
- Equipamentos móveis prontos para uso (ex: notebooks, tablets, roteadores portáteis);
- Redundância mínima de equipamentos críticos (ex: notebooks de reserva, carregadores, pontos de acesso, links alternativos);
- Backup de configurações, acessos e ferramentas essenciais, para continuidade da operação em caso de falhas.

Todos os equipamentos e soluções utilizadas devem estar atualizados, licenciados e atender aos princípios de segurança da informação, incluindo:

- Autenticação multifator ou forte para sistemas críticos;
- Armazenamento seguro de dados técnicos e registros operacionais;
- Garantia de que nenhuma ferramenta ou equipamento comprometerá a confidencialidade, integridade ou disponibilidade dos dados da administração pública.

A contratada poderá ser auditada a qualquer tempo quanto aos recursos utilizados na prestação dos serviços, devendo comprovar licenciamento, aderência técnica e conformidade com as boas práticas exigidas neste instrumento. O não atendimento a esses requisitos poderá configurar **não conformidade contratual**, com repercussões nos indicadores de desempenho, nos relatórios de fiscalização e na responsabilização contratual.

**Base de Conhecimento e Transferência de Conhecimento**

Durante toda a vigência contratual, a contratada será responsável pela construção, atualização e manutenção contínua da Base de Conhecimento (Knowledge Base) da Prefeitura Municipal, integrando os principais componentes da estrutura de governança de TI. Essa base deverá estar devidamente estruturada dentro da ferramenta oficial de ITSM da Administração, e deverá conter, no mínimo:

- Catálogo de Serviços: descrição clara e atualizada de todos os serviços prestados, suas categorias, subcategorias, SLAs e critérios de prioridade;
- CMDB – Base de Itens de Configuração: inventário dos ativos de TI e seus relacionamentos, com histórico de alterações, incidentes, intervenções e responsáveis;
- Base de Conhecimento Operacional: procedimentos, manuais, scripts, fluxos de atendimento, soluções aplicadas, resoluções de problemas e recomendações para melhoria contínua;
- Histórico de Incidentes e Soluções: documentação estruturada de falhas relevantes, análise de causa raiz e ações corretivas aplicadas;
- Base de Erros Conhecidos (Known Errors): mapeamento de falhas recorrentes e respectivas soluções de contorno ou correções definitivas.

Essa base deverá estar integrada à ferramenta ITSM da Prefeitura, sendo obrigatoriamente acessível às equipes de N1, N2, N3 e de serviços especializados. Deverá permitir:

- Controle de versões e validação por responsáveis técnicos;
- Rastreabilidade de todas as alterações realizadas;
- Integração com os processos de gerenciamento de incidentes, problemas, mudanças e ativos;
- Atualização contínua, acompanhando a evolução do ambiente de TI, das soluções implantadas e dos processos da Administração.

**Transferência de Conhecimento em Caso de Encerramento Contratual**

No caso de encerramento contratual, a contratada deverá realizar a transferência formal e completa de toda a base de conhecimento, incluindo ativos documentais, relatórios, registros e demais materiais técnicos gerados ao longo da execução do contrato.

A entrega deverá contemplar:

- Documentação técnica completa, incluindo manuais, inventários, scripts, registros de alterações e históricos de atendimento;
- Relatório final de transição contendo os tópicos abordados, responsáveis envolvidos e confirmação de entrega por parte da contratante.

Essa medida tem como objetivo assegurar a continuidade operacional da área de tecnologia da Prefeitura, evitando perda de informação crítica, falhas de transição ou interrupções indesejadas na prestação dos serviços.

**Campanhas de Conscientização e Apoio à Comunicação Interna**

A contratada deverá apoiar a Prefeitura na promoção da Central de Serviços de TI, dos novos procedimentos operacionais e das políticas de segurança da informação, por meio de ações conjuntas de comunicação institucional, desenvolvidas em colaboração com os setores de Comunicação e de Tecnologia da Informação da Administração.

Esse apoio incluirá, no mínimo:

- Participação ativa na elaboração de materiais de comunicação como cartilhas, folders, apresentações, vídeos explicativos e e-mails informativos;
- Apoio técnico na explicação dos fluxos de atendimento, canais de suporte, procedimentos de abertura de chamados e SLAs definidos;
- Apoio na divulgação interna de mudanças estruturais implantadas, como a adoção do sistema ITSM, novos níveis de suporte e novas soluções de TI;
- Contribuição para a conscientização dos usuários quanto às boas práticas de uso dos serviços de TI, incentivando o registro correto de solicitações e o uso adequado dos canais oficiais;
- Apoio na comunicação das políticas de segurança da informação, reforçando a cultura institucional de segurança, responsabilidade no uso dos recursos tecnológicos e adesão às normas vigentes.

As ações deverão ser planejadas, executadas e avaliadas de forma colaborativa, com foco na adesão dos servidores ao novo modelo de atendimento, na clareza da comunicação interna e na promoção da confiança e fluidez na utilização dos serviços da Central de Serviços.

**Pesquisa de Satisfação do Atendimento**

A contratada deverá implantar e manter um mecanismo automatizado de pesquisa de satisfação vinculada aos atendimentos realizados, com foco na transparência, na melhoria contínua e no controle de qualidade dos serviços prestados pela Central de Serviços.

**Requisitos obrigatórios**

- A pesquisa deverá ser disparada automaticamente pela ferramenta de ITSM assim que o chamado for encerrado;
- Para os atendimentos via WhatsApp, o envio da pesquisa deverá ocorrer imediatamente após o encerramento da conversa;
- O modelo de avaliação adotado será em escala de 1 a 5 estrelas, considerando:
  - Notas 1 a 3: insatisfatórias;
  - Notas 4 e 5: satisfatórias;
- Para notas de 1 a 3, o sistema de atendimento via whatsapp deverá obrigatoriamente apresentar a pergunta: “O que poderia ser melhorado neste atendimento?”, com campo de resposta obrigatória;
- Todas as avaliações deverão ser registradas e associadas aos respectivos chamados no ITSM ou na ferramenta de WhatsApp utilizada.

**Tratamento e acompanhamento das avaliações**

- Toda avaliação com nota 1 a 3 deverá ser reavaliada pela liderança da equipe da contratada;
- Será obrigatório o contato ativo com o usuário insatisfeito para entender o problema, validar a crítica e propor ações corretivas;
- A contratada deverá elaborar:
  - Relatório semanal contendo todos os atendimentos insatisfatórios e as providências adotadas;
  - Relatório mensal consolidado com análise quantitativa e qualitativa das avaliações;
- Os relatórios serão enviados à fiscalização do contrato e servirão como base de avaliação de desempenho.

**Metas de resposta e satisfação**

- Nos três primeiros meses será apurado o índice médio de satisfação para definir metas progressivas;
- Após a fase inicial, será exigido:
  - Índice mínimo de satisfação: 90% (média ponderada);
  - Participação mínima nas pesquisas: 25% dos chamados, sendo desejável alcançar 50%;
- A contratada deverá adotar ações permanentes de incentivo ao engajamento dos usuários na pesquisa.

**Avaliação contratual**

A satisfação dos usuários será considerada indicador relevante para avaliação do contrato, podendo inclusive ser utilizada como critério adicional na eventual Prova de Conceito (PoC). O não cumprimento das metas mínimas de satisfação, bem como a ausência de ações corretivas diante de avaliações negativas, será considerado descumprimento contratual, passível de sanções conforme os termos pactuados.

**Acordo de Nível de Serviço (SLA)**

O Acordo de Nível de Serviço (SLA) estabelece os prazos máximos para o atendimento e solução de demandas recebidas pela Central de Serviços da contratada, conforme critérios de classificação e prioridade definidos neste Termo de Referência. Os SLAs servirão de base para apuração de indicadores de desempenho, elaboração de relatórios, aplicação de glosas e avaliação da qualidade dos serviços prestados.

**Definições**

- **Tempo de Atendimento (TA):** tempo entre o registro do chamado e a **primeira tratativa por parte da equipe técnica**. Aplica-se principalmente aos atendimentos Nível 1.
- **Tempo de Solução (TS):** tempo entre o registro do chamado e sua **resolução completa** por parte do grupo solucionador (N1, N2, N3 ou serviços especializados).
- **Tempo de Resposta:** aplicável ao tratamento de **eventos automatizados** (ex: alertas de monitoramento), mensura o tempo entre a geração do evento e a ação inicial de resposta técnica.

**Classificação dos Chamados**

Os chamados serão classificados em três tipos principais, com SLAs diferenciados conforme urgência, impacto ou complexidade:

1. **Incidentes:** falhas, indisponibilidades ou interrupções de serviço.
2. **Requisições de Serviço:** solicitações de criação, configuração, acesso, permissões, etc.
3. **Rotinas Agendadas:** atividades recorrentes com cronograma pré-definido.

**Tabela de Tempo Máximo de Solução – Incidentes**

| Prioridade | Descrição | Tempo Máximo de Solução (TS) |
|---|---|---|
| P1 | Urgência crítica com alto impacto | 1 hora |
| P2 | Alta prioridade, mas com menor impacto | 2 horas |
| P3 | Média prioridade, impacto pontual | 4 horas |
| P4 | Baixa prioridade, impacto reduzido | 8 horas |
| P5 | Muito baixa, agendável ou impacto mínimo | 12 horas |

**Tabela de Tempo Máximo de Solução – Requisições e Rotinas**

| Complexidade | Descrição | Tempo Máximo de Solução (TS) |
|---|---|---|
| Baixa | Simples, com esforço técnico reduzido | 4 horas úteis |
| Média | Moderada, envolve mais de um recurso | 8 horas úteis |
| Alta | Complexa, afeta vários sistemas ou setores | 16 a 40 horas úteis |

***Atendimentos agendados deverão seguir o horário previamente definido com o solicitante, sendo medidos também pelo cumprimento da agenda.

**Tempo Máximo de Atendimento (TA) por Canal**

| Canal de Abertura | Tempo Máximo de Atendimento (TA) |
|---|---|
| WhatsApp | Até 5 minutos |
| Telefone | Até 5 minutos |
| Sistema de ITSM (formulário) | Até 15 minutos |

*** O não cumprimento do TA poderá gerar impacto nos indicadores de desempenho mensal da contratada.

**Pausa no SLA por Dependência de Terceiros**

O SLA poderá ser temporariamente suspenso nos casos em que a resolução da demanda estiver condicionada à atuação de fornecedores externos da Prefeitura, desde que observados os seguintes critérios:

- Registro formal da data e hora de início e fim da pausa na ferramenta de ITSM;
- Justificativa documentada e classificada como "dependência externa";
- Acompanhamento ativo da contratada junto ao fornecedor;
- Retomada automática da contagem do SLA após resposta ou solução do fornecedor.

**Exemplo:** acionamento de empresa de link de internet, locadora de equipamentos ou fornecedor de software.

**Monitoramento, Validação e Penalidades**

- Todos os SLAs deverão ser monitorados mensalmente e constar nos relatórios técnicos e operacionais entregues à fiscalização;
- O índice mínimo de cumprimento dos SLAs de TA e TS será de 90% por período de apuração, considerando:
  - Todos os tipos de chamados (incidentes, requisições, rotinas);
  - Todos os canais de atendimento (WhatsApp, telefone, e-mail, sistema ITSM);
  - Todas as equipes da contratada (N1, N2, N3 e especialistas);

- O descumprimento dos SLAs poderá resultar em:
  - Glosa proporcional no valor mensal, conforme definido em contrato;
  - Notificações formais para adequação;
  - Aplicação de penalidades contratuais, incluindo rescisão por descumprimento reiterado.

Justificativas técnicas para eventuais descumprimentos deverão ser apresentadas pela contratada e avaliadas pela fiscalização do contrato.

**Estrutura Mínima da Equipe e Perfis Profissionais**

A contratada deverá disponibilizar equipe técnica qualificada, em quantitativo e estrutura compatíveis com as exigências deste Termo de Referência, garantindo a execução integral dos serviços contratados, em regime de atendimento contínuo, com cobertura em horários comerciais, plantões e regime 24x7, conforme definido neste instrumento.

A composição mínima da equipe deverá contemplar, obrigatoriamente:

- 1 (um) Gerente Técnico do Contrato;
- 1 (um) Líder Técnico de Suporte Nível 1 e Nível 2;
- 1 (um) Líder Técnico de Suporte Nível 3;
- 2 (dois) Profissional de Suporte Nível 1 (N1);
- 1 (um) Profissional de Suporte Nível 2 (N2);
- 1 (um) Profissional de Suporte Nível 3 (N3);
- 1 (um) Especialista em Segurança da Informação.

**Observação:** A definição do quantitativo total de profissionais por nível é de responsabilidade da contratada, que deverá dimensionar sua equipe conforme a complexidade do contrato e a necessidade de cumprimento integral dos SLAs e quantitativo de atendimentos a serem solicitados. No entanto, será obrigatória a apresentação de profissionais distintos para cada um dos perfis mínimos definidos acima.

**Perfis Profissionais e Requisitos Mínimos**

As exigências de formação, experiência e conhecimentos abaixo descritas devem ser entendidas como requisitos mínimos para aceitação dos profissionais, complementando as atribuições técnicas já descritas nos itens 5.3 a 5.6 deste Termo de Referência.

**Gerente Técnico do Contrato**

- Ensino superior completo em TI ou áreas afins;
- Experiência mínima de 10 anos em ambientes de porte semelhante;
- Desejável certificação ITIL ou equivalente;

- Conhecimento comprovado em gestão de contratos de serviços de TI, metodologias de governança, SLAs, relatórios e coordenação de equipes multidisciplinares;
- Conhecimento geral das soluções técnicas previstas neste contrato.

**Líder Técnico de Suporte Nível 1 e Nível 2**

- Ensino superior em andamento ou completo na área de TI;
- Experiência mínima de 5 anos em suporte técnico e liderança de equipes operacionais;
- Domínio de ferramentas ITSM, gestão de escalonamento e priorização;
- Conhecimento técnico em redes, Windows, antivírus, acesso remoto e atendimento a usuários.

**Líder Técnico de Suporte Nível 3**

- Ensino superior completo em TI ou áreas correlatas;
- Experiência mínima de 5 anos em administração de servidores e infraestrutura crítica;
- Vivência em coordenação de equipes técnicas, gestão de problemas e implantação de soluções de infraestrutura;
- Conhecimento avançado em sistemas operacionais (Linux e Windows), virtualização, storage, firewall, Active Directory e monitoramento;
- Conhecimento técnico das soluções contratadas.

**Profissionais de Suporte Nível 1 (N1)**

- Ensino médio técnico completo em informática ou área correlata;
- Experiência mínima de 2 anos em atendimento técnico e registro de chamados;
- Conhecimentos obrigatórios:
  - ITSM, Windows, softwares corporativos, antivírus;
  - Atendimento remoto, triagem e comunicação clara com o usuário.

**Profissionais de Suporte Nível 2 (N2)**

- Ensino médio técnico completo;
- Experiência mínima de 3 anos em suporte técnico intermediário;
- Conhecimentos obrigatórios:
  - Diagnóstico e correção de falhas, impressoras, permissões;
  - Apoio a sistemas, antivírus, scripts e testes.

**Profissionais de Suporte Nível 3 (N3)**

- Ensino superior completo em TI;
- Experiência mínima de 5 anos em administração de servidores e redes;
- Conhecimentos obrigatórios:
  - Linux, Windows Server, AD, File Server, DNS, DHCP;
  - Virtualização (KVM, Hyper-V, VMware), Zabbix, backup, firewall, VPNs;
  - PostgreSQL, MySQL, tuning e segurança de infraestrutura.

**Especialistas em Segurança da Informação**

- Ensino superior completo em TI ou áreas correlatas;
- Experiência mínima de 10 anos em projetos de segurança da informação;
- Conhecimentos obrigatórios:
  - Políticas de segurança, ISO/IEC 27001, avaliação de riscos, controles técnicos;
  - Due diligence, auditoria, apoio a contratações com foco em SI;
- Desejáveis certificações: ISO 27001 Lead Implementer, CISSP, CompTIA Security+, CISM, entre outras.

**Validação e Substituição de Profissionais**

A contratada deverá apresentar, em até 30 dias após a assinatura do contrato, a relação nominal dos profissionais alocados, com os seguintes documentos:

- Currículo resumido;
- Certificados e atestados de capacitação;
- Comprovação do vínculo com a empresa (CLT ou contrato).

A equipe será submetida à validação da Prefeitura, que poderá recusar profissionais que:

- Não atendam aos requisitos mínimos exigidos;
- Apresentem documentação incompleta ou inconsistências;
- Não possuam vínculo adequado com a contratada.

Em caso de recusa, a contratada terá até 10 dias úteis para apresentar substituto compatível, sob pena de descumprimento contratual, podendo ser aplicada sanção ou convocação da próxima colocada.

**Documentos para Comprovação de Qualificação Profissional**

A qualificação e experiência dos profissionais deverão ser comprovadas por meio de um ou mais dos seguintes documentos:

- Currículo atualizado com funções exercidas e períodos de atuação;
- Cópias de certificados, diplomas ou documentos acadêmicos;
- Atestados de capacidade técnica emitidos por empresas públicas ou privadas;
- Declarações assinadas por responsáveis técnicos de projetos anteriores;
- Carteira de trabalho (CLT), contratos ou outros documentos que evidenciem a atuação.

A fiscalização poderá solicitar documentos complementares a qualquer tempo. A apresentação de documentos falsos ou informações inverídicas poderá ensejar reprovação do profissional e aplicação das penalidades previstas na legislação e no contrato.

**Soluções e Sistemas a Serem Implantados**

A presente contratação contempla a implantação, operação e sustentação de um conjunto de soluções técnicas de tecnologia da informação e segurança da informação, a serem distribuídas em três categorias principais conforme o modelo de implantação: **on-premises (local), híbrido (inicialmente na nuvem com possibilidade de internalização)** e **totalmente em nuvem (cloud-only)**.

Essas soluções visam à modernização da infraestrutura de TI da Prefeitura, à proteção de ativos críticos, à gestão centralizada dos serviços e à elevação do nível de maturidade em segurança da informação, conforme detalhado nos subitens a seguir.

**Soluções com Implantação On-Premises (Sede da Prefeitura)**

Estas soluções deverão ser implantadas diretamente na infraestrutura local da Prefeitura, garantindo controle, autonomia e disponibilidade sobre os ativos críticos de autenticação e compartilhamento interno de dados:

- **Active Directory (AD):**
  - Implantação de controlador de domínio para autenticação centralizada;
  - Criação de GPOs, estrutura por unidades organizacionais e perfis de acesso;
  - Controlador redundante, com replicação entre DCs e contingência local;
  - Integração futura com ITSM, RMM, antivírus e demais soluções do contrato.
- **File Server com DFS (Distributed File System):**
  - Servidor de arquivos com estrutura por setor, permissões por grupo e cotas definidas;
  - Replicação ativa via DFS para redundância;
  - Mapeamento automático nas estações de trabalho e versionamento de arquivos.

**Observação:** Ambas as soluções deverão ser implantadas com arquitetura de alta disponibilidade, autenticação segura e mecanismos de recuperação.

**Soluções com Implantação Inicial na Nuvem e Internalização Posterior na sede da Contratante ou em nuvem indicada pela Contratante**

Estas soluções deverão ser inicialmente provisionadas na infraestrutura em nuvem da contratada, com **garantia contratual de migrabilidade total para ambiente local (on-premises – fornecido pela Contratante)** ou em nuvem indicada pela contratante, sem perda de dados, funcionalidades ou continuidade.

A contratada será responsável por toda a operação técnica durante o período em nuvem, incluindo segurança, backup, continuidade e rastreabilidade. A qualquer momento, mediante solicitação da Prefeitura, as soluções deverão ser migradas para ambiente interno, com apoio completo da contratada.

As soluções desta categoria incluem:

- **Ferramenta de ITSM + Inventário de ativos:**
  - Catálogo de serviços, gestão de chamados, controle de SLA;
  - Gestão de ativos (CMDB), com agente de inventário instalado nos equipamentos;
  - Integração com Active Directory e envio automático de pesquisas de satisfação.
- **RMM (Gerenciamento e monitoramento remoto de desktops e servidores):**
  - Acesso remoto, automação de scripts, atualizações, agendamentos e correções;
  - Monitoramento de saúde das estações, coleta de logs, relatórios e alertas;
  - Integração com a equipe de N1/N2/N3 e base de conhecimento.

- **Monitoramento:**
  - Monitoramento de servidores, links, serviços e disponibilidade;
  - Dashboards em tempo real com indicadores visuais para tomada de decisão;
  - Alarmes e integrações com logs, e-mail e WhatsApp.

- **Gestão de Logs / SIEM:**
  - Coleta e análise de logs de segurança e eventos;
  - Regras de detecção de anomalias, correlação e geração de alertas;
  - Integração com antivírus, AD, firewall e demais sistemas.

- **Análise de Vulnerabilidades:**
  - Mapeamento e escaneamento periódicos de vulnerabilidades técnicas;
  - Classificação por severidade, com relatórios e planos de correção;
  - Possibilidade de integração com o plano de gerenciamento de riscos.

Todas essas soluções deverão ser **exclusivas e dedicadas à contratante**, com backup diário, autenticação forte, controle de acesso e redundância garantida durante o período de funcionamento na nuvem da contratada.

**Soluções 100% em Nuvem (Cloud-Only)**
Estas soluções deverão operar integralmente em nuvem, por inviabilidade técnica ou econômica de operação local. A contratada deverá garantir:

- Certificação de segurança e conformidade das plataformas utilizadas;
- Backup externo seguro, com replicação e rastreabilidade;
- Suporte técnico em conformidade com o SLA de disponibilidade.

As soluções incluem:

- **Backup em Nuvem (BaaS):**
  - Solução com agendamento, versionamento e retenção de dados críticos;
  - Armazenamento em nuvem com replicação geográfica;
  - Política de recuperação com objetivo de tempo de recuperação (RTO) e objetivo de ponto de recuperação (RPO) definidos no contrato;
  - Acesso seguro e monitoramento da integridade dos dados.
  - Possibilidade de manter cópias de backups em dispositivos de armazenamento na sede da prefeitura

- **Antivírus com Console Central em Nuvem:**
  - Proteção contra malware, ransomware, phishing e ameaças persistentes;
  - Gerenciamento centralizado com aplicação de políticas por grupo;
  - Filtragem web por categoria;
  - Relatórios de conformidade;
  - Atualizações automáticas e análise de comportamento em tempo real.

**Regras de Implantação, Manutenção e Evolução das Soluções**

**Setup da Solução**

Cada solução prevista nesta contratação deverá passar por um processo de implantação técnica inicial (setup), conduzido integralmente pela contratada, contemplando:

- Levantamento técnico de requisitos e ambiente, com reuniões com a equipe de TI da Prefeitura;
- Parametrização, configuração e integração com a infraestrutura existente, incluindo Active Directory, rede, serviços e demais componentes correlacionados;
- Provisionamento técnico completo, seja em ambiente local (on-premises) ou em nuvem (da contratada), com criação das estruturas, usuários, regras e integrações necessárias;
- Execução de testes técnicos funcionais, testes de carga e desempenho, validações operacionais e testes de contingência (quando aplicável);
- Geração e entrega da documentação técnica completa, incluindo: diagrama da arquitetura implantada, parâmetros utilizados, registros de testes e POPs (procedimentos operacionais padrão).

O setup será tratado como entregável técnico independente, com custo definido na proposta da contratada, desvinculado da operação mensal. A execução do setup poderá exigir o uso de infraestrutura temporária em nuvem (servidores, instâncias, conectividade etc.), cujos custos deverão estar incorporados ao valor do setup.

A aceitação de cada solução implantada dependerá da validação técnica pela fiscalização da Prefeitura, com base nos seguintes critérios:

- Entrega funcional operando conforme os requisitos;
- Disponibilidade mínima dos serviços (em ambiente simulado);
- Evidências dos testes realizados;
- Documentação entregue e aprovada.
-

A contratada deverá garantir que nenhuma solução entre em operação sem passar pelo processo completo de setup e validação técnica.

**Manutenção e Sustentação Operacional**

Após a conclusão do setup de cada solução, caberá à contratada garantir sua operação contínua, eficiente e segura, observando as seguintes diretrizes:

- As atividades rotineiras de operação, suporte, ajustes simples, monitoramento, manutenção corretiva e preventiva deverão ser executadas pelas equipes de suporte técnico (N1, N2, N3 e gerente técnico), sem ônus adicional;
- Será obrigatória a manutenção contínua da documentação técnica, com atualização a cada mudança relevante;
- Toda a operação deverá ser rastreável via sistema ITSM, com registros de intervenções, logs de eventos e relatórios periódicos;
- A contratada será responsável por garantir, dentro da operação mensal:
  - A renovação e manutenção dos licenciamentos necessários;
  - O pagamento de infraestrutura em nuvem utilizada (armazenamento, banda, instâncias, conectividade e outros custos operacionais).

Quando a manutenção exigir atividades classificadas como especializadas — como tuning de análise de vulnerabilidade, ajustes avançados em SIEM, reconfiguração de política de segurança ou hardening de serviços — estas deverão ser realizadas exclusivamente pela equipe de serviços especializados em segurança da informação, com horas debitadas do banco de horas técnicas contratado (UST).

**Customizações Futuras, Novas Funcionalidades e Reimplantações**

Ao longo da vigência contratual, a qualquer momento, poderão ser identificadas novas demandas que não estavam previstas no setup inicial, como:

- Implantação de novos módulos ou funcionalidades dentro das soluções já contratadas;
- Integrações com outros sistemas internos ou externos;
- Reorganizações relevantes na estrutura das ferramentas (por exemplo, novas OUs no AD, remodelagem de dashboards, mudança na topologia de rede);

- Migração de ambiente (nuvem para local ou vice-versa);
- Reinstalações ou reimplantações após incidentes críticos (ransomware, falhas graves, perda de dados, entre outros).

Essas ações deverão ser tratadas como serviços extraordinários, executadas exclusivamente pela equipe especializada e cobradas por consumo do banco de horas técnicas (USTs), conforme a complexidade e esforço estimado. A execução dependerá de:

- Aprovação formal da contratante;
- Elaboração de plano técnico resumido com escopo e impacto;
- Registro e controle via sistema ITSM.

**Requisitos para Soluções em Nuvem – Datacenter e Segurança**

Todas as soluções previstas nesta contratação que operem em ambiente de nuvem pública, privada ou híbrida deverão estar hospedadas em infraestrutura de datacenter que atenda a requisitos mínimos de segurança, disponibilidade, escalabilidade, conformidade legal e continuidade de serviços, conforme detalhado a seguir.

**Localização e Certificações**

- O datacenter utilizado deverá estar fisicamente localizado em território brasileiro, com vista à observância da Lei Geral de Proteção de Dados (LGPD), considerando o tratamento de dados pessoais e sensíveis;
- O ambiente deverá possuir certificação válida e auditável ISO/IEC 27001 (Segurança da Informação) e ISO/IEC 27701 (Privacidade da Informação);
- A infraestrutura física deverá ser classificada, no mínimo, como Tier III, segundo o padrão do Uptime Institute, garantindo redundância, tolerância a falhas e alta disponibilidade operacional.

**Requisitos Técnicos de Segurança**

O ambiente de nuvem deverá possuir os seguintes controles mínimos de segurança:

- Conectividade via VPN site-to-site dedicada, com criptografia IPsec;
- Toda a configuração da VPN, incluindo o apoio à borda da Prefeitura, será de responsabilidade da contratada;
- Firewall gerenciado, com:
  - Regras específicas por servidor/serviço;
  - Controle de acesso por IP e porta;
  - Geração de logs, detecção de tentativas de intrusão e bloqueios;
- WAF (Web Application Firewall) obrigatório para todos os sistemas acessíveis via web;
- Segmentação lógica de rede (VLANs) entre as camadas de aplicação, banco de dados e serviços expostos;
- Autenticação multifator (MFA) para todos os acessos administrativos à infraestrutura;
- Acesso remoto permitido apenas via VPN ou redes explicitamente autorizadas, com:
  - Bloqueio de portas padrão;
  - Registros de acesso e alertas de atividades suspeitas;
- Monitoramento contínuo da postura de segurança, com escaneamento de vulnerabilidades e mecanismos de correção;
- Armazenamento seguro dos dados da Prefeitura, com registros criptografados, controle de acesso e logs de integridade.

**Requisitos de Continuidade e Recuperação**

A infraestrutura da contratada deverá ser capaz de garantir continuidade e recuperação dos serviços em caso de incidentes críticos, observando:

- Escalonamento vertical e horizontal sob demanda (ex: aumento de CPU, memória, instâncias);
- Replicação entre zonas de disponibilidade, quando suportado;
- Backups automáticos diários, armazenados em áreas logicamente isoladas da instância principal;
- Política de Disaster Recovery (DR) que assegure:
  - Capacidade de recuperação em até 2 horas após incidente grave (RTO);
  - Retenção e versionamento conforme política da Prefeitura;
  - Verificação periódica da integridade dos backups e registros de recuperação de teste;

- A contratada deverá apresentar plano técnico de DR e evidências de que a arquitetura implantada suporta os requisitos definidos.

**Requisitos de Disponibilidade e Segurança**

A contratada deverá assegurar alta disponibilidade das soluções em nuvem fornecidas, com os seguintes parâmetros:

- Disponibilidade mínima exigida: 99% ao mês, calculada com base no tempo efetivo de operação;
- Será exigido monitoramento contínuo da disponibilidade, com relatórios mensais por serviço;
- Serão aceitas janelas de manutenção programadas, limitadas a:
  - Até 4 horas por mês;
  - Exclusivamente entre 22h e 5h (horário de Brasília);
  - Comunicadas à Prefeitura com no mínimo 48 horas de antecedência;
- Não serão considerados como falha de disponibilidade:
  - Períodos de inatividade previamente agendados e aprovados;
  - Falhas de rede sob responsabilidade da Prefeitura;
- O descumprimento reiterado da disponibilidade mínima poderá ensejar:
  - Advertência formal;
  - Glosa proporcional;
  - Penalidades contratuais, incluindo rescisão por inadimplemento técnico.
- As soluções devem ser atualizadas mensalmente para garantir que não estejam vulneráveis – todas as atualizações devem ser registradas formalmente na plataforma de ITSM;

**Implantação de Solução de Active Directory Redundante com File Server e DFS**

Esta solução tem como objetivo a implantação de uma infraestrutura local (on-premises) robusta e integrada para autenticação de usuários, gestão de acessos e compartilhamento de arquivos institucionais, baseada em Active Directory com controladores de domínio redundantes e servidor de arquivos com replicação via DFS (Distributed File System).

A solução deverá ser implantada no datacenter da sede da Contratante, com equipamentos fornecidos pela Contratante, garantindo alta disponibilidade, controle granular de permissões, compatibilidade com as políticas de segurança da informação e integração com demais sistemas técnicos da organização.
A seguir, apresenta-se o detalhamento técnico da solução, dividido em componentes funcionais:

| **Active Directory (AD):** |
|---|
| Implantação de, no mínimo, dois controladores de domínio redundantes; |
| Configuração de replicação multimestre entre controladores; |
| Integração com serviço de DNS interno, com zonas seguras e resolução local; |
| Implantação do serviço DHCP, com escopo reservado e integração com o AD; |
| Configuração de servidor de horário (NTP) confiável, com sincronização entre DCs; |
| Criação de estrutura de Unidades Organizacionais (OUs) por secretaria, setor ou perfil – a ser definido em plano de projeto; |
| Criação de grupos de segurança e grupos de distribuição; |
| Configuração de GPOs (Group Policy Objects) com, no mínimo: |
| Políticas de complexidade de senha; |
| Bloqueio de sessão por inatividade; |
| Expiração de senha; |
| Definição de papel de parede institucional; |
| Mapeamento automático de unidades de rede; |
| Scripts de login e restrições básicas de desktop.<br>outras |
| **File Server com DFS:** |
| Instalação de File Server com estrutura de pastas por setor; |
| Aplicação de permissões com base nos grupos de segurança do AD; |
| Implantação de solução de DFS Namespace com replicação ativa (DFS-R) entre dois servidores; |
| Segmentação lógica por diretórios; |

| |
|---|
| Agendamento de replicações; |
| Registro e auditoria de alterações de arquivos; |
| Políticas de cota de disco por grupo ou usuário (quando aplicável); |
| Backup local configurado de acordo com a política da Prefeitura. |
| ***Responsabilidades da Contratada*** |
| **Implantação e Configuração:** |
| Prover mão de obra técnica para configuração dos servidores, instalação do sistema operacional, atualizações e serviços associados; |
| Realizar a criação das estruturas de OUs, grupos, usuários e GPOs iniciais; |
| Criar os compartilhamentos, permissões e replicações no DFS; |
| Configurar e validar os serviços de DNS, DHCP e NTP. |
| **Participação Técnica e Alinhamento:** |
| Participar de reunião técnica com a equipe da Prefeitura para levantamento de requisitos, definição das boas práticas e estratégias de implantação; |
| Apoiar a definição de padrões de nomenclatura, estrutura lógica e regras de segurança. |
| ***Entregáveis Obrigatórios*** |
| **Documentação Técnica:** |
| Diagrama lógico da estrutura de domínio, file server e replicação DFS; |
| Lista de OUs, grupos, GPOs e suas configurações; |
| Procedimentos operacionais padrão (POP) para rotinas administrativas (criação de usuário, redefinição de senha, adição ao domínio, mapeamento de rede); |
| Relatório final da implantação, com checklists de validação e evidências de testes. |
| **Treinamento:** |
| Treinamento básico para colaboradores da Prefeitura responsáveis pela administração do ambiente, com foco em: |
| Inclusão de novos dispositivos no domínio; |
| Criação e remoção de usuários; |
| Redefinição de senhas; |
| Aplicação de permissões de rede e uso de arquivos compartilhados; |
| Treinamento voltado também para fornecedores externos, como empresa de locação de equipamentos, que necessitem integrar seus dispositivos à estrutura de domínio de forma segura e conforme os procedimentos estabelecidos. |

**Observações e Considerações Técnicas Finais**
A implantação da solução deverá ser realizada em conformidade com as boas práticas do mercado e diretrizes da Contratante, sendo obrigatória a validação técnica por parte da fiscalização contratual antes da aceitação final.
Todos os serviços, configurações, integrações e documentações deverão ser auditáveis, rastreáveis e aprovados formalmente. O não cumprimento de qualquer requisito previsto poderá ensejar a recusa da entrega e aplicação das sanções contratuais cabíveis.

**Implantação da Solução de ITSM com Módulo de Inventário e CMDB**
A presente contratação contempla a implantação de uma solução completa e integrada de ITSM (Information Technology Service Management), com funcionalidades de gestão de serviços, controle de ativos, base de conhecimento, CMDB (Configuration Management Database), gerenciamento de mudanças e projetos, conforme as boas práticas da biblioteca ITIL.

A ferramenta deverá ser implantada inicialmente na nuvem da contratada, com possibilidade contratual de futura migração para ambiente on-premises da Prefeitura, sem perda de dados, histórico ou funcionalidades. A solução deverá estar alinhada aos princípios de usabilidade, acessibilidade, interoperabilidade e segurança, além de cumprir os critérios técnicos definidos a seguir.

| |
|---|
| **CMDB e Inventário** |

| |
|---|
| Gestão de ativos de TI, incluindo: computadores, notebooks, monitores, dispositivos de rede, impressoras, cartuchos, telefones e softwares; |
| Mapeamento completo de hardware e software instalado, incluindo data de aquisição, alocação, garantias e status de uso; |
| Integração com agente de inventário (modo ativo e passivo); |
| Relacionamento dos ativos com chamados, contratos e usuários; |
| Controle de movimentação e histórico de alterações. |
| **Helpdesk e Gestão de Chamados** |
| Abertura de chamados via: |
| Painel web (self-service); |
| E-mail (automatizado); |
| API externa (para integração com outras ferramentas); |
| Classificação dos chamados em: |
| Incidente, Requisição, Problema, Mudança, Projeto; |
| Cadastro e manutenção do Catálogo de Serviços conforme ITIL; |
| Permissão para associar chamados a: |
| Projetos; |
| Tarefas; |
| Itens de CMDB; |
| Outros chamados (relação incidente–problema, etc.); |
| Definição e acompanhamento de SLAs (tempo de atendimento, de solução, intermediário); |
| Criação de regras de urgência, impacto e prioridade; |
| Categorização por serviço, setor, unidade ou secretaria; |
| Criação de etiquetas (tags), origem da requisição, e status personalizados (novo, em atendimento, pendente, planejado, solucionado, fechado); |
| Inclusão de observadores, atribuição por grupo ou usuário, e definição de perfis: |
| Administrador, Supervisor, Técnico, Observador, Somente leitura, etc.; |
| Log de todas as ações executadas em cada chamado, com data, hora e responsável; |
| Envio de notificações automáticas por e-mail; |
| Regras automatizadas para tratamento de chamados, aprovação e escalonamento. |
| **Gestão de Problemas, Mudanças e Projetos** |
| Módulo de gerenciamento de problemas: correlação com incidentes e ações proativas; |
| Módulo de gestão de mudanças, com controle de ciclo de vida, aprovações e planos de rollback; |
| Gerenciamento de projetos, com: |
| Visão em Kanban e Gantt; |
| Atribuição de tarefas e prazos; |
| Relacionamento com chamados; |
| Timeline de andamento e relatórios por projeto. |
| ***Integrações, Segmentações e Governança*** |
| Integração nativa com Active Directory (LDAP), permitindo autenticação unificada e controle de permissões por unidade organizacional; |
| Possibilidade de segmentar a visibilidade dos chamados por secretaria ou unidade administrativa, garantindo que cada gestor visualize apenas sua estrutura; |
| Possibilidade de geração de relatórios customizados, com exportação em múltiplos formatos (PDF, CSV, Excel); |
| Configuração de pesquisas de satisfação automatizadas, com envio imediato após encerramento do chamado. |
| ***Requisitos de Infraestrutura e Continuidade*** |
| A solução deverá ser implantada inicialmente na nuvem do fornecedor, com possibilidade de migração futura para ambiente on-premises da Prefeitura; |
| **A estrutura da solução deverá ser:** |
| Preferencialmente open source ou com mapa de dados aberto e estruturado, de modo que seja possível futura internalização; |

| |
|---|
| Capaz de fornecer documentação técnica da estrutura do banco de dados (modelo relacional, chaves, relacionamentos) |
| **A infraestrutura de hospedagem deverá seguir os critérios definidos no item 5.16.5, incluindo:** |
| Backup diário com retenção definida; |
| Disaster recovery com RTO de até 2 horas; |
| VPN site-to-site com a Prefeitura; |
| Análises recorrentes de vulnerabilidades. |
| ***Entregáveis e Treinamento*** |
| **Manual técnico e operacional da ferramenta implantada, incluindo:** |
| Estrutura de serviços cadastrados; |
| Papéis e permissões configurados; |
| Catálogo de serviços e estrutura de CMDB; |
| Procedimentos de abertura, encerramento e reclassificação de chamados; |
| **Treinamento para:** |
| Equipe técnica de TI da Prefeitura (uso administrativo e supervisão); |
| Usuários finais (painel de abertura de chamados, status e acompanhamento); |
| Fornecedores ou empresas terceiras que utilizarão o sistema. |

13.1.2 **Implantação da Solução de RMM (Remote Monitoring and Management)**

A presente contratação contempla a implantação de uma solução corporativa de RMM (Remote Monitoring and Management), voltada para o gerenciamento remoto, automação, coleta de informações, acesso técnico, monitoramento e manutenção preventiva dos ativos computacionais da Prefeitura.

A solução deverá estar alinhada às boas práticas de gestão de infraestrutura, com suporte a ambientes híbridos (Windows, Linux, MacOS), ampla capacidade de automação, alto grau de rastreabilidade e compatibilidade com o modelo de suporte técnico em múltiplos níveis (N1, N2, N3).

| |
|---|
| **Monitoramento e Gestão Remota:** |
| Acesso remoto direto aos dispositivos gerenciados, sem necessidade de aprovação do usuário final; |
| Console de administração com acesso via navegador (dashboard de alertas e monitoramento em tempo real); |
| Acesso remoto à linha de comando (PowerShell, CMD, shell Linux); |
| Gerenciamento remoto de arquivos, upload/download, visualização de diretórios; |
| Gerenciamento de serviços do sistema operacional (start/stop/status); |
| Acesso à visualização de logs de eventos; |
| Possibilidade de matar processos remotamente. |
| **Automação de Tarefas e Checagens:** |
| Execução remota de scripts (PowerShell, Python, Shell, Bash, Deno, Nushell); |
| Agendamento de tarefas automatizadas (diárias, semanais, mensais); |
| Deploy em massa de tarefas, checagens e templates para grupos de equipamentos; |
| Criação de checagens automatizadas baseadas em métricas como CPU, disco, memória, eventos de log, status de serviços, scripts; |
| Possibilidade de execução recorrente de scripts para coleta, manutenção ou correção. |
| **Notificações, Alertas e Ações Integradas:** |
| Envio de alertas via e-mail, SMS e Webhooks, com configuração por tipo de evento ou criticidade; |
| Integração com API aberta REST, com documentação para integrações externas; |
| Permissão para criar URL Actions, executadas diretamente nos dispositivos monitorados. |
| **Gestão de Inventário e Atualizações:** |
| Coleta e relatórios automáticos de hardware e software; |
| Identificação de sistemas operacionais e drivers desatualizados; |
| Relatórios customizáveis e prontos (máquinas desatualizadas, softwares instalados, ativos sem conexão, etc.); |
| Controle de atualizações do sistema operacional (patch management), com política de agendamento e aprovação. |
| **Segurança, Usuários e Permissões:** |

| |
|---|
| Autenticação obrigatória com duplo fator (MFA) para todos os acessos administrativos; |
| Controle granular de permissões por tipo de perfil (admin, operador, supervisor, auditor, etc.); |
| Log completo de todas as ações realizadas pelos usuários da plataforma; |
| Possibilidade de separar os equipamentos por unidade organizacional (secretaria, setor ou grupo lógico); |
| Sistema compatível com múltiplos sistemas operacionais: |
| Windows 7, 8.1, 10, 11, Server 2008 R2 a 2022 |
| Linux (qualquer distribuição com systemd) |
| MacOS (Intel e Apple Silicon – M1/M2) |
| ***Requisitos de Implantação e Operação*** |
| A solução deverá ser implantada inicialmente na nuvem do fornecedor, com possibilidade de migração para ambiente on-premises da Prefeitura; |
| A infraestrutura da solução deverá atender aos requisitos descritos no item 5.16.5 (Datacenter em Nuvem), incluindo: |
| Certificações ISO 27001/27701; |
| VPN site-to-site com a sede da Prefeitura; |
| Alta disponibilidade, WAF, segmentação de rede e DR com RTO ≤ 2 horas; |
| Backup diário da aplicação e dados. |
| **A solução deverá ser licenciada para suportar todos os ativos computacionais da Prefeitura, conforme tabela a ser definida no Termo de Referência;** |
| O acesso ao sistema deverá ser feito via navegador, com compatibilidade total com os principais navegadores; |
| O sistema deverá permitir instalação de agente leve em cada dispositivo gerenciado, com atualizações automáticas e conexão persistente. |
| ***Entregáveis e Treinamento*** |
| **Manual técnico da solução, contendo:** |
| Estrutura de grupos, usuários, permissões; |
| Rotinas de automações configuradas; |
| Regras de alerta e notificação; |
| Integrações via API ou Webhook, quando houver. |
| **Treinamento prático para:** |
| Equipes de gestão e técnicas da Prefeitura; |
| Supervisores e técnicos de atendimento que utilizarão os recursos de acesso remoto e monitoramento. |

13.1.3 **Implantação da Solução de Monitoramento de Ativos, Servidores, Redes e Sistemas**

A presente contratação contempla a implantação de uma solução corporativa de monitoramento contínuo e inteligente, com capacidade de supervisionar a infraestrutura crítica da Prefeitura Municipal, detectando falhas, analisando desempenho, emitindo alertas e gerando relatórios de SLA e disponibilidade.

A ferramenta deverá ser compatível com múltiplas tecnologias e arquiteturas (ambientes físicos, virtuais, em nuvem e híbridos), integrando-se com outras soluções já previstas neste Termo e permitindo ampla personalização visual e operacional.

| **Abrangência e Tipos de Monitoramento** |
|---|
| Monitoramento de ativos de rede, servidores físicos e virtuais, serviços e aplicações, incluindo: |
| Links de internet e VPNs; |
| Switches, roteadores, access points e firewalls; |
| Servidores Windows, Linux, BSD, MacOS, virtualizados e bare-metal; |
| Dispositivos com sensores (IoT), câmeras IP e storages; |
| Sistemas internos, sites públicos, APIs REST e SOAP; |
| Sistemas operacionais, bancos de dados, aplicações locais e web; |
| Integridade de arquivos e logs; |
| Compatível com diversos métodos de coleta, incluindo: |
| Com agente ou sem agente (agentless); |
| SNMP, ICMP (ping), TCP/UDP, WMI, IPMI, SSH, HTTP, ODBC, custom scripts; |

| |
|---|
| Capacidade de acesso direto a sistemas Windows via WMI, sem agente; |
| Capacidade de instalação de agente leve em qualquer sistema operacional suportado; |
| Compatível com virtualização, containers e ambientes multi-cloud. |
| **Coleta Inteligente e Análise Avançada** |
| Coleta de métricas em tempo real com granularidade configurável; |
| Possibilidade de definição de gatilhos inteligentes (triggers) com: |
| Detecção de anomalias baseadas em comportamento; |
| Previsão de tendências e consumo futuro; |
| Detecção de degradação de desempenho; |
| Suporte a monitoramento web e de APIs com simulação de usuário, tempo de resposta e status; |
| Suporte a monitoramento de bancos de dados com query personalizada (MySQL, PostgreSQL, Oracle, etc.); |
| Suporte à verificação de integridade de arquivos e checagem de logs; |
| Possibilidade de autorremediação: execução de ações corretivas automáticas como: |
| Reinício de serviços; |
| Execução de scripts; |
| Escalonamento ou reatribuição de carga. |
| **Visualização, Alertas e Integrações** |
| Criação de: |
| Dashboards técnicos e gerenciais personalizadas; |
| Mapas de rede lógicos e georreferenciados; |
| Visões específicas por setor, sistema ou localização física; |
| Alertas via múltiplos canais: |
| E-mail, SMS, Telegram, Webhook (API), painéis e logs; |
| Suporte à customização da mensagem de alerta (conteúdo, canal, prioridade, grupo); |
| Definição de níveis de notificação/escalonamento, com rotas de alerta por tipo de evento ou severidade; |
| Integração com plataforma de ITSM para: |
| Registro automático de incidentes; |
| Acompanhamento contínuo dos ativos relacionados; |
| Integração com soluções externas via API REST. |
| **Requisitos de SLA e Relatórios** |
| Monitoramento e cálculo automático dos SLAs de disponibilidade para todos os sistemas críticos; |
| Capacidade de emitir relatórios de: |
| Disponibilidade geral e por serviço; |
| SLA por período, sistema e unidade organizacional; |
| Tempo médio de indisponibilidade e tempo de resposta; |
| Tendência de falhas e eventos recorrentes; |
| Agendamento de relatórios periódicos automáticos (PDF, CSV); |
| Exportação de dados da ferramenta para outros sistemas, com mapa de dados e API documentada; |
| Geração de indicadores chave de desempenho (KPIs) da infraestrutura monitorada. |
| **Implantação e Operação** |
| **Durante o setup, a CONTRATADA deverá:** |
| Mapear e cadastrar todos os ativos da Prefeitura (roteadores, links, sistemas, sensores, câmeras, etc.); |
| Configurar os métodos de coleta adequados por tipo de ativo; |
| Criar mapas de rede personalizados, hierárquicos e geográficos; |
| Definir grupos de dispositivos por secretaria ou localização; |
| Criar dashboards separadas para: |
| Equipe técnica (TI); |
| Gestão estratégica (visão resumida de SLA, incidentes, disponibilidade). |
| **A solução será hospedada inicialmente na nuvem da contratada, devendo atender aos requisitos definidos no item 5.16.5 – Datacenter, incluindo:** |
| WAF, backup, VPN, DR em até 2h; |
| Documentação técnica, segurança e continuidade. |

| **Entregáveis e Treinamento** |
|---|
| **Entregáveis mínimos:** |
| Listagem de todos os ativos cadastrados; |
| Relatórios de SLA e disponibilidade configurados; |
| Mapa de rede implantado; |
| Painéis e dashboards por perfil de usuário; |
| Configurações de escalonamento de alertas. |
| **Treinamento:** |
| Treinamento técnico para equipe de TI; |
| Manual de leitura dos relatórios e uso das interfaces; |
| Apoio na leitura de indicadores estratégicos. |

13.1.4 **Implantação da Solução de Gestão de Logs e SIEM**

A presente contratação contempla a implantação da solução Wazuh como plataforma de SIEM (Security Information and Event Management), para a gestão centralizada de logs e eventos de segurança. A solução deverá atender aos requisitos técnicos, operacionais e normativos exigidos, promovendo ampla visibilidade sobre os eventos críticos, rastreabilidade, detecção de ameaças e aderência a padrões de conformidade, em alinhamento com a ISO/IEC 27001, LGPD e demais marcos regulatórios aplicáveis.

A solução deverá ser integrada ao ambiente da Prefeitura, cobrindo endpoints, servidores, redes, aplicações e serviços em nuvem, com atuação em todos os níveis da operação (N1, N2, N3 e serviços especializados).

| **Coleta e Análise de Dados de Segurança (SIEM)** |
|---|
| Agregação e análise em tempo real de dados de eventos de segurança; |
| Coleta de telemetria de endpoints, dispositivos de rede, cargas de trabalho em nuvem e aplicações; |
| Detecção de anomalias e indicadores de comprometimento (IoCs); |
| Enriquecimento contextual dos alertas para acelerar investigações; |
| Redução do tempo médio de resposta a incidentes. |
| **Análise de Logs** |
| Coleta de logs do sistema operacional e de aplicações; |
| Análise baseada em regras para detectar erros, falhas, atividades maliciosas, violações de política e problemas operacionais; |
| Indexação, correlação e armazenamento seguro de logs; |
| Consultas, dashboards e relatórios customizados. |
| **Detecção de Vulnerabilidades** |
| Identificação de vulnerabilidades em endpoints monitorados; |
| Priorização de vulnerabilidades para agilizar a remediação; |
| Integração com banco de dados de CVEs; |
| Apoio à conformidade regulatória e redução da superfície de ataque. |
| **Avaliação de Configuração de Segurança (SCA)** |
| Verificação de conformidade da configuração de sistemas com benchmarks (ex: CIS); |
| Detecção de falhas, desvios e práticas inseguras; |
| Avaliação periódica e automatizada com recomendações de correção; |
| Configurações personalizáveis de verificação. |
| **Monitoramento de Integridade de Arquivos (FIM)** |
| Monitoramento contínuo de alterações em arquivos críticos; |
| Detecção de modificações não autorizadas, deleções ou inserções; |
| Geração de alertas imediatos com trilha de auditoria. |
| **Detecção de Malware e Atividades Maliciosas** |
| Identificação de comportamentos suspeitos nos endpoints; |
| Regras pré-configuradas (rulesets), SCA, Rootcheck e FIM para detecção de ameaças; |
| Capacidade de customização das regras de detecção. |
| **Caça a Ameaças (Threat Hunting)** |

| |
|---|
| Retenção, indexação e consulta de dados para investigação pós-evento; |
| Mapeamento com a matriz MITRE ATT&CK; |
| Integração com feeds de Threat Intelligence externos; |
| Suporte a APIs e log forwarding para ferramentas de análise avançada. |
| **Resposta a Incidentes** |
| Respostas automáticas a eventos (ex: bloqueio de IP, encerramento de processo, execução de comandos); |
| Execução remota de ações corretivas; |
| Identificação de IoCs e suporte à análise forense. |
| **Relatórios e Compliance** |
| Geração de relatórios para os seguintes padrões e regulamentos: |
| ISO 27001, PCI-DSS, NIST 800-53, GDPR, SOC2, HIPAA, entre outros; |
| Dashboards e relatórios automatizados para comprovação de aderência; |
| Relatórios agendados e exportáveis; |
| Insights executivos baseados em eventos de segurança. |
| ***Funcionalidades Avançadas e Integrações*** |
| Agente universal Wazuh: para proteção de endpoints com suporte aos principais sistemas operacionais (Windows, Linux, MacOS, BSD e outros); |
| Suporte a containers e monitoramento nativo de ambientes Docker (hosts, imagens, volumes, runtime, rede); |
| Integração com plataformas de nuvem e SaaS como: |
| AWS, Azure, Google Cloud, Microsoft 365, GitHub, etc.; |
| Workload Protection para cargas locais e em nuvem; |
| Postura de segurança e gestão de conformidade em ambientes cloud; |
| Integrações com: |
| Ferramentas de visualização (Kibana, Grafana); |
| Plataformas de ITSM e automação via API e Webhooks; |
| Plataformas de resposta a incidentes (SOAR). |
| ***Requisitos de Implantação e Segurança*** |
| A solução deverá ser hospedada inicialmente na nuvem da contratada e cumprir os requisitos do item 6.16.5 – Datacenter, incluindo: |
| Proteção por WAF, backup diário, VPN com a Prefeitura e recuperação em até 2h; |
| Segmentação lógica e política de segurança rigorosa; |
| **A configuração inicial deverá contemplar:** |
| Integração com os servidores, sistemas e ativos críticos da Prefeitura; |
| Definição de regras de segurança, alertas, níveis de severidade; |
| Implantação de dashboards específicos por área e por tipo de evento; |
| Configuração de notificações e respostas automatizadas. |
| ***Entregáveis e Treinamento*** |
| **Entregáveis mínimos:** |
| Documento com inventário de ativos monitorados; |
| Regras de correlação e respostas configuradas; |
| Relatórios de conformidade e segurança; |
| Acesso à base de dados e estrutura lógica da plataforma. |
| **Treinamento:** |
| Para equipe técnica de TI e segurança da informação da Prefeitura (uso da interface, regras, investigação); |
| Para a equipe de TI sobre como consultar, reagir e entender os alertas; |
| Manual completo de uso e administração da solução. |

13.1.5 **Implantação de Solução de Análise de Vulnerabilidades Técnicas**

A presente contratação contempla a implantação e operação contínua de uma solução especializada de análise técnica de vulnerabilidades, com base em padrões técnicos reconhecidos internacionalmente (CVE, CPE, NVT), para a avaliação de segurança da infraestrutura de TI da Prefeitura Municipal.

A ferramenta deverá ser capaz de detectar falhas em diferentes tipos de ativos e ambientes, emitir relatórios detalhados, classificar os riscos por severidade e apoiar tecnicamente a correção das vulnerabilidades detectadas, garantindo a evolução da postura de segurança institucional.

| |
|---|
| **A solução utilizada para a análise de vulnerabilidades deverá possuir, no mínimo, as seguintes capacidades:** |
| Escaneamento autenticado e não autenticado de hosts; |
| Suporte à varredura com base em protocolos como SSH, SMB, SNMP, HTTP, HTTPS, IPMI, ODBC, entre outros; |
| Classificação de vulnerabilidades por severidade (Critical, High, Medium, Low, Informational); |
| Atualização automática da base de dados de vulnerabilidades (CVE/CPE/NVT); |
| Perfis de varredura configuráveis por tipo de ativo ou ambiente; |
| Emissão de relatórios técnicos detalhados com: |
| Score de risco; |
| Descrição técnica da vulnerabilidade; |
| Recomendação de correção e links para remediação; |
| Armazenamento histórico de varreduras para análise de evolução da postura de segurança. |
| ***Abrangência das Análises*** |
| As análises deverão incluir, no mínimo: |
| Servidores físicos e virtuais (Windows, Linux e derivados); |
| Estações de trabalho (desktops e notebooks); |
| Dispositivos de rede: switches, firewalls, roteadores, access points; |
| Equipamentos de IoT: câmeras IP, DVRs, sensores e dispositivos conectados; |
| Sistemas operacionais, serviços em nuvem, e aplicações web internas ou externas. |
| Observação: Toda e qualquer solução ou dispositivo conectado na rede da Prefeitura que possua endereço IP ativo deverá obrigatoriamente ser considerado nos ciclos de análise de vulnerabilidades. |
| ***Frequência e Ciclo de Correção*** |
| A análise de vulnerabilidades deverá ser executada pelo menos uma vez a cada 3 (três) meses, ou sob demanda, quando formalmente solicitada pela Prefeitura. |
| **A cada ciclo autorizado de varredura, a CONTRATADA deverá:** |
| Executar o escaneamento completo conforme escopo definido; |
| Apresentar relatório técnico com identificação, severidade e orientações de mitigação; |
| Apoiar tecnicamente a equipe da Prefeitura na correção de vulnerabilidades classificadas como Críticas ou Altas; |
| Quando a vulnerabilidade envolver solução de terceiros, atuar em conjunto com o fornecedor envolvido, apoiando o entendimento do problema e orientando quanto à solução adequada; |
| Após validação da correção, realizar um novo escaneamento nos ativos afetados; |
| Emitir relatório comparativo de validação, demonstrando as correções aplicadas e o status atualizado das vulnerabilidades. |
| ***Requisitos Técnicos e Ciclo de Vida da Solução*** |
| A solução deverá ser inicialmente implantada em ambiente seguro de nuvem, conforme os requisitos do item 5.16.5 – Datacenter, e posteriormente deverá ser migrada para o ambiente on-premises da Prefeitura, mantendo: |
| Todo o histórico de varreduras realizadas; |
| A rastreabilidade dos relatórios e evidências de correções; |
| Os perfis de varredura e as configurações aplicadas. |
| A CONTRATADA deverá ainda apoiar tecnicamente a elaboração da Política de Gestão de Vulnerabilidades Técnicas da Prefeitura, documento normativo que definirá diretrizes formais, periodicidade, responsáveis e critérios para o tratamento de vulnerabilidades. |
| ***Entregáveis*** |
| Plano inicial de configuração e execução das análises de vulnerabilidades; |
| Relatórios técnicos de cada varredura realizada (com score, severidade e recomendações); |
| Relatórios de validação (pós-correção); |

| |
|---|
| Comparativo entre ciclos (linha do tempo da evolução); |
| Política formal de Gestão de Vulnerabilidades Técnicas redigida e aprovada em conjunto com a Prefeitura; |
| Registro em ata das reuniões de apresentação e validação de cada entrega técnica. |

7.2 **Solução de Antivírus com EDR e Filtro de Conteúdo**

A presente contratação contempla a implantação de uma solução integrada de proteção de endpoints, composta por antivírus de última geração, EDR (Endpoint Detection and Response), e filtro de conteúdo com bloqueio por categorias. A solução deverá ser fornecida sob o modelo de software como serviço (SaaS), com console de gestão centralizada em nuvem e cobertura para todos os dispositivos institucionais, incluindo estações, servidores e dispositivos móveis.

A solução deverá garantir proteção em tempo real, capacidade de resposta automatizada a incidentes, relatórios gerenciais e segmentação de políticas por perfil de uso, com base em boas práticas de segurança da informação, conformidade com a LGPD e com os referenciais ISO/IEC 27001 e 22301.

| **Proteção Antivírus e Anti-Malware** |
|---|
| A solução deverá incluir recursos avançados de prevenção, detecção e neutralização de ameaças conhecidas e desconhecidas, incluindo: |
| Mecanismo de antivírus com motor de detecção baseado em assinatura e heurística; |
| Proteção contra: |
| Vírus, worms, trojans, ransomware, rootkits e adware; |
| Spyware, keyloggers e scripts maliciosos; |
| Exploração de vulnerabilidades conhecidas (exploit protection); |
| Análise comportamental (Behavioral Detection) para bloqueio de ameaças desconhecidas; |
| Proteção em tempo real de arquivos, processos e registro do sistema; |
| Proteção durante acesso a dispositivos removíveis (USB, HD externo); |
| Módulo de análise baseada em nuvem (cloud threat intelligence); |
| Scan agendado e sob demanda por grupos de máquinas ou usuários; |
| Modo silencioso para varredura sem impactar o desempenho do usuário; |
| Relatório de detecção e histórico de ameaças por equipamento; |
| Proteção para sistemas operacionais Windows, Linux, MacOS, Android e iOS; |
| Identificação e bloqueio de processos ou conexões maliciosas em execução; |
| Atualizações automáticas de assinaturas de vírus e mecanismos de detecção. |
| **EDR (Endpoint Detection and Response)** |
| Visibilidade total do comportamento do endpoint e da cadeia de ataque; |
| Análise contextual com base em MITRE ATT&CK; |
| Detecção em tempo real de movimentações laterais, persistência, escalonamento de privilégios e comandos suspeitos; |
| Resposta automatizada com: |
| Isolamento de rede; |
| Interrupção de processo; |
| Rollback de sistema; |
| Consolidação de alertas por incidente e correlação de eventos; |
| Investigações guiadas com histórico da ameaça, origem e impacto; |
| Execução de scripts de remediação remotamente; |
| Coleta de artefatos para investigação forense. |
| **Filtro de Conteúdo (URL Filtering)** |
| Bloqueio de navegação por categorias de conteúdo malicioso, improdutivo ou inapropriado; |
| Atualização automática da base de URLs e domínios; |
| Relatórios de tentativa de acesso e bloqueios por usuário, equipamento e horário; |
| Categorias mínimas obrigatórias a serem bloqueadas: |
| Pornografia e conteúdo adulto; |
| Drogas e entorpecentes; |

| |
|---|
| Armas e violência; |
| Redes sociais e mensageria; |
| Ferramentas de VPN e Proxy; |
| Hacking, cibercrime, conteúdo ofensivo; |
| Sites com malware, phishing ou blacklisted por threat intelligence. |
| As políticas de bloqueio devem ser aplicáveis por **perfil, grupo de usuários ou equipamento**, com possibilidade de exceção e escalonamento. |
| ***Implantação e Integração*** |
| A CONTRATADA deverá realizar a implantação da solução em todos os dispositivos da Prefeitura, incluindo: |
| Estações de trabalho (desktops, notebooks); |
| Servidores locais e em nuvem; |
| Dispositivos móveis corporativos (smartphones e tablets com Android e iOS); |
| A instalação deverá incluir: |
| Instalação do agente; |
| Definição de políticas padrão; |
| Ativação de todos os módulos de proteção; |
| Teste de operação e conectividade com o painel central. |
| ***Gestão Centralizada*** |
| Consola de gestão única em nuvem; |
| Visão de todos os dispositivos protegidos, status de proteção, alertas e conformidade; |
| Perfis de acesso: administrador, técnico, leitura, auditor; |
| Suporte a autenticação em dois fatores (MFA); |
| Integração com ferramentas de backup, ITSM e resposta a incidentes. |
| ***Requisitos de Segurança da Solução em Nuvem*** |
| A solução será 100% hospedada na nuvem do fornecedor, e o datacenter utilizado deverá: |
| Estar localizado no território nacional; |
| Ser certificado com: |
| ISO/IEC 27001 (Segurança da Informação); |
| ISO/IEC 22301 (Continuidade de Negócios); |
| Ser classificado como Tier III ou superior, com redundância e alta disponibilidade; |
| O painel de controle deverá ser acessível apenas via HTTPS com autenticação segura. |
| ***Entregáveis e Treinamento*** |
| ***Entregáveis:*** |
| Relatório técnico da implantação por unidade e grupo; |
| Lista dos dispositivos protegidos e com agente ativo; |
| Políticas aplicadas (proteção, EDR e filtro de conteúdo); |
| Relatório das primeiras 4 semanas de operação com detecções, bloqueios e ações realizadas. |
| ***Treinamento:*** |
| Para equipe técnica: instalação, gerenciamento, resposta a alertas e uso do EDR; |
| Para equipe de governança: leitura de relatórios e acompanhamento da postura de segurança. |

**Solução de Backup em Nuvem com Segurança Avançada e Recuperação de Desastres**
Esta contratação contempla a implantação de uma solução de **backup gerenciado em nuvem com funcionalidades nativas de recuperação de desastres (DRaaS)**, proteção contra ransomware, gestão centralizada e automação de políticas. A solução será fornecida em modelo SaaS, acessível via console web segura, garantindo a continuidade dos serviços públicos mesmo diante de incidentes críticos.

**Funcionalidades Técnicas Obrigatórias:**

| |
|---|
| ***Arquitetura, Segurança e Gestão Centralizada*** |
| Plataforma em modelo SaaS nativo, com acesso exclusivo via console web (HTTPS); |
| Acesso restrito exclusivamente por autenticação multifator (MFA); |

| |
|---|
| Capacidade de criação de perfis distintos de usuários e grupos de acesso, com permissões granulares (administração, operação, somente leitura, auditoria); |
| Trilha de auditoria completa (logs de todas as ações realizadas) por qualquer operador, incluindo: |
| Login/logout; |
| Execução de backup ou restauração; |
| Alteração de política ou exclusão de dados; |
| Visibilidade em tempo real de todos os dispositivos protegidos, status dos planos de backup e alertas pendentes; |
| Histórico completo das execuções de backup, falhas, restaurações e eventos críticos. |
| ***Operações de Backup – Recursos Avançados*** |
| Criação e aplicação de planos de backup personalizados, com: |
| Seleção de arquivos, pastas, volumes, discos, máquinas inteiras; |
| Escolha de múltiplos destinos: nuvem, NAS, local, repositórios externos; |
| Retenção configurável de 1 dia até 10 anos por política; |
| Criptografia AES-256 para dados em trânsito e em repouso; |
| Métodos suportados: |
| Backup Full, Incremental, Diferencial e Contínuo (CDP); |
| Backup de dispositivos físicos, virtuais, containers e dispositivos móveis; |
| Suporte a backup de dados e configurações de painéis de controle web como: |
| cPanel, Plesk e equivalentes; |
| Suporte a backup e restauração de aplicações como: |
| Microsoft SQL Server, MySQL, MariaDB, Oracle, SAP HANA, PostgreSQL, MongoDB; |
| Compatível com ambientes virtualizados e hypervisores: |
| VMware vSphere, Free ESXi, Hyper-V, RHEV, KVM, Proxmox; |
| Backup de servidores hospedados em Microsoft Azure e AWS; |
| Conversão entre formatos P2V, V2P, V2V, com suporte a restauração dissimilar (bare-metal recovery); |
| Opção de montar volumes de backup como discos legíveis diretamente pelo sistema de arquivos (Windows Explorer ou shell). |
| ***Suporte a Ambientes Colaborativos e Cloud SaaS*** |
| Backup nativo de ambientes colaborativos, com suporte a: |
| Microsoft 365 (Exchange, OneDrive, SharePoint, Teams, Reuniões); |
| Google Workspace (Gmail, Drive, Shared Drive, Agenda, Contatos); |
| Suporte a múltiplas organizações (multi-tenant); |
| Restauração granular de objetos, inclusive entre diferentes organizações; |
| Backup de dados criptografados com suporte a: |
| BitLocker, McAfee Endpoint Encryption, PGP Whole Disk Encryption; |
| Compatibilidade com ambientes com backup local (NAS/Storage) e remoto (cloud); |
| ***Recursos de Proteção e Segurança Integrada*** |
| Verificação automática de integridade dos dados backupeados; |
| Proteção contra ransomware e malware integrada à plataforma, com: |
| Scan nativo dos arquivos de backup; |
| Verificação de ameaças no momento do restore; |
| Backup forense com marcação de snapshots críticos; |
| Suporte à criação de backups imutáveis, protegidos contra exclusão ou sobrescrita, por prazo definido pela prefeitura; |
| Proteção contra exclusão não autorizada de backups; |
| Detecção e bloqueio de ameaças ao agente de backup instalado nos endpoints; |
| Controle de autenticação para acesso a dados sensíveis. |
| ***Orquestração de Recuperação de Desastres*** |
| Failover e failback de máquinas protegidas com: |
| Testes programados de failover; |
| Execução com simulação em nuvem (DR as a Service); |

| |
|---|
| Sincronização e failback automático; |
| Suporte à criação de runbooks personalizados, com orquestração de: |
| Ordem de inicialização dos serviços; |
| Criação de redes virtuais protegidas no ambiente de DR; |
| Aplicação de firewall e regras de DNS específicas; |
| Suporte a firewall no DR, configuração de DNS, VPN IPSec site-to-site, entre ambientes; |
| DR hospedado no Brasil com disponibilidade 24x7x365. |
| ***Segurança Cibernética e Recursos Avançados*** |
| Detecção e prevenção de ameaças integradas ao processo de backup e restore: |
| Antivírus, antimalware, anti-ransomware; |
| Prevenção de exploits e verificação de assinatura estendida; |
| Proteção no momento do restore com varredura de segurança; |
| Wipe remoto de dispositivos comprometidos; |
| Avaliação contínua de vulnerabilidades; |
| Monitoramento baseado em IA e machine learning; |
| Inventário de hardware e software dos dispositivos protegidos; |
| Gerenciamento de patches e atualizações críticas. |
| ***Requisitos de Compatibilidade*** |
| Suporte aos sistemas operacionais: |
| Windows Server 2008 e superiores; |
| Windows 7 ou superior; |
| Linux kernel 2.6.9 e superiores (RHEL, Debian, Ubuntu, CentOS); |
| MacOS X Maverick 10.9 e superiores; |
| Suporte aos hipervisores: |
| VMware vSphere, Free ESXi, Hyper-V, RHEV, KVM; |
| Suporte aos principais navegadores do mercadonavegadores: |
| Chrome, Firefox, Edge, Safari, IE; |
| Suporte a conectividade com NAS local sem custo adicional, se solicitado; |
| Suporte a expansão de armazenamento em nuvem a quente, sem interrupção. |
| ***Implantação Inicial*** |
| A contratada deverá realizar a configuração inicial da solução de backup, incluindo o licenciamento, instalação e aplicação de políticas de proteção para: |
| Todos os servidores físicos que a Prefeitura solicitar ou vier a instalar; |
| Todos os servidores virtuais existentes e futuros, conforme demanda da Prefeitura; |
| As estações de trabalho definidas como críticas ou VIPs, com base em critérios estabelecidos em conjunto com a área de TI da Prefeitura. |
| **Observação:** Não haverá limitação quanto ao número de dispositivos protegidos, desde que respeitado o volume de armazenamento contratado na nuvem. |
| A contratação contempla um volume inicial de até 10 TB de armazenamento em nuvem, a ser utilizado de acordo com os planos de backup e as políticas de retenção definidas pela Prefeitura. |
| **Observação:** Este volume poderá ser expandido sob demanda, mediante solicitação formal, à medida que a infraestrutura de backup evoluir ou os requisitos de retenção se ampliarem. |
| Além disso, caso seja solicitado, a solução de backup deverá ser configurada para utilizar dispositivos locais de armazenamento (como NAS ou pastas compartilhadas internas), disponibilizados pela própria Prefeitura. |
| Nos casos citados no item anterior (backup usando NAS locais), não haverá limitação de espaço adicional ou custo adicional, considerando que o armazenamento local será provido fora do escopo do fornecedor da solução. |
| ***Requisitos de Conformidade e Datacenter*** |
| A solução e o ambiente de DR deverão estar em datacenter no Brasil, com: |
| Certificação ISO 27001 (Segurança); |
| Certificação ISO 22301 (Continuidade de Negócios); |
| Classificação Tier III ou superior. |
| Desejável: |

| |
|---|
| Certificação ISO 27701 (Privacidade); |
| **Entregáveis e Treinamento** |
| **Entregáveis:** |
| Relatório técnico de implantação; |
| Lista de ativos protegidos e plano de proteção configurado; |
| Políticas de backup e DR por grupo ou sistema; |
| Relatório de validação com evidências de funcionamento da solução. |
| **Treinamento:** |
| Treinamento técnico para equipe da Prefeitura sobre: |
| Criação e gestão de planos de backup e restore; |
| Teste e execução de planos de DR (failover/failback); |
| Monitoramento de integridade e segurança dos dados. |

**Quadro-Resumo das Soluções Técnicas, Setup e Manutenção**
A presente contratação contempla a implantação e operação de um conjunto de soluções técnicas estratégicas, com diferentes modelos de implantação, manutenção e gerenciamento, conforme os requisitos funcionais e operacionais da Prefeitura.

O quadro a seguir apresenta uma visão consolidada das soluções previstas, indicando se exigem setup técnico inicial (implantação funcional), se demandam manutenção mensal contínua, além de observações específicas relevantes:

| Nº | Solução Técnica | Setup Inicial | Manutenção Mensal | Observações Específicas |
|---|---|---|---|---|
| 1 | Active Directory + File Server com DFS | Sim | Não | Manutenção será realizada pela equipe N3 da contratada. |
| 2 | Ferramenta de ITSM + Inventário (CMDB) | Sim | Sim | Inclui catálogo de serviços, inventário de ativos e integração com AD. |
| 3 | Ferramenta de RMM | Sim | Sim | Customização, criação de scripts, alertas, relatórios e cadastro de todos os dispositivos. |
| 4 | Monitoramento (Zabbix ou equivalente) | Sim | Sim | Cadastrar todos os ativos, configurar dashboards, mapas de rede e alertas. |
| 5 | Gestão de Logs e SIEM (Wazuh ou equivalente) | Sim | Sim | Parametrização completa, configuração de regras, alertas e integração com demais sistemas. |
| 6 | Análise de Vulnerabilidades Técnicas | Sim | Sim | Setup inclui primeira análise completa e geração de relatório técnico. |
| 7 | Antivírus com EDR e Filtro de Conteúdo | Sim | Sim | Instalação em todos os dispositivos definidos, configuração de políticas e filtros ativos. |
| 8 | Plataforma de Backup em Nuvem com Recuperação de Desastres (DR) | Sim | Sim | Setup com instalação, configuração de políticas e validação do ambiente com até 10 TB de armazenamento. |

**Observações sobre os Setups das Soluções**
Todas as soluções técnicas listadas devem ser implantadas de forma completa, funcional e operacional, conforme as diretrizes da Prefeitura. O setup inicial de cada solução não se limita à instalação do software, mas inclui também sua parametrização, personalização e ativação real em produção e treinamento e capacitação quando necessário, com cobertura total do ambiente e entrega pronta para uso.

| |
|---|
| **Active Directory + File Server com DFS:** instalação dos 2 controladores, criação das OUs, GPOs, replicação com DFS, definição de perfis de acesso, e inclusão de todas as máquinas no domínio. Migração de dados atuais da Prefeitura para o novo file server. |

| |
|---|
| **ITSM + Inventário (CMDB):** implantação da plataforma, definição do catálogo de serviços, estruturação e carga do CMDB, instalação dos agentes, integração com Active Directory e aplicação de políticas e SLAs. |
| **RMM:** instalação da plataforma, cadastro de todos os dispositivos da Prefeitura, configuração de tarefas automatizadas, relatórios técnicos, alertas e scripts de automação. |
| **Monitoramento:** inclusão de todos os ativos da Prefeitura (switches, servidores, links, APs etc.), criação de dashboards técnicos e gerenciais, definição de mapas de rede e configuração de alertas por criticidade. |
| **Gestão de Logs e SIEM:** instalação da solução, definição de fontes de logs (servidores, firewalls, endpoints), criação de regras de alerta e automação, dashboards de visibilidade e integração com ITSM. |
| **Análise de Vulnerabilidades:** configuração da ferramenta, execução da primeira análise de vulnerabilidades completa, geração de relatório técnico com recomendações, orientação para correção e planejamento de ciclo contínuo (pelo menos trimestral). |
| **Antivírus com EDR e Filtro de Conteúdo:** instalação do agente em todos os dispositivos definidos pela Prefeitura, definição de perfis de bloqueio, categorias de filtro de conteúdo, configuração de políticas e relatórios de operação. |
| **Backup em Nuvem com DR:** instalação e configuração dos agentes de backup, definição de políticas e retenções, validação do ambiente para até 10 TB de armazenamento inicial em nuvem, e, se solicitado, configuração para backup local via NAS ou pasta compartilhada. |

**Observação sobre a Manutenção Mensal das Soluções**

- A manutenção mensal das soluções será exigida somente enquanto houver custo recorrente associado à infraestrutura em nuvem, licenciamento ou suporte técnico contínuo.
- Caso a solução seja internalizada ou deixe de gerar custos, a manutenção mensal poderá ser descontinuada, mediante validação formal.
- A medição da manutenção será realizada com base em relatórios mensais detalhados, contendo:
  - Status de funcionamento e disponibilidade;
  - Volume de dados protegidos (backup);
  - Detecções e alertas (segurança);
  - SLAs cumpridos;
  - Evidências de operação técnica contínua.

**Cronograma de Implantação das Soluções Técnicas**

A implantação das soluções técnicas será realizada em etapas mensais, conforme o planejamento técnico abaixo, visando garantir a maturidade gradual do ambiente de TI e a adoção segura das ferramentas, processos e políticas. O cronograma leva em consideração a complexidade de cada solução, as dependências operacionais e a curva de aprendizado dos usuários.

| Mês | Atividade Principal |
|---|---|
| 1 | Implantação do Antivírus com EDR em todas as estações em funcionamento.<br>Implantação da solução de backup nas estações que hoje atuam como centralizadores de arquivos.<br>Execução de um gap Analysis de segurança da informação.<br>Elaboração das principais políticas e procedimentos de segurança para o município. |
| 2 | Início da implantação do Active Directory e File Server com DFS.<br>Início da implantação da ferramenta de ITSM + Inventário (CMDB).<br>Início da atuação assistida da equipe N1, N2 e N3, em conjunto com a equipe da Prefeitura. |
| 3 | Continuidade da configuração e finalização da implantação do AD + DFS.<br>Finalização e ativação da ferramenta de ITSM com catálogo e inventário inicial. |
| 4 | Implantação da ferramenta de RMM (gestão remota e scripts).<br>Implantação da solução de Monitoramento |
| 5 | Implantação da ferramenta de Gestão de Logs e SIEM<br>Implantação da ferramenta de análise de vulnerabilidades e a realização da primeira Análise de Vulnerabilidades Técnicas com emissão de relatório e planejamento das correções. |

| Mês | Atividade Principal |
|---|---|
| 6 | Consolidação de todas as ferramentas em produção.<br>Correções e ajustes pós-análise de vulnerabilidades.<br>Monitoramento da maturidade dos ambientes.<br>Continuidade do suporte técnico (N1, N2, N3) e atuação contínua da equipe de segurança. |
| Mês 7 em diante | Execução de rotinas de avaliação, revalidação e melhoria das ferramentas já implantadas.<br>Ajustes finos, treinamentos complementares, testes de DR e validações com a equipe interna.<br>Sustentação plena do ambiente com todas as soluções ativas. |

**Observações Finais sobre o Cronograma**

- O cronograma proposto poderá ser ajustado conforme a estratégia da Prefeitura, considerando fatores como a disponibilidade de infraestrutura, agenda institucional, priorização de áreas críticas e tempo de resposta dos fornecedores envolvidos.
- Toda execução de atividade dependerá de aprovação prévia da equipe da Prefeitura, que será responsável por liberar os acessos, ambientes, arquivos e equipes envolvidas no processo.
- A equipe de serviços especializados em segurança da informação atuará de forma transversal e contínua desde o primeiro mês, acompanhando e assessorando todas as fases da implantação.
- As atividades técnicas executadas deverão ser registradas no sistema ITSM e formalizadas por meio de relatórios mensais técnicos, utilizados como base para medição, validação de entregas e acompanhamento da evolução contratual.

**Requisitos de Privacidade e Proteção de Dados Pessoais**

Considerando as obrigações estabelecidas pela Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD), e tendo em vista que os serviços contratados podem envolver o tratamento direto ou indireto de dados pessoais e sensíveis, a empresa CONTRATADA atuará, legalmente, como operadora de dados pessoais, sendo a Prefeitura a controladora, nos termos do art. 5º, incisos VI e X da LGPD.

**Dados Pessoais Potencialmente Tratados**

Mesmo que o acesso direto a esses dados não seja parte da atividade principal da CONTRATADA, o simples fato de haver acesso potencial ou capacidade técnica de manipulação já caracteriza tratamento de dados pessoais, exigindo a aplicação de medidas específicas de proteção e conformidade. Entre os dados potencialmente tratados, destacam-se:

- Dados cadastrais e funcionais de servidores públicos municipais (cargos, remunerações, históricos);
- Dados pessoais de crianças e adolescentes (Educação e Assistência Social);
- Dados de saúde de munícipes (prontuários, diagnósticos, exames, agendamentos);
- Demais dados sensíveis armazenados em backups ou acessados durante a execução do contrato.

**Obrigações Mínimas da Contratada quanto à Privacidade**

A CONTRATADA deverá possuir, manter atualizados e apresentar, sempre que solicitado pela Administração Pública, os seguintes documentos e mecanismos:

- Política de Privacidade (interna e para terceiros);
- Plano de Gestão de Incidentes com notificação obrigatória à Prefeitura em até 24h;
- Relatório de Impacto à Proteção de Dados Pessoais (RIPD);
- Mapeamento de Fluxo de Dados (ROPA);
- Mecanismos de gestão de consentimento e atendimento aos titulares, quando aplicável;
- Termos de Confidencialidade firmados com todos os envolvidos;
- Relatório de Privacy by Design e Privacy by Default das soluções contratadas;
- Evidência de treinamentos regulares em privacidade e proteção de dados;
- Relatório técnico sobre minimização, necessidade e rastreabilidade de acessos.

A Prefeitura poderá, a qualquer tempo, requisitar evidências técnicas e relatórios que comprovem a aderência da contratada aos princípios e exigências da LGPD.

**Certificação ISO como Evidência de Conformidade**

Caso a CONTRATADA possua **certificação ISO/IEC 27701 válida e atualizada**, esta será aceita como evidência de implementação de um sistema de gestão de privacidade aderente à LGPD (Lei Geral de Proteção de Dados). Será exigido apenas o envio do certificado para validação.

**Comunicação de Incidentes**

Todo e qualquer incidente que envolva acesso indevido, vazamento, perda, modificação ou exposição de dados pessoais deverá ser comunicado formalmente à Prefeitura em até 24 horas, com a seguinte estrutura mínima:

- Descrição do incidente e impacto estimado;
- Categorias e volume de dados afetados;
- Causa raiz, quando identificada;
- Medidas de contenção, mitigação e recuperação adotadas;
- Ações preventivas propostas.

**Considerações Técnicas Finais**

**Validação Técnica e Checklist de Setup**

Para fins de aceitação contratual, será considerada como implantação efetiva de uma solução técnica apenas quando forem cumpridos, cumulativamente, os seguintes requisitos:

- Todas as funcionalidades descritas neste Termo de Referência estiverem ativas e operacionais;
- Todos os ativos previstos estiverem devidamente configurados, cadastrados ou integrados à solução;
- Existirem evidências técnicas, como relatórios, capturas de tela, registros de logs, dashboards operacionais ou acesso funcional validado;
- A equipe da Prefeitura tiver realizado a validação técnica do setup, com apoio da fiscalização contratual.

A aceitação de cada setup deverá ser formalizada por meio de checklist técnico padrão, assinado pela fiscalização do contrato, e será parte integrante do processo de medição e liberação de pagamentos.

**Auditoria Técnica e Fiscal da Prestação dos Serviços**

Todas as soluções contratadas e entregas técnicas executadas estarão sujeitas à auditoria técnica e à fiscalização pela Prefeitura, podendo incluir as seguintes ações:

- Testes funcionais nas soluções implantadas (ex.: restauração de backup, aplicação de políticas, geração de alertas, execução de scripts);
- Avaliação da conformidade dos SLAs pactuados;
- Amostragem técnica de estações de trabalho, servidores e sistemas cobertos;
- Validação dos controles de segurança, continuidade e integridade das soluções;
- Verificação do cumprimento dos requisitos definidos nos setups, políticas e rotinas de manutenção;
- Entrevistas com usuários atendidos, aplicação de pesquisas de satisfação e análise de indicadores de desempenho.

A contratada deverá manter registros auditáveis, logs técnicos e relatórios de operação devidamente organizados e acessíveis, sendo obrigatória sua apresentação sempre que requisitado pela fiscalização.

**Declaração das Soluções Tecnológicas Propostas**

Como parte integrante da proposta técnica, a licitante deverá apresentar declaração formal contendo a relação completa das soluções tecnológicas que pretende utilizar para atendimento aos itens deste Termo de Referência.

Essa declaração tem por objetivo assegurar a rastreabilidade, a transparência e a verificação da aderência das soluções ofertadas aos requisitos técnicos previstos no edital, nas provas de conceito e nas funcionalidades obrigatórias descritas neste documento.

A declaração deverá obrigatoriamente:

- Estar apresentada conforme modelo do Anexo 4 – Declaração das Soluções Tecnológicas Propostas;
- Informar, para cada solução:
  - O item correspondente no TR;
  - O nome da solução proposta;
  - A versão da solução (quando aplicável);
  - O fabricante responsável;
- Estar assinada por representante legal da licitante;

- Estar acompanhada da documentação técnica oficial (manual, datasheet, guia técnico, whitepaper, etc.) que comprove a aderência da solução aos requisitos do Termo de Referência, redigida em português ou inglês;
- Apresentar a documentação em formato PDF, organizada por solução;
- Permitir, opcionalmente, o acréscimo de links de referência para sites oficiais das soluções, como complemento à documentação anexada.

A ausência da declaração, a omissão de qualquer das soluções exigidas, ou a não apresentação da documentação técnica comprobatória acarretará a desclassificação da proposta técnica, nos termos do art. 59 da Lei nº 14.133/2021.

## 6. DOS RECURSOS ORÇAMENTÁRIOS:

**6.1.** As despesas para atender a esta licitação estão programadas em dotação orçamentária própria, prevista no orçamento do Município para o exercício de 2025, na classificação abaixo:

**UNIDADE: 02.07.01 – SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO E FINANÇAS - SEAF**
**2009 – MANUTENÇÃO DAS AÇÕES DA SEC. MUNICIPAL DE ADMINISTRAÇÃO**
**3390.40 – SERVICOS DE TEC. DA INFO. E COMUNICACAO - PJ**
**FONTES:**
**15000000 – RECURSOS NÃO VINCULADOS DE IMPOSTOS,**
**15010000 – OUTROS RECURSOS NÃO VINCULADOS.**

## 7. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO:

**7.1.** O custo estimado total da contratação é de **R$ 1.285.055,46 (um milhão, duzentos e oitenta e cinco mil, cinquenta e cinco reais e quarenta e seis centavos)**, conforme custos unitários apostos na tabela acima
**7.2.** O custo estimado foi apurado a partir de mapa de preços constante do processo administrativo, elaborado com base em orçamentos recebidos de empresas especializadas, em pesquisas de mercado.
**7.3.** O pagamento será efetuado em até 30 (trinta) dias após a entrega da nota fiscal devidamente atestada pelo setor competente, acompanhada de todas as certidões fiscais e trabalhista

## 8. DA SUBCONTRATAÇÃO.

8.1. É vedada a subcontratação total ou parcial dos serviços de mão de obra técnica contratada, incluindo as atividades de suporte técnico em múltiplos níveis (N1, N2, N3), gerenciamento operacional, serviços especializados em segurança da informação, atendimento a usuários, execução de políticas de segurança da informação e quaisquer outras funções diretamente relacionadas à entrega do objeto principal deste contrato.
8.2. Será admitida, contudo, a subcontratação de soluções técnicas, plataformas tecnológicas, serviços em nuvem (cloud computing), ferramentas de backup, antivírus, SIEM, RMM, ITSM e correlatos, desde que:

- a CONTRATADA mantenha responsabilidade integral pela execução, entrega, conformidade e qualidade dos serviços;
- tais soluções estejam identificadas, com respectivos fabricantes ou fornecedores, na proposta técnica;
- sejam observadas as exigências de confidencialidade, segurança da informação e proteção de dados pessoais, conforme legislação aplicável;
- os custos estejam contemplados na proposta de preços da CONTRATADA, sem repasse adicional à Contratante.

8.3. Em nenhuma hipótese a CONTRATADA poderá repassar, ceder ou delegar a terceiros a gestão, operação, coordenação ou execução direta dos serviços contratados de suporte técnico ou segurança da informação, sob pena de rescisão contratual e aplicação das sanções previstas.

## 9. DA ALTERAÇÃO SUBJETIVA.

**9.1.** 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. DO MODELO DE GESTÃO DO OBJETO E DO CONTRATO.

**10.1.** 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.
**10.2.** Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.
**10.3.** As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.
**10.4.** O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.
**10.5.** 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).
**10.6.** O fiscal do contrato será auxiliado pelos órgãos de assessoramento jurídico e de controle interno da Administração.
**10.7.** O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração.
**10.7.1.** O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados, nos termos da Lei nº 14.133, de 2021, art. 117, §1º.
**10.7.2.** Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção.
**10.7.3.** O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.
**10.7.4.** No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato.
**10.7.5.** O fiscal técnico do contrato comunicar ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual.
**10.8.** 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.
**10.8.1.** Caso ocorram descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência.
**10.9.** O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.
**10.9.1.** O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.
**10.9.2.** O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.
**10.9.3.** O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.
**10.9.4.** O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso.
**10.10.** 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.
**10.11.** O gestor do contrato deverá elaborará relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração.

## 11. DO CRITERIO DE JULGAMENTO

Em razão da natureza especializada dos serviços de tecnologia da informação e segurança da informação, da complexidade técnica do objeto e da necessidade de assegurar o mais elevado padrão de qualidade na execução contratual, o julgamento das propostas deverá ocorrer segundo o critério de Técnica e Preço, nos termos do art. 36 da Lei nº 14.133/2021.

Esse critério garante a escolha da proposta mais vantajosa para a Administração com base em dois fatores: a qualidade técnica da proposta (experiência e certificações) e a competitividade econômica do preço ofertado.

A ponderação entre os fatores será a seguinte:

- 60% (sessenta por cento) para a Proposta Técnica;
- 40% (quarenta por cento) para a Proposta de Preços.

A Nota Final (NF) será calculada com base na média ponderada entre o Índice Técnico (IT) e o Índice de Preço (IP), segundo a fórmula:

$$NF = (IT \times 60 + IP \times 40) / 10$$

Onde:

- IT = Índice Técnico, obtido conforme detalhamento no item 10.1;
- IP = Índice de Preço, proporcional ao menor preço apresentado.

Será exigido, como condição mínima de classificação, que a licitante atinja nota técnica **igual ou superior a 60 pontos**, a fim de que participe da etapa de análise de preços. Essa exigência visa assegurar que somente fornecedores com qualificação técnica compatível possam ser habilitados à fase final de julgamento.

**Avaliação Técnica: Composição e Pontuação**
A pontuação máxima da Proposta Técnica será de 100 pontos, distribuída da seguinte forma:

- Experiência Técnica – até 60 pontos

Apurada por meio de atestados de capacidade técnica emitidos por pessoas jurídicas de direito público ou privado, comprovando a execução de serviços compatíveis com os critérios estabelecidos neste TR.

- Fator Qualidade (Certificações Técnicas) – até 40 pontos

Aferida com base na apresentação de certificações ISO/IEC 27001 (Segurança da Informação) e ISO/IEC 27701 (Privacidade da Informação), em nome da licitante e com escopo aderente ao objeto do contrato.

**Experiência Técnica (Atestados de Capacidade Técnica) – 60 pontos**
A pontuação referente à experiência técnica da licitante será apurada com base na apresentação de atestados de capacidade técnica emitidos por pessoas jurídicas de direito público ou privado, que comprovem a execução anterior de serviços com escopo compatível aos exigidos nesta contratação.

Cada atestado que atenda aos requisitos técnicos descritos a seguir atribuirá até 6 (seis) pontos, totalizando até o limite máximo de 60 (sessenta) pontos.

| Critérios de Pontuação Técnica | Pontuação |
|---|---|
| **1. Implantação de Sistema de Gestão de Segurança da Informação (SGSI) com base na ISO/IEC 27001 ou equivalente - Atestado que comprove que a empresa executou projeto de implantação de SGSI conforme os princípios e controles definidos na norma ISO/IEC 27001 ou padrão equivalente, preferencialmente com posterior certificação da organização contratante.** | 6 pontos |
| **2. Elaboração de Políticas e Procedimentos de Segurança da Informação -** Atestado que comprove a execução de serviços voltados à elaboração de políticas, normas, procedimentos e planos de segurança, incluindo, entre outros: Política de Segurança da Informação, Política de Senhas, Política de Controle de Acesso, Plano de Continuidade, Plano de Resposta a Incidentes, Plano de Backup, Plano de Recuperação de Desastres. | 6 pontos |
| **3. Execução de Avaliação de Riscos ou Análise de Gaps em Segurança da Informação -** Atestado que comprove a realização de avaliação de riscos, análise de vulnerabilidades, ou gap analysis com base nos requisitos da norma ISO/IEC 27001, ISO 31000 ou frameworks reconhecidos. | 6 pontos |
| **4. Implantação de Solução ITSM (Sistema de Gestão de Chamados e Ativos de TI) -** Atestado que comprove a implantação de plataforma de ITSM com funcionalidades de abertura e gestão de chamados, controle de ativos, catálogo de serviços, base de conhecimento, escalonamento técnico e emissão de relatórios gerenciais. A solução deverá contemplar a gestão dos níveis de atendimento (N1, N2, N3) e integração com ferramentas de monitoramento. | 6 pontos |
| **5. Execução de Suporte Técnico Nível 1 e Nível 2 -** Atestado que comprove a prestação de serviços de atendimento técnico remoto e/ou presencial nos níveis 1 e 2, com classificação de chamados, atendimento por tipo de incidente, categorização e registro em ferramenta de service desk. Deve conter período de execução e escopo atendido. | 6 pontos |
| **6. Execução de Suporte Técnico Nível 3 -** Atestado que comprove a atuação técnica especializada para resolução de demandas complexas em ambientes de servidores, rede, segurança ou infraestrutura crítica, classificada como Suporte Nível 3. O atestado deve mencionar atuação corretiva, preventiva e/ou de melhoria contínua em ambiente corporativo. Deve conter período de execução e escopo atendido. | 6 pontos |
| **7. Implantação e Gerenciamento de Active Directory (AD) com redundância para Controle de Acesso -** Atestado que comprove a implantação e administração de ambientes com Active Directory, incluindo a criação e gestão de grupos, políticas de GPO, unidades organizacionais (OUs), autenticação integrada e estrutura de permissões por perfil. Inclui integração com serviços de diretório e autenticação. | 6 pontos |
| **8. Implantação e Gestão de Solução de Backup com Armazenamento em Nuvem -** Atestado que comprove o fornecimento, implantação, monitoramento e gestão de solução de backup com armazenamento em nuvem, incluindo políticas de retenção, versionamento, criptografia, e execução de testes de restauração. | 6 pontos |
| **9. Implantação de Solução de Gestão de Logs (SIEM) -** Atestado que comprove a implantação de solução de gestão e correlação de logs (SIEM), com coleta de eventos de segurança, análise em tempo real, criação de regras de alerta, dashboards operacionais e trilha de auditoria. Preferencialmente com integração a ativos diversos (servidores, firewalls, endpoints). | 6 pontos |
| **10. Implantação de Solução de Monitoramento Remoto e Disponibilidade de Ativos -** Atestado que comprove a implantação de ferramenta de monitoramento de ativos, recursos de rede, servidores e disponibilidade de sistemas, com geração de alertas, dashboards, acompanhamento de incidentes e relatórios de disponibilidade. | 6 pontos |

**Requisitos Obrigatórios dos Atestados:**

Todos os atestados apresentados deverão:

- Ser emitidos por pessoa jurídica de direito público ou privado;
- Estar em papel timbrado da entidade emitente, devidamente assinado por responsável legal;
- Conter descrição clara e objetiva dos serviços executados, alinhada com os critérios acima;

- Informar:
  - Nome da instituição contratante;
  - Período de execução;
  - Quantitativo ou abrangência do serviço;
  - Nome, cargo, telefone e e-mail do responsável pela emissão (para eventual diligência).

No caso de atestados emitidos por empresas privadas, poderão ser exigidos, em fase de análise técnica ou diligência, os seguintes documentos complementares:

- Cópia do contrato ou instrumento jurídico correspondente;
- Três últimas notas fiscais emitidas antes da publicação do edital;
- Reconhecimento de firma do signatário do atestado;
- Procuração ou comprovação dos poderes de representação do signatário, se aplicável.

Importante: Não serão aceitos atestados emitidos por empresas do mesmo grupo econômico, com sócios em comum, ou com vínculos societários entre emitente e licitante.

**Regras de Pontuação:**

- Cada atestado que comprove um dos critérios técnicos: 6 pontos;
- Não serão aceitos atestados compostos (que atendam mais de um critério em um único atestado sem clareza objetiva);
- Pontuação máxima total permitida: 60 pontos.

**Fator de Qualidade – Certificações Técnicas (até 40 pontos)**

A pontuação atribuída ao fator de qualidade técnica será aferida com base na apresentação de certificações formais emitidas por organismos acreditados, em nome da licitante (matriz ou filial), que demonstrem, de forma inequívoca, que a empresa possui sistemas de gestão implementados e operacionais, diretamente relacionados ao escopo desta contratação.

Tais certificações deverão atestar a conformidade da organização com normas internacionais amplamente reconhecidas, voltadas à segurança da informação e à proteção de dados pessoais, elementos centrais deste contrato, considerando o grau de criticidade dos serviços prestados.

Serão admitidas para fins de pontuação técnica as seguintes certificações:

- Certificação ISO/IEC 27001 – até 25 (vinte e cinco) pontos: válida para empresas que possuam sistema de gestão da segurança da informação implementado, com escopo compatível com atividades de operação de infraestrutura de TIC, consultoria em segurança da informação, suporte técnico especializado em tecnologia da informação. O escopo técnico deverá estar claramente vinculado às obrigações contratuais previstas neste Termo de Referência.
- Certificação ISO/IEC 27701:2019 – até 15 (quinze) pontos: válida para empresas certificadas em sistema de gestão da privacidade da informação, com escopo compatível com atividades de operação de infraestrutura de TIC, consultoria em segurança da informação, suporte técnico especializado em tecnologia da informação. O escopo técnico deverá estar claramente vinculado às obrigações contratuais previstas neste Termo de Referência.

As certificações apresentadas deverão obrigatoriamente atender aos seguintes requisitos formais:

- Estar válidas na data de abertura da licitação, conforme indicado no documento oficial emitido pelo organismo certificador;
- Ser apresentadas em cópia simples ou autenticada, em idioma original;
- Conter a identificação expressa da unidade certificada, seja matriz ou filial, que participará da execução contratual;
- Apresentar o escopo técnico certificado de forma clara e objetiva, seja diretamente no certificado ou em declaração complementar do organismo certificador, demonstrando a compatibilidade com as exigências deste TR.

A ausência das certificações referidas não configura fator impeditivo à habilitação da licitante, todavia, sua apresentação conferirá pontuação técnica adicional e objetiva, representando diferencial competitivo para empresas que atuem com nível de maturidade institucional de segurança da informação e privacidade alinhado às boas práticas de mercado e à normativa técnica vigente.

O objetivo desta avaliação é fomentar a seleção de empresas com capacidade organizacional comprovada, estruturalmente aderentes ao modelo de governança e segurança requerido pela Administração Pública, sobretudo no que tange à integridade, disponibilidade, confidencialidade e privacidade das informações tratadas.

**Cálculo da Nota Final da Proposta**

Para a definição da proposta mais vantajosa à Administração, será adotada metodologia de julgamento pelo critério de Técnica e Preço, conforme disposto no art. 36 da Lei nº 14.133/2021 e conforme detalhamento constante do item 10 deste Termo de Referência. A avaliação das propostas seguirá uma abordagem objetiva e proporcional, que considera a qualificação técnica da licitante e a vantajosidade econômica de sua proposta.

**Etapas de Avaliação e Fórmulas Aplicadas**

**a) Cálculo da Nota Técnica (NT)**

A Nota Técnica será composta pela soma dos pontos obtidos nos seguintes componentes:

- Experiência Técnica (até 60 pontos) – conforme descrito no subitem 10.1.1;
- Fator de Qualidade – Certificações Técnicas (até 40 pontos) – conforme descrito no subitem 10.1.2.
-

A pontuação máxima da NT será, portanto, de 100 (cem) pontos.

**b) Cálculo do Índice Técnico (IT)**

A nota técnica atribuída a cada licitante será convertida em um índice padronizado, proporcional à melhor nota técnica recebida entre todas as concorrentes, mediante a seguinte fórmula:

$$IT = (NPTp / NPTa) \times 10$$

Onde:

- IT = Índice Técnico da licitante avaliada;
- $NPT_p$ = Nota da Proposta Técnica da licitante avaliada;
- $NPT_a$ = Maior Nota Técnica entre todas as propostas apresentadas.

Esse método garante que a proposta tecnicamente mais bem pontuada receba índice igual a 10, servindo de base para a proporcionalidade das demais.

**c) Cálculo do Índice de Preço (IP)**

A pontuação referente ao preço será igualmente convertida em índice, com base no menor preço global apresentado entre todos os licitantes, conforme fórmula:

$$IP = (MP / VPP) \times 10$$

Onde:

- IP = Índice de Preço da licitante;
- MP = Menor Preço Global apresentado entre todas as propostas;
- VPP = Valor da Proposta de Preço da licitante avaliada.

Dessa forma, o menor preço apresentado receberá índice 10, e os demais serão ajustados proporcionalmente.

**d) Cálculo da Nota Final (NF)**

A Nota Final será obtida mediante ponderação entre o Índice Técnico (IT) e o Índice de Preço (IP), segundo os pesos previamente estabelecidos:

- 60% para o componente técnico;
- 40% para o componente preço.

A fórmula de cálculo da NF será:

$$NF = (IT \times 60 + IP \times 40) / 100$$

Onde:

- **NF** = Nota Final da licitante;

- **IT** = Índice Técnico;
- **IP** = Índice de Preço.

**e) Classificação Final**
A licitante que obtiver a **maior Nota Final (NF)** será classificada em **primeiro lugar**, observadas as demais condições de habilitação jurídica, regularidade fiscal e trabalhista, qualificação econômico-financeira e ausência de impedimentos legais. Em caso de empate na Nota Final, aplicar-se-á o disposto nos art. 60 da Lei nº 14.133/2021.

13.2.1 **Quadro de Autodeclaração Técnica**
Para fins de avaliação técnica, o licitante deverá preencher o Quadro de Autodeclaração Técnica obrigatoriamente (conforme modelo).

Neste quadro, a licitante deverá declarar:
- Se atende ou não a cada critério técnico previsto nos subitens 10.1.1 (Experiência Técnica) e 10.1.2 (Fator de Qualidade – Certificações Técnicas);
- Se anexa ou não a comprovação documental correspondente;

O preenchimento correto, completo e coerente deste quadro é de responsabilidade da licitante, não substituindo, em hipótese alguma, a entrega efetiva dos documentos comprobatórios originais, que são imprescindíveis à validação da pontuação técnica pela Comissão de Julgamento.

A pontuação estimada poderá ser indicada pela licitante como referência preliminar, ficando a atribuição da pontuação definitiva condicionada à validação pela Comissão Técnica de Julgamento durante a fase de análise técnica das propostas.

A pontuação atribuída será validada exclusivamente com base nas evidências documentais apresentadas.

2 **Quadro de Autodeclaração Técnica**
**Observação:** Este quadro deve ser preenchido e assinado pela licitante, como parte integrante da proposta técnica. O objetivo é permitir a autodeclaração do atendimento aos critérios técnicos previstos no Termo de Referência, com a respectiva indicação de cumprimento e entrega dos documentos comprobatórios. A pontuação será atribuída exclusivamente com base nos documentos comprobatórios entregues, sendo este quadro meramente auxiliar para fins de organização da análise técnica.

2.1.1.1 **Quadro de Autodeclaração – Experiência Técnica (até 60 pontos)**

| Item | Critério Técnico | Cumpre? (Sim/Não) | Comprovação Anexa? (Sim/Não) |
|---|---|---|---|
| 1 | Implantação de SGSI com base na ISO/IEC 27001 | | |
| 2 | Elaboração de Políticas e Procedimentos de Segurança da Informação | | |
| 3 | Avaliação de Riscos ou Gap Analysis com base na ISO 27001 ou 31000 | | |
| 4 | Implantação de Solução ITSM (Gestão de Chamados e Ativos) | | |
| 5 | Execução de Suporte Técnico N1 e N2 | | |
| 6 | Execução de Suporte Técnico N3 | | |
| 7 | Implantação e Administração de Active Directory (AD) | | |
| 8 | Implantação e Gestão de Backup com Armazenamento em Nuvem | | |
| 9 | Implantação de Solução de Gestão de Logs (SIEM) | | |
| 10 | Implantação de Solução de Monitoramento Remoto e Disponibilidade | | |

| Item | Critério Técnico | Cumpre? (Sim/Não) | Comprovação Anexa? (Sim/Não) |
|---|---|---|---|
| **Total de Pontos (máximo 60):** | | | |

2.1.1.2 **Quadro de Autodeclaração – Certificações Técnicas (até 40 pontos)**

| Item | Certificação Técnica | Cumpre? (Sim/Não) | Comprovação Anexa? (Sim/Não) |
|---|---|---|---|
| 11 | Certificação ISO/IEC 27001 – até 25 pontos | | |
| 12 | Certificação ISO/IEC 27701 – até 15 pontos | | |
| **Total de Pontos (máximo 40):** | | | |

13.1.2 **Apresentação das Propostas Técnica e de Preço**

A licitante deverá apresentar, de forma separada e organizada, os seguintes documentos como parte integrante da proposta:

**a) Proposta de Preço:**

Deverá ser apresentada conforme o modelo padronizado constante – Modelo de Proposta de Preço, contendo todos os itens previstos neste Termo de Referência. A proposta deverá seguir obrigatoriamente as instruções indicadas abaixo:

| Item | Descrição | Unidade de Medida | Implantação (Setup) | Manutenção Mensal | Banco de Horas (USTs) | Valor Anual |
|---|---|---|---|---|---|---|
| 1 | Gerenciamento Técnico e Operacional do Contrato - Presencial e Remoto | Mês de vigência contratual | | | | |
| 2 | Serviços Técnicos de Suporte Nível 1 (N1) - 24x7 - Remoto | Mês de vigência contratual com disponibilidade de até 500 chamados no mês corrente. | | | | |
| 3 | Serviços Técnicos de Suporte Nível 2 (N2) - 24x7 - Remoto e Presencial | Mês de vigência contratual com disponibilidade de até 150 chamados no mês corrente. | | | | |
| 4 | Serviços Técnicos de Suporte Nível 3 (N3) - 24x7 - Remoto e Presencial | Mês de vigência contratual com disponibilidade de até | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 50 chamados no mês corrente. | | | | |
| 5 | Serviços Especializados de Segurança da Informação - 24x7 - Remoto e Presencial | UST - Contrato anual com 1200 UST | | | | |
| 6 | Implantação de Solução de Active Directory Redundante com File Server e DFS | Implantação (setup) | | | | |
| 7 | Implantação da Solução de ITSM com Módulo de Inventário e CMDB | Implantação (setup) + Mês de vigência contratual | | | | |
| 8 | Implantação da Solução de RMM (Remote Monitoring and Management) - Para até 600 máquinas (servidores e desktops) | Implantação (setup) + Mês de vigência contratual | | | | |
| 9 | Implantação da Solução de Monitoramento de Ativos, Servidores, Redes e Sistemas | Implantação (setup) + Mês de vigência contratual | | | | |
| 10 | Implantação da Solução de Gestão de Logs e SIEM | Implantação (setup) + Mês de vigência contratual | | | | |
| 11 | Implantação de Solução de Análise de Vulnerabilidade Técnica - servidores, desktops, sistemas e rede | Implantação (setup) + Mês de vigência contratual | | | | |
| 12 | Solução de Antivírus com EDR e Filtro de Conteúdo - 580 licenças (servidores e desktops) | Implantação (setup) + Mês de vigência contratual | | | | |
| 13 | Solução de Backup em Nuvem com Segurança Avançada e Recuperação de Desastres - 10TB de armazenamento em | Implantação (setup) + Mês de vigência contratual | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | nuvem localizados em Datacenter no Brasil | | | | | |
| **Subtotal** | | | | | | |

**Valor Global da Proposta:** R$ _____ (valor por extenso)

**Instrução adicional:** "A licitante deverá preencher o valor global da proposta neste campo, apresentando-o em reais (R$) com duas casas decimais e, obrigatoriamente, também por extenso."

7.2 **Divergência entre valores unitários e valor global**

Em caso de divergência entre os valores unitários indicados na tabela, no subtotal e o valor global apresentado ao final, prevalecerão os valores unitários. A Administração procederá à correção aritmética da proposta, adotando o somatório dos itens como base para o valor global.

Caso a divergência comprometa a exequibilidade da proposta ou indique erro material grave, a proposta poderá ser desclassificada, conforme previsto no art. 59, I, da Lei nº 14.133/2021.

7.3 **Instruções obrigatórias para preenchimento da proposta de preços:**

1. A licitante deverá preencher integralmente o modelo acima, conforme os quantitativos e escopo previstos neste Termo de Referência.
2. Todos os valores individuais constantes da tabela de proposta deverão ser expressos em reais (R$), com duas casas decimais, contemplando todos os encargos incidentes, tais como tributos, insumos, licenças, serviços de terceiros, fretes, encargos sociais, trabalhistas, previdenciários, despesas com deslocamento e quaisquer outros custos diretos ou indiretos necessários para o pleno cumprimento do objeto, não sendo admitido qualquer ônus adicional à Administração.
3. A linha de Subtotal deverá ser obrigatoriamente preenchida pela licitante, contendo o somatório de cada coluna: valores de implantação (setup), manutenção mensal e banco de horas (se houver). Esses subtotais devem corresponder à soma das linhas de cada item da tabela principal.
4. O Valor Global da proposta deverá considerar o **somatório dos valores de implantação, manutenção mensal e banco de horas (USTs)**, conforme aplicável. O Valor Global da Proposta deverá representar o somatório final de todos os subtotais apresentados. O valor global deverá ser apresentado ao final da tabela, expresso em reais (R$) com duas casas decimais e descrito por extenso.
5. A proposta deverá ser apresentada em papel timbrado da licitante, com a assinatura do responsável legal, contendo CNPJ, endereço completo e contato oficial.
6. É vedada a apresentação de planilha em formato diferente do modelo estabelecido neste anexo. A utilização de modelos próprios, incompletos ou despadronizados acarretará a desclassificação da proposta.
7. A proposta de preços deverá ter validade mínima de 60 (sessenta) dias, contados a partir da data de abertura das propostas.
8. Em campos da tabela onde não se aplicar a cobrança de determinado item (por exemplo, ausência de implantação, manutenção mensal ou banco de horas), a licitante deverá preencher o valor com "R$ 0,00", para manter a consistência da estrutura da proposta e viabilizar a correta apuração do valor global.

7.4 **Instrução Complementar – Obrigatoriedade da Declaração**

Além da tabela de preços preenchida conforme o modelo acima, a proposta de preços deverá conter, obrigatoriamente, em documento anexo ou no corpo da própria proposta, a seguinte declaração expressa, assinada pelo representante legal da licitante:

**Declaração Obrigatória da Licitante**

A licitante, por meio de seu representante legal, declara, para os devidos fins, que:

- Está integralmente ciente e de acordo com todas as exigências constantes no Termo de Referência e seus anexos;
- A proposta apresentada contempla todos os encargos diretos e indiretos, tributos, insumos, ferramentas, licenças, deslocamentos, pessoal técnico, suporte e quaisquer outras despesas necessárias à perfeita execução dos serviços;
- Os valores apresentados estão expressos em reais (R$), com duas casas decimais, e possuem validade mínima de 60 (sessenta) dias;
- Compromete-se, caso vencedora, a executar o objeto proposto nos exatos termos da documentação apresentada, sem omissões ou exclusões não justificadas;
- Reconhece como válida e aceita a estrutura de preços por item, os métodos de medição, as obrigações e as sanções previstas neste Termo de Referência.

A ausência desta declaração na proposta poderá ensejar a desclassificação da proposta, por vício formal ou por descumprimento das exigências do Termo de Referência.

**b) Proposta Técnica:**
Deverá conter a Declaração das Soluções Tecnológicas, conforme modelo, e o Quadro de Autodeclaração Técnica, acompanhado dos documentos comprobatórios exigidos.

**Declaração das Soluções Técnicas Propostas**

| Item | Descrição | Solução Proposta | Versão Solução | Fabricante |
|---|---|---|---|---|
| 1 | Solução de ITSM com Módulo de Inventário e CMDB | | | |
| 2 | Solução de RMM (Remote Monitoring and Management) | | | |
| 3 | Solução de Monitoramento de Ativos, Servidores, Redes e Sistemas | | | |
| 4 | Solução de Gestão de Logs e SIEM | | | |
| 5 | Solução de Análise de Vulnerabilidade Técnica | | | |
| 6 | Solução de Antivírus com EDR e Filtro de Conteúdo - 580 licenças (servidores e desktops) | | | |
| 7 | Solução de Backup em Nuvem com Segurança Avançada e Recuperação de Desastres | | | |

**Declaração:**
A LICITANTE, por meio de seu representante legal, declara, para os devidos fins, que:
1. As soluções tecnológicas acima listadas serão integralmente utilizadas na execução dos serviços objeto deste certame;
2. Todas as soluções propostas estão em conformidade com os requisitos técnicos estabelecidos no Termo de Referência e na Prova de Conceito (PoC);
3. A documentação técnica oficial que comprova a aderência das soluções encontra-se anexa a esta declaração, organizada por item correspondente, em formato PDF, redigida em português ou inglês;
4. Eventuais links para páginas oficiais do fabricante foram incluídos como referência complementar, não substituindo a documentação anexa;
5. Está ciente de que a omissão de qualquer item, a ausência da documentação ou o não atendimento às exigências poderá acarretar a desclassificação da proposta técnica, nos termos da Lei nº 14.133/2021.

**OBSERVAÇÃO:** A apresentação completa e correta desses documentos é condição obrigatória para pontuação na fase de julgamento técnico, nos termos definidos neste Termo de Referência.

## 12. DAS REGRAS BÁSICAS DO REGISTRO DE PREÇO.

12.1. Não será utilizado nessa contratação o Sistema de Registro de Preço

## 13. PROVA DE CONCEITO.

13.1. Como etapa complementar à análise técnica documental, será realizada Prova de Conceito (PoC), com caráter eliminatório, destinada à demonstração prática da eficácia, aderência e usabilidade das soluções ofertadas pelas licitantes. O objetivo da PoC é assegurar que os sistemas propostos atendam, de forma objetiva e verificável, aos requisitos técnicos estabelecidos neste Termo de Referência, antes da celebração contratual definitiva.

13.2. Serão obrigatoriamente submetidas à PoC as seguintes soluções críticas para o funcionamento do ambiente técnico-operacional da Administração:

- Solução de ITSM com Módulo de Inventário e CMDB;
- Solução de RMM (Remote Monitoring and Management);
- Solução de Monitoramento de Ativos e Serviços;
- Solução de SIEM (Gerenciamento de Logs e Eventos de Segurança);
- Solução de Backup Gerenciado com Armazenamento em Nuvem;
- Solução de Atendimento via WhatsApp.

13.3, A demonstração deverá ocorrer em ambiente controlado (sandbox ou instância real de testes), com avaliação presencial pela equipe técnica da Administração ou, alternativamente, por meio de comissionamento remoto assistido, conforme data informada pela Comissão de Avaliação.

13.4. Será considerada aprovada na Prova de Conceito a licitante que comprovar o atendimento integral (100%) aos critérios técnicos estabelecidos. A não demonstração, a inconformidade com qualquer um dos requisitos exigidos ou a impossibilidade de comprovação técnica no momento da PoC resultará na desclassificação da proposta, conforme disposto no art. 59 da Lei Federal nº 14.133/2021.

13.5. Observação: A Administração se reserva o direito de solicitar, durante a realização da PoC, simulações complementares, testes adicionais ou questionamentos técnicos, desde que relacionados às funcionalidades previstas neste Termo de Referência, a fim de verificar a plena compatibilidade das soluções ofertadas.

13.6. Os baremas de avaliação técnica da PoC, com seus respectivos critérios e parâmetros objetivos, estão detalhados na **Tabelas de Avaliação da Prova de Conceito**:

**Prova de Conceito – Sistema de ITSM (Gestão de Chamados, Inventário e CMDB)**

| Nº | Critério Avaliado | Atendido (✓/✗) | Observações da Comissão |
|---|---|---|---|
| 1 | A solução está hospedada em nuvem protegida por WAF ativo | | |
| 2 | Possui autenticação multifator (MFA) ou integração com SSO | | |
| 3 | Possui módulo completo de CMDB com inventário de hardware e software integrado | | |
| 4 | Permite abertura de chamados via painel web, e-mail e API externa | | |
| 5 | Suporta classificação de chamados por tipo: incidente, requisição, problema, mudança, projeto | | |
| 6 | Possui catálogo de serviços customizável conforme ITIL | | |
| 7 | Implementa regras de SLA com urgência, impacto e prioridade | | |
| 8 | Permite atribuição de chamados por perfis/grupos e diferentes níveis de usuário | | |

| Nº | Critério Avaliado | Atendido (✓/✗) | Observações da Comissão |
|---|---|---|---|
| 9 | Mantém log completo de ações em chamados com data, hora e responsável | | |
| 10 | Integração nativa com Active Directory (LDAP) para autenticação e permissões | | |
| 11 | Apresenta dashboards operacionais e gerenciais em tempo real | | |
| 12 | Plataforma conta com ambiente de disaster recovery estruturado | | |
| 13 | Possui possibilidade de operação futura em ambiente on-premises | | |
| 14 | Estrutura com mapa de dados aberto e documentação técnica disponível para internalização futura | | |
| 15 | Permite geração de relatórios customizados (PDF, CSV, Excel) | | |
| 16 | Sistema de pesquisa de satisfação automatizada após encerramento de chamados | | |
| 17 | Permite gestão de projetos com tarefas, cronogramas e relacionamento com chamados | | |
| 18 | Interface responsiva com acesso por desktop, tablet e smartphone | | |
| 19 | Possibilidade de customização visual com identidade da Prefeitura (cores, logotipo, textos) | | |
| 20 | Manual técnico da ferramenta está disponível com estrutura de serviços e papéis configurados | | |
| **Total de Pontos (máximo 20):** | | | |

**Prova de Conceito – Solução de RMM (Remote Monitoring and Management)**

| Nº | Critério Avaliado | Atendido (✓/✗) | Observações da Comissão |
|---|---|---|---|
| 1 | Plataforma acessível via navegador web, com compatibilidade com os navegadores modernos (Chrome, Edge, Firefox, Safari) | | |
| 2 | Compatibilidade com múltiplos sistemas operacionais (Windows, Linux, MacOS) | | |
| 3 | Autenticação obrigatória com duplo fator (MFA) para acessos administrativos | | |
| 4 | Controle granular de permissões por perfil de usuário (admin, operador, auditor, etc.) | | |
| 5 | Segmentação lógica dos equipamentos monitorados por secretaria, unidade organizacional ou grupo técnico | | |

| Nº | Critério Avaliado | Atendido (✓/✗) | Observações da Comissão |
|---|---|---|---|
| 6 | Acesso remoto completo aos dispositivos monitorados (interface gráfica e terminal) | | |
| 7 | Acesso remoto via linha de comando (CMD, PowerShell, Bash, Shell) | | |
| 8 | Gerenciamento remoto de arquivos e serviços do sistema operacional | | |
| 9 | Execução remota de scripts (PowerShell, Shell, Python, etc.) | | |
| 10 | Agendamento de tarefas automatizadas e deploy em massa para grupos de dispositivos | | |
| 11 | Checagens automatizadas com base em métricas (CPU, disco, memória, logs, serviços) | | |
| 12 | Coleta automática e periódica de inventário de hardware e software | | |
| 13 | Identificação e controle de atualizações de sistema operacional (patch management) | | |
| 14 | Relatórios prontos e customizáveis: ativos desconectados, máquinas desatualizadas, softwares instalados | | |
| 15 | Log completo de todas as ações realizadas pelos usuários, com data, hora e responsável | | |
| 16 | Possibilidade de migração futura para ambiente on-premises da Prefeitura | | |
| **Total de Pontos (máximo 18):** | | | |

**Prova de Conceito – Plataforma de Monitoramento**

| Nº | Critério Avaliado | Atendido (✓/✗) | Observações da Comissão |
|---|---|---|---|
| 1 | Monitora links de internet e conexões VPN | | |
| 2 | Monitora switches, roteadores, access points e firewalls | | |
| 3 | Monitora servidores com sistemas operacionais Windows e Linux | | |
| 4 | Monitora sensores IoT e câmeras IP | | |
| 5 | Monitora sistemas internos, sites públicos e aplicações web | | |
| 6 | Monitora bancos de dados relacionais (ex: MySQL, PostgreSQL, Oracle) | | |
| 7 | Compatível com métodos de coleta SNMP, ICMP (ping), e conexões via agentes | | |
| 8 | Possui dashboard personalizável com visão em tempo real dos ativos monitorados | | |

| Nº | Critério Avaliado | Atendido (✓/✗) | Observações da Comissão |
|---|---|---|---|
| 9 | Permite criação de mapas de rede personalizados (hierárquicos ou georreferenciados) | | |
| 10 | Permite definição de gatilhos inteligentes (triggers) para alertas por criticidade ou comportamento | | |
| 11 | Envia alertas por e-mail, SMS, Telegram e Webhook/API | | |
| 12 | Integra-se com plataforma ITSM para registro automático de incidentes | | |
| 13 | Realiza monitoramento e cálculo automático de SLA por ativo ou sistema | | |
| 14 | Gera relatórios de disponibilidade, tempo médio de indisponibilidade e falhas recorrentes | | |
| 15 | Possibilidade de migração futura para ambiente on-premises da Prefeitura | | |
| **Total de Pontos (máximo 15):** | | | |

**Prova de Conceito – Solução de SIEM e Gestão de Logs**

| Nº | Critério Avaliado | Atendido (✓/✗) | Observações da Comissão |
|---|---|---|---|
| 1 | Coleta e análise de eventos de segurança em tempo real de endpoints, rede e nuvem | | |
| 2 | Coleta de logs de sistemas operacionais, aplicações e serviços | | |
| 3 | Detecção de anomalias, erros, falhas e indicadores de comprometimento (IoCs) | | |
| 4 | Integração com base de dados de vulnerabilidades (CVEs) e detecção ativa de vulnerabilidades | | |
| 5 | Avaliação automatizada da configuração de segurança (SCA) conforme benchmarks como CIS | | |
| 6 | Monitoramento de integridade de arquivos (FIM) com geração de alertas por alterações | | |
| 7 | Geração de relatórios de conformidade para normas como ISO 27001, PCI, NIST e LGPD | | |
| 8 | Dashboards customizáveis com visão por tipo de alerta, área ou sistema | | |
| 9 | Execução automática de ações de resposta (ex: bloqueio de IP, encerramento de processo, envio de comando) | | |
| 10 | Suporte a APIs REST, Webhooks e integração com ferramentas externas (ITSM, visualização, automação) | | |
| 11 | Compatibilidade com sistemas operacionais Linux e Windows | | |

| Nº | Critério Avaliado | Atendido (✓/✗) | Observações da Comissão |
|---|---|---|---|
| 12 | Integração com plataformas de nuvem e SaaS (ex: Azure, AWS, Microsoft 365, GitHub) | | |
| 13 | Possibilidade de investigação por hunting (MITRE ATT&CK, regras customizadas, IOC e Threat Intelligence) | | |
| 14 | Geração de relatórios automatizados com exportação em PDF, CSV ou por API | | |
| 15 | Possibilidade de migração futura para ambiente on-premises da Prefeitura | | |
| **Total de Pontos (máximo 15):** | | | |

**Prova de Conceito – Solução de Backup Gerenciado com Segurança Avançada e Recuperação de Desastres**

| Nº | Critério Avaliado | Atendido (✓/✗) | Observações da Comissão |
|---|---|---|---|
| 1 | Plataforma SaaS com acesso via console web, protegido por autenticação multifator (MFA) | | |
| 2 | Perfis de usuário com permissões granulares (admin, operação, auditoria etc.) e trilha de auditoria detalhada | | |
| 3 | Criação de planos de backup personalizados com múltiplos destinos (nuvem, local, NAS) e retenção configurável | | |
| 4 | Criptografia AES-256 para dados em trânsito e em repouso | | |
| 5 | Proteção contra exclusão não autorizada de backups (backup imutável) | | |
| 6 | Suporte à expansão de armazenamento em nuvem a quente, sem interrupção dos serviços | | |
| 7 | Backup de Microsoft 365 (Exchange, OneDrive, SharePoint, Teams) e restauração granular entre organizações | | |
| 8 | Suporte a ambientes com backup local (NAS/Storage) e remoto (cloud compatível com S3, Azure, AWS) | | |
| 9 | Backup de ambientes virtualizados com suporte a hypervisores: VMware, Hyper-V, Proxmox, KVM, RHEV, Free ESXi | | |
| 10 | Backup de bancos de dados: Microsoft SQL Server, MySQL, PostgreSQL | | |
| 11 | Proteção contra ransomware integrada (varredura no backup e no restore, snapshots forenses, agentes protegidos) | | |
| 12 | Orquestração de DR com failover/failback, execução simulada, runbooks personalizados e redes virtuais protegidas | | |
| 13 | Compatibilidade com sistemas operacionais Windows, Linux, MacOS, e dispositivos móveis (quando aplicável) | | |

| Nº | Critério Avaliado | Atendido (✓/✗) | Observações da Comissão |
|---|---|---|---|
| 14 | Montagem de volumes de backup como unidades acessíveis pelo sistema operacional (exploração direta de arquivos) | | |
| 15 | Datacenter no Brasil com certificações mínimas: Tier III, ISO 27001, ISO 22301 | | |
| **Total de Pontos (máximo 15):** | | | |

**Plataforma de Atendimento via WhatsApp com Monitoramento e Pesquisa de Satisfação**

| Nº | Critério Avaliado | Atendido (✓/✗) | Observações da Comissão |
|---|---|---|---|
| 1 | A plataforma registra integralmente as conversas, com controle por atendente e por grupo | | |
| 2 | Permite o envio e recebimento de mensagens de texto, áudios, imagens e arquivos | | |
| 3 | Aplica automaticamente pesquisa de satisfação ao final de cada atendimento | | |
| 4 | Em caso de nota 1, 2 ou 3, envia pergunta complementar para justificativa ou reabertura do atendimento | | |
| 5 | Mede e registra tempo de resposta, tempo de atendimento total e tempo médio por técnico e por grupo | | |
| **Total de Pontos (máximo 5):** | | | |

## 13. DO PAGAMENTO.

14.1. O pagamento será realizado no prazo máximo de até 30 (trinta) dias, contados a partir do recebimento da Nota Fiscal ou Fatura, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado, sempre após a realização das entregas.
14.2. Considera-se ocorrido o recebimento da nota fiscal ou fatura no momento em que o órgão contratante atestar a execução do objeto do contrato.
14.3. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 Lei nº 14.133/2021.
14.4. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.
14.5. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.
14.6. Antes de cada pagamento à contratada, será realizada de forma on-line consulta aos sítios eletrônicos oficiais para verificar a manutenção das condições de habilitação exigidas no edital.
14.7. Constatando-se a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

14.8. Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta on-line mediante consulta aos sítios eletrônicos oficiais para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.
14.9. Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.
14.10. Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.
14.11. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação de habilitação.
14.11.1. Será rescindido o contrato em execução com a contratada inadimplente, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante.
14.12. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.
14.12.1. A Contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123/2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

## 15. DO REAJUSTE.

15.1. Os preços contratados poderão sofrer reajuste, cuja data-base está vinculada à data do orçamento estimado, nos termos do art. 25, §7º da Lei nº 14.133/2021.
15.2. Nos reajustes subsequentes ao primeiro, o intervalo mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.
15.3. No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.
15.4. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.
15.5. Caso o índice estabelecido para reajuste venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.
15.6. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.
15.7. O reajuste será realizado por apostilamento.

## 16. DAS HIPÓTESES DE RESCISÃO

**16.1.** O futuro contrato poderá ser rescindido, a critério da Contratante, nas hipóteses de inadimplemento parcial ou total de quaisquer obrigações contidas neste termo de referência, nos termos do art. 137 da Lei Federal 14.133/2021, desde que efetivamente reste comprovado prejuízo à finalidade pública pretendida com a contratação;
**16.2.** Cabe à parte prejudicada ou interessada a comprovação do efetivo prejuízo que justifique a rescisão contratual, caso ocorra quaisquer dos motivos indicados na legislação;
**16.3.** A rescisão contratual será processada nos autos de processo de gestão, sempre se garantindo o contraditório e a ampla defesa;
**16.4.** Na ocorrência de rescisão contratual, ficam assegurados os direitos da Administração contidos na legislação, sem prejuízo de quaisquer outros previstos pela legislação

## 17. DAS SANÇÕES ADMINISTRATIVAS.

**17.1.** Comete infração administrativa nos termos da Lei nº 14.133/2021, a Contratada que:
Der causa à inexecução parcial ou total do contrato;

a. Deixar de entregar os documentos exigidos no certame;
b. Não mantiver a proposta, salvo em decorrência de fato superveniente devidamente justificado;
c. Não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo de validade da proposta;
d. Ensejar o retardamento da execução ou entrega do objeto da licitação sem motivo justificado;
e. Apresentar declaração ou documentação falsa;
f. Fraudar a licitação ou praticar ato fraudulento na execução do contrato;
g. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
h. Praticar atos ilícitos com vistas a frustrar os objetivos da licitação;
i. Praticar ato lesivo previsto no art. 5º da Lei nº 12.846/2013.

**17.2.** O licitante/adjudicatário que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

**a)** Advertência por escrito, por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante;
**b)** Multa
**c)** Impedimento de licitar e contratar;
**d)** Declaração de inidoneidade para licitar ou contratar.

**17.3.** A penalidade de multa pode ser aplicada cumulativamente com as demais sanções.

**17.4.** A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto na Lei nº 14.133/2021.

**17.5.** As multas devidas e/ou prejuízos causados à Contratante serão deduzidos dos valores a serem pagos, ou recolhidos em favor do município de Morro do Chapéu, ou deduzidos da garantia, ou ainda, quando for o caso, serão inscritos na Dívida Ativa e cobrados judicialmente.

17.5.1. Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de **30 dias**, a contar da data do recebimento da comunicação enviada pela autoridade competente.

**17.6.** Caso o valor da multa não seja suficiente para cobrir os prejuízos causados pela conduta do licitante, o município de Morro do Chapéu poderá cobrar o valor remanescente judicialmente, conforme artigo 419 do Código Civil.

**17.7.** A autoridade competente, na aplicação das sanções, levará em consideração a natureza e a gravidade da conduta do infrator, as peculiaridades do caso concreto, as circunstâncias agravantes ou atenuantes e o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

**17.8.** Se, durante o processo de aplicação de penalidade, se houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846/2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização - PAR.

**17.9.** A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846/2013, seguirão seu rito normal na unidade administrativa.

**17.10.** O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

**17.11.** As penalidades serão obrigatoriamente publicadas no órgão Oficial de Imprensa do órgão ou entidade pública.

## 18. DA GARANTIA DE EXECUÇÃO.

**18.1.** Não haverá exigência de garantia contratual da execução dos artigos 96 e seguintes da Lei nº 14.133, de 2021.

## 19. OBRIGAÇÕES DA CONTRATANTE.

**19.1.** São obrigações da Contratante:

19.1.1. Receber o objeto no prazo e condições estabelecidas no Edital e seus anexos;

19.1.2. Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;
19.1.3. Comunicar à Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;
19.1.4. Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de comissão/servidor especialmente designado;
19.1.5. Efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital e seus anexos, observada a ordem cronológica para cada fonte diferenciada de recursos, nos termos do art. 141 da Lei nº 14.133/2021;
**19.2.** A Administração não responderá por quaisquer compromissos assumidos pela Contratada com terceiros, ainda que vinculados à execução do presente Termo de Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da Contratada, de seus empregados, prepostos ou subordinados.

## 20. OBRIGAÇÕES DA CONTRATADA.

**20.1.** A Contratada deve cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:
20.1.1. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Termo de Referência e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, procedência e prazo de validade;
20.1.2. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);
20.1.3. Responsabilizar-se pelos danos causados diretamente à Administração ou a terceiros em razão da execução do contrato;
20.1.4. Reparar, corrigir, remover, reconstruir ou substituir, a suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes de sua execução ou de materiais nela empregados;
20.1.5. Comunicar à Contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;
20.1.6. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;
20.1.7. Indicar preposto para representá-la durante a execução do contrato;
20.1.8. Implantação de programa de integridade pelo licitante vencedor, no prazo de 6 (seis) meses, em caso de licitação de grande vulto, nos termos do artigo 25, §4º da Lei nº 14.133/2021;
20.1.9. Cumprir com a reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e para aprendiz, além de atender às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei nº 8.213/1991.

**Luiz Edil Marques Cavalcante**
**Assessor Técnico**

**ANEXO II**
**MODELO DE DECLARAÇÃO DE CUMPRIMENTO DO DISPOSTO NO INC.XXXIII, DO ART. 7º DA CF**

CONCORRÊNCIA ELETRÔNICO Nº ____/2025
PROCESSO ADMINISTRATIVO Nº ____/2025

**OBJETO: CONTRATAÇÃO DE EMPRESA PARA PRESTAÇÃO DE SERVIÇO ESPECIALIZADO EM TECNOLOGIA DA INFORMAÇÃO E SEGURANÇA DA INFORMAÇÃO, INCLUINDO SUPORTE TÉCNICO EM MÚLTIPLOS NÍVEIS (N1, N2 E N3), IMPLANTAÇÃO E OPERAÇÃO DE SOLUÇÕES DE SEGURANÇA (BACKUP, ANTIVÍRUS, SIEM, RMM, ITSM, ENTRE OUTRAS), APOIO À RESPOSTA A INCIDENTES, E ESTRUTURAÇÃO DE POLÍTICAS E NORMAS DE SEGURANÇA, VISANDO GARANTIR A CONTINUIDADE DOS SERVIÇOS PÚBLICOS, A ESTABILIDADE DA INFRAESTRUTURA DE TI DO MUNICÍPIO DE MORRO DO CHAPÉU/BA**

(Nome da Empresa.....) devidamente inscrita no CNPJ sob o nº ....., com sua sede à Rua..... (endereço completo), declara, para os fins do disposto no inciso VI do art. 68 da Lei Federal nº 14.133/2021, acrescido pela Lei n.º 9.854/99, que não emprega menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não empregamos menor de 16 (dezesseis) anos.

**Ressalva**: emprega menor, a partir de 14 (quatorze) anos, na condição de aprendiz ( )

**Observação**: em caso afirmativo, assinalar a ressalva acima.

Local e data,

**(Assinatura do representante legal)**
Nome e identidade do representante legal

**ANEXO III**
**MODELO DE CARTA DE APRESENTAÇÃO DA PROPOSTA**

CONCORRÊNCIA ELETRÔNICO Nº ____/2025
PROCESSO ADMINISTRATIVO Nº ____/2025

OBJETO: **CONTRATAÇÃO DE EMPRESA PARA PRESTAÇÃO DE SERVIÇO ESPECIALIZADO EM TECNOLOGIA DA INFORMAÇÃO E SEGURANÇA DA INFORMAÇÃO, INCLUINDO SUPORTE TÉCNICO EM MÚLTIPLOS NÍVEIS (N1, N2 E N3), IMPLANTAÇÃO E OPERAÇÃO DE SOLUÇÕES DE SEGURANÇA (BACKUP, ANTIVÍRUS, SIEM, RMM, ITSM, ENTRE OUTRAS), APOIO À RESPOSTA A INCIDENTES, E ESTRUTURAÇÃO DE POLÍTICAS E NORMAS DE SEGURANÇA, VISANDO GARANTIR A CONTINUIDADE DOS SERVIÇOS PÚBLICOS, A ESTABILIDADE DA INFRAESTRUTURA DE TI DO MUNICÍPIO DE MORRO DO CHAPÉU/BA**

Atendendo às exigências deste EDITAL, estamos apresentando nossa "PROPOSTA COMERCIAL" relativa ao presente CONCORRÊNCIA ELETRÔNICA, cujo o valor total é de ..... (por extenso) de acordo com as especificações relacionadas na proposta de preços em anexo.

**Declaramos expressamente que:**
1) Concordamos integralmente e sem qualquer restrição com as condições desta Licitação, expressas neste PREGÃO ELETRÔNICO, bem assim com as condições de contratação estabelecidas na minuta do Contrato anexa ao Edital.
2) Manteremos válida a Proposta pelo prazo mínimo de 60 (sessenta) dias, a contar da data da sua apresentação e abertura.
3) Temos conhecimento dos locais e das condições da realização do objeto deste edital e seus anexos.
4) Na realização do objeto licitado (serviços/compras/fornecimento) observaremos rigorosamente as Normas Técnicas brasileiras, bem assim as recomendações e instruções da Fiscalização da Prefeitura Municipal de MORRO DO CHAPÉU, assumindo, desde já, a integral e exclusiva responsabilidade pela perfeita realização dos trabalhos.
5) Que nos preços propostos estão incluídos todos os encargos, previdenciários, fiscais (ICMS e outros), comerciais, trabalhistas, tributários, embalagens, fretes, seguros, tarifas, descarga, transporte, responsabilidade civil e demais despesas incidentes ou que venham a incidir direta ou indiretamente sobre o objeto desta licitação.
6) Que a Prefeitura não admitirá qualquer alegação posterior que vise o ressarcimento de custos não considerados nos preços, ressalvadas as hipóteses de criação ou majoração de encargos fiscais
7) Que está desimpedida de licitar e/ou contratar com a Administração direta e indireta da União, dos Estados, do Distrito Federal e dos Municípios, abrangendo, inclusive, as entidades com personalidade jurídica de direito privado sob controle do poder público e as fundações por ele instituídas ou mantidas.
8) Que a empresa se encontra habilitada para participar do certame e efetuar contratação nos termos da legislação pertinente.
9) Indicação do banco, número da conta e agência do licitante vencedor, para fins de pagamento.
10) Qualificação completa do representante da empresa que assinará o futuro contrato.
11) Meios de contato: Telefone, celular, e-mails.

Local e data,

**(Assinatura do representante legal)**
Nome e identidade do representante legal

**CONTINUAÇÃO**
**MODELO DE PLANILHA DE PREÇOS**
**EDITAL DE CONCORRÊNCIA ELETRÔNICA N°. 005/2025**

**01 –** IDENTIFICAÇÃO DA EMPRESA LICITANTE:
NOME DA EMPRESA:
CNPJ/MF:
ENDEREÇO:
BAIRRO: CIDADE/UF: CEP:
FONE: ( ) FAX: ( )
NOME PARA CONTATO:

| Item | Descrição | Unidade de Medida | Implantação (Setup) | Manutenção Mensal | Banco de Horas (USTs) | Valor Anual |
|---|---|---|---|---|---|---|
| 1 | Gerenciamento Técnico e Operacional do Contrato - Presencial e Remoto | Mês de vigência contratual | | | | |
| 2 | Serviços Técnicos de Suporte Nível 1 (N1) - 24x7 - Remoto | Mês de vigência contratual com disponibilidade de até 500 chamados no mês corrente. | | | | |
| 3 | Serviços Técnicos de Suporte Nível 2 (N2) - 24x7 - Remoto e Presencial | Mês de vigência contratual com disponibilidade de até 150 chamados no mês corrente. | | | | |
| 4 | Serviços Técnicos de Suporte Nível 3 (N3) - 24x7 - Remoto e Presencial | Mês de vigência contratual com disponibilidade de até 50 chamados no mês corrente. | | | | |
| 5 | Serviços Especializados de Segurança da Informação - 24x7 - Remoto e Presencial | UST - Contrato anual com 1200 UST | | | | |
| 6 | Implantação de Solução de Active Directory Redundante com File Server e DFS | Implantação (setup) | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 7 | Implantação da Solução de ITSM com Módulo de Inventário e CMDB | Implantação (setup) + Mês de vigência contratual | | | | |
| 8 | Implantação da Solução de RMM (Remote Monitoring and Management) - Para até 600 máquinas (servidores e desktops) | Implantação (setup) + Mês de vigência contratual | | | | |
| 9 | Implantação da Solução de Monitoramento de Ativos, Servidores, Redes e Sistemas | Implantação (setup) + Mês de vigência contratual | | | | |
| 10 | Implantação da Solução de Gestão de Logs e SIEM | Implantação (setup) + Mês de vigência contratual | | | | |
| 11 | Implantação de Solução de Análise de Vulnerabilidade Técnica - servidores, desktops, sistemas e rede | Implantação (setup) + Mês de vigência contratual | | | | |
| 12 | Solução de Antivírus com EDR e Filtro de Conteúdo - 580 licenças (servidores e desktops) | Implantação (setup) + Mês de vigência contratual | | | | |
| 13 | Solução de Backup em Nuvem com Segurança Avançada e Recuperação de Desastres - 10TB de armazenamento em nuvem localizados em Datacenter no Brasil | Implantação (setup) + Mês de vigência contratual | | | | |
| **Subtotal** | | | | | | |

**Valor Global da Proposta:** R$ _____ (valor por extenso)

**Instrução adicional:** "A licitante deverá preencher o valor global da proposta neste campo, apresentando-o em reais (R$) com duas casas decimais e, obrigatoriamente, também por extenso."

**02 -** DADOS BANCÁRIOS:
Conta n.º: _____
Agencia n.º: _____
Banco: _____
**03 -** CONDIÇÕES DE PAGAMENTO: conforme Edital
**04 -** VALIDADE DA PROPOSTA: 60 (sessenta) dias.
**05 -** PRAZO PARA FORNECIMENTO/SERVIÇOS – Imediatamente após a solicitação.
**06 -** PREÇOS: Os preços são os apresentados na planilha anexa.

**Divergência entre valores unitários e valor global**

Em caso de divergência entre os valores unitários indicados na tabela, no subtotal e o valor global apresentado ao final, prevalecerão os valores unitários. A Administração procederá à correção aritmética da proposta, adotando o somatório dos itens como base para o valor global.

Caso a divergência comprometa a exequibilidade da proposta ou indique erro material grave, a proposta poderá ser desclassificada, conforme previsto no art. 59, I, da Lei nº 14.133/2021.

**Instruções obrigatórias para preenchimento da proposta de preços:**

A licitante deverá preencher integralmente o modelo acima, conforme os quantitativos e escopo previstos neste Termo de Referência.

Todos os valores individuais constantes da tabela de proposta deverão ser expressos em reais (R$), com duas casas decimais, contemplando todos os encargos incidentes, tais como tributos, insumos, licenças, serviços de terceiros, fretes, encargos sociais, trabalhistas, previdenciários, despesas com deslocamento e quaisquer outros custos diretos ou indiretos necessários para o pleno cumprimento do objeto, não sendo admitido qualquer ônus adicional à Administração.

A linha de Subtotal deverá ser obrigatoriamente preenchida pela licitante, contendo o somatório de cada coluna: valores de implantação (setup), manutenção mensal e banco de horas (se houver). Esses subtotais devem corresponder à soma das linhas de cada item da tabela principal.

O Valor Global da proposta deverá considerar o **somatório dos valores de implantação, manutenção mensal e banco de horas (USTs)**, conforme aplicável. O Valor Global da Proposta deverá representar o somatório final de todos os subtotais apresentados. O valor global deverá ser apresentado ao final da tabela, expresso em reais (R$) com duas casas decimais e descrito por extenso.

A proposta deverá ser apresentada em papel timbrado da licitante, com a assinatura do responsável legal, contendo CNPJ, endereço completo e contato oficial.

É vedada a apresentação de planilha em formato diferente do modelo estabelecido neste anexo. A utilização de modelos próprios, incompletos ou despadronizados acarretará a desclassificação da proposta.

A proposta de preços deverá ter validade mínima de 60 (sessenta) dias, contados a partir da data de abertura das propostas.

Em campos da tabela onde não se aplicar a cobrança de determinado item (por exemplo, ausência de implantação, manutenção mensal ou banco de horas), a licitante deverá preencher o valor com “R$ 0,00”, para manter a consistência da estrutura da proposta e viabilizar a correta apuração do valor global.

**Instrução Complementar – Obrigatoriedade da Declaração**

Além da tabela de preços preenchida conforme o modelo acima, a proposta de preços deverá conter, obrigatoriamente, em documento anexo ou no corpo da própria proposta, a seguinte declaração expressa, assinada pelo representante legal da licitante:

**Declaração Obrigatória da Licitante**

A licitante, por meio de seu representante legal, declara, para os devidos fins, que:

- Está integralmente ciente e de acordo com todas as exigências constantes no Termo de Referência e seus anexos;
- A proposta apresentada contempla todos os encargos diretos e indiretos, tributos, insumos, ferramentas, licenças, deslocamentos, pessoal técnico, suporte e quaisquer outras despesas necessárias à perfeita execução dos serviços;
- Os valores apresentados estão expressos em reais (R$), com duas casas decimais, e possuem validade mínima de 60 (sessenta) dias;
- Compromete-se, caso vencedora, a executar o objeto proposto nos exatos termos da documentação apresentada, sem omissões ou exclusões não justificadas;
- Reconhece como válida e aceita a estrutura de preços por item, os métodos de medição, as obrigações e as sanções previstas.

Local e data.
PROPONENTE:
DADOS DA PROPONENTE:
Nome:
Razão Social:
Endereço Completo/Telefone:

Local e data,

**(Assinatura do representante legal)**
Nome e identidade do representante legal

**ANEXO IV**
**MODELO DECLARAÇÃO DE PLENO CONHECIMENTO**

CONCORRÊNCIA ELETRÔNICA Nº ____/2025
PROCESSO ADMINISTRATIVO Nº ____/2025

OBJETO: **CONTRATAÇÃO DE EMPRESA PARA PRESTAÇÃO DE SERVIÇO ESPECIALIZADO EM TECNOLOGIA DA INFORMAÇÃO E SEGURANÇA DA INFORMAÇÃO, INCLUINDO SUPORTE TÉCNICO EM MÚLTIPLOS NÍVEIS (N1, N2 E N3), IMPLANTAÇÃO E OPERAÇÃO DE SOLUÇÕES DE SEGURANÇA (BACKUP, ANTIVÍRUS, SIEM, RMM, ITSM, ENTRE OUTRAS), APOIO À RESPOSTA A INCIDENTES, E ESTRUTURAÇÃO DE POLÍTICAS E NORMAS DE SEGURANÇA, VISANDO GARANTIR A CONTINUIDADE DOS SERVIÇOS PÚBLICOS, A ESTABILIDADE DA INFRAESTRUTURA DE TI DO MUNICÍPIO DE MORRO DO CHAPÉU/BA**

A empresa .... C.N.P.J. nº , sediada .... declara, sob as penas da lei, que até a presente data inexistem fatos impeditivos para sua habilitação no processo licitatório, CONCORRÊNCIA ELETRÔNICA nº ____/2025 da Prefeitura Municipal de Morro do Chapéu-BA, ciente da obrigatoriedade de declarar ocorrências posteriores e ainda o **pleno conhecimento e atendimento às exigências de habilitação**, cientes das sanções factíveis de serem aplicadas.

Local e data,

**(Assinatura do representante legal)**
Nome e identidade do representante legal

**ANEXO V**
**MINUTA DO CONTRATO**

**O MUNICÍPIO DE MORRO DO CHAPÉU-BA**, pessoa jurídica de direito público interno, inscrito no CNPJ sob nº. **13.717.517/0001-48**, situada na Rua Coronel Dias Coelho n° 188, neste ato representado por sua gestora, a Srª Juliana Pereira Araújo Leal, brasileira, casada, advogada, do outro lado a empresa, **xxxxxxxxxxxx**, pessoa jurídica de direito privado, estabelecida na xxxxxxxxxxxxxxxxxxx, CEP xxxx inscrita do CNPJ/MF, sob o nº xxxxxxxxxxx, aqui representada pelo **xxxxxxxxxxxxxxxx**, brasileiro, >>>>>>>>>, inscrito no CPF sob o nº >>>>>>>>>>>>>>>, RG nº >>>>>>>>>>, residente e domiciliado à >>>>>>>>>>>>>>>>>>>> CEP >>>>>>>>>>>>>>>>>> aqui denominado **CONTRATADA**, resolvem firmar o presente contrato, sob o regime de execução indireta por preço unitário, nos termos do procedimento licitatório **CONCORRÊNCIA ELETRÔNICA Nº 005/2025,** observadas as disposições contidas na Lei Federal nº 14.133, de 01/04/2021, e com fundamento nas disposições e princípios gerais, na forma e condições seguintes

**CLÁUSULA PRIMEIRA - Do Objeto**

**1.2.** 1.1. O presente contrato tem por objeto a **CONTRATAÇÃO DE EMPRESA PARA PRESTAÇÃO DE SERVIÇO ESPECIALIZADO EM TECNOLOGIA DA INFORMAÇÃO E SEGURANÇA DA INFORMAÇÃO, INCLUINDO SUPORTE TÉCNICO EM MÚLTIPLOS NÍVEIS (N1, N2 E N3), IMPLANTAÇÃO E OPERAÇÃO DE SOLUÇÕES DE SEGURANÇA (BACKUP, ANTIVÍRUS, SIEM, RMM, ITSM, ENTRE OUTRAS), APOIO À RESPOSTA A INCIDENTES, E ESTRUTURAÇÃO DE POLÍTICAS E NORMAS DE SEGURANÇA, VISANDO GARANTIR A CONTINUIDADE DOS SERVIÇOS PÚBLICOS, A ESTABILIDADE DA INFRAESTRUTURA DE TI DO MUNICÍPIO DE MORRO DO CHAPÉU/BA**, conforme especificações e quantitativos indicados no processo Administrativo nº 225/2025 e relacionados nas planilhas contidas nos Anexos da CONCORRÊNCIA ELETRÔNICA N° 005/2025 e na proposta vencedora.

1.2. A execução do presente contrato será realizada de acordo às necessidades do Município de Morro do Chapéu.

1.3. Constitui parte integrante deste contrato todos os documentos e instruções que compõem a CONCORRÊNCIA ELETRÔNICA N° 005/2025, completando o presente instrumento para todos os fins de direito, independentemente de sua transcrição, obrigando-se as partes em todos os seus termos.

1.3.1. Ficam também fazendo parte deste CONTRATO, as normas vigentes, as instruções, a Ordem de Serviço e, mediante aditamento, qualquer modificação que venha ser necessária durante sua vigência.

**CLÁUSULA SEGUNDA – Responsabilidade das Partes:**

**2.1. Além das condições dispostas no Termo de Referência (Anexo I do edital) Obriga-se a CONTRATANTE**:

a) A Contratante obriga-se a:

b) Verificar minuciosamente, no prazo fixado, a conformidade dos bens recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivos;

c) Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de servidor especialmente designado;

d) Efetuar o pagamento no prazo previsto;

**2.2. Além das condições dispostas no Termo de Referência (Anexo I do edital), obriga-se a CONTRATADA:**

a) Responder, independentemente de culpa, por qualquer dano pessoal ou patrimonial a CONTRATANTE, ou ainda a terceiros, na execução do objeto deste Termo e da licitação, não sendo excluída, ou mesmo reduzida, a responsabilidade pelo fato de haver fiscalização ou acompanhamento pela CONTRATANTE.

b) Manter, durante todo o período do contrato, todas as condições de habilitação e qualificação exigidas na licitação, e quando da realização do pagamento pelo Município de Morro do Chapéu-Bahia, comunicando, imediatamente, a superveniência de fato impeditivo da manutenção dessa condição, nos termos da Lei 14.133/21 e suas alterações posteriores.

c) Cumprir outras obrigações previstas no Código de Proteção e Defesa do Consumidor (Lei n° 8.078/90) que sejam compatíveis com o regime de direito público.

d) Responder, integralmente, por perdas e danos que vier a causar a esta Prefeitura ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou dos seus prepostos, independentemente de outras cominações contratuais ou legais a que estiver sujeita.

e) Prestar os esclarecimentos que forem solicitados pelo Município de Morro do Chapéu-Bahia.

f) Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;
g) Responsabilizar-se pelas despesas dos tributos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, fretes, seguros, deslocamento de pessoal, prestação de garantia e quaisquer outras que incidam ou venham a incidir na execução do contrato;
h) A inadimplência com referência aos encargos e obrigações estabelecidos não transfere ao Município de Morro do Chapéu-Bahia a responsabilidade pelo seu pagamento, nem poderá onerar o fornecimento, razão pela qual a Empresa Vencedora renuncia expressamente a qualquer vínculo de solidariedade, ativa ou passiva, com a Contratante;
i) Quando for o caso, assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação de acidentes de trabalho, quando em ocorrência da espécie forem vítimas os seus profissionais no desempenho de alguma atividade pertinente ao fornecimento ou em conexão ou contingência, na forma como a expressão;
j) Manter, pessoal e equipamentos suficientes para o atendimento;
k) Assumir inteira responsabilidade quanto à qualidade dos serviços;
l) A futura contratada deverá disponibilizar de quantos equipamentos o município necessite, até o limite de horas a ser contratado.

**CLÁUSULA TERCEIRA – Do Valor**
3.1. O valor do presente contrato é de R$ _____, conforme definido na proposta apresentada e itens abaixo:

| ITEM | ESPECIFICAÇÕES | UND. | QUANT. | VALOR UNITÁRIO | VALOR TOTAL |
|---|---|---|---|---|---|

3.2. Nos preços já estão inclusos todos os custos necessários à execução do fornecimento do presente contrato, bem como todos os impostos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, fretes, deslocamento de pessoal, transporte, garantia dos materiais/acessórios e quaisquer outros que incidam ou venham a incidir sobre o objeto licitado constante da proposta. Não será permitido, portanto, que tais encargos sejam discriminados em separado.

**CLÁUSULA QUARTA – Do Pagamento**
4.1. A contratante pagará a contratada de acordo com a quantidade efetivamente executada e entregue, em até 30 (trinta) dias após a apresentação das Notas Fiscais correspondentes e depois de atestada pelo Contratante a efetiva satisfação do objeto contratual.
4.1.1. Os valores deverão ser pagos a CONTRATADA através de crédito na Conta Corrente....., da Agência ..... Banco..... .
4.2. A liquidação das despesas obedecerá ao estabelecido na Lei nº 4320/64.
4.3. Os pagamentos poderão ser sustados pelo Município nos seguintes casos:
a) Não cumprimento das obrigações assumidas que possam de qualquer forma prejudicar a contratante;
b) Inadimplência de obrigações da contratada para com o Município, por conta do estabelecido no contrato;
4.4. Nenhum pagamento será efetuado enquanto houver qualquer pendência de liquidação ou obrigação que lhe for imposta, sem que isto gere direito ao pleito de reajustamento de preços ou correção.
4.5. Fica assegurado ao contratado, na forma do art. 130 da Lei 14.133/21 e alterações posteriores, estabelecer o equilíbrio financeiro do contrato, desde que devidamente comprovado.
4.6. Obriga-se a Contratada, nos termos do art. 92, inciso XVI da Lei 14.133/21, manter-se durante a execução do presente contrato, em compatibilidade com as obrigações aqui assumidas, todas as condições de habilitação e qualificação exigidas por ocasião da licitação.
4.7. Para efeito de pagamento serão computados apenas os quantitativos efetivamente fornecidos.

**CLÁUSULA QUINTA – Condições gerais da Execução**
5.1 A execução do objeto seguirá a seguinte dinâmica:
a) O início da execução do objeto será a partir da assinatura do Contrato de Prestação de Serviços;
b) Os serviços devem ser prestados no Município de Morro do Chapéu, nas suas unidades administrativas.

5.2. A execução dos serviços objeto desta contratação tem como finalidade assegurar a estabilidade, disponibilidade, segurança e continuidade das operações tecnológicas da Prefeitura Municipal, mediante a prestação de serviços técnicos especializados em tecnologia da informação e segurança da informação. A atuação da contratada envolverá suporte técnico operacional em múltiplos níveis (N1, N2 e N3), bem como a implantação e operação de soluções essenciais de infraestrutura, segurança e governança de TI, voltadas à modernização do ambiente computacional da Administração.

5.3. Atualmente, o parque tecnológico da Prefeitura é composto por aproximadamente 386 equipamentos em operação, entre desktops e notebooks, além de 111 impressoras. Há também 49 desktops, 8 notebooks e 23 impressoras fora de uso, por motivos técnicos. Com a contratação paralela de novos equipamentos por meio de locação, o parque será ampliado para 526 estações ativas (sendo 387 desktops e 139 notebooks), além de 155 impressoras, considerando ainda uma margem de crescimento de até 10%, em razão da posse de novos servidores públicos aprovados em concurso.

5.4. Com a modernização proposta, serão implantadas soluções estratégicas, como controladores de domínio (Active Directory) com redundância, servidores de arquivos com alta disponibilidade, antivírus corporativo, backup em nuvem, gestão de acessos, análise de vulnerabilidades, gestão de logs, monitoramento, sistema ITSM, inventário automatizado, entre outras medidas alinhadas às boas práticas de segurança da informação.

5.5. Para suportar essa estrutura, a contratada deverá dispor de uma equipe técnica multidisciplinar estruturada em três níveis de atendimento:

- **Nível 1 (N1):** atendimento inicial, triagem, resolução de demandas comuns e contato direto com o usuário final;
- **Nível 2 (N2):** atendimento técnico intermediário, voltado à resolução de incidentes e solicitações não solucionadas pelo N1;
- **Nível 3 (N3):** atendimento especializado, voltado à infraestrutura crítica, ambientes complexos e soluções de segurança da informação.

5.6. Considerando o porte da operação e o número de usuários atendidos, aproximadamente 1600 servidores entre estatutários, comissionados e temporários os atendimentos deverão observar os seguintes regimes:

- **N1 e N2 – Atendimento Regular:** segunda a sexta-feira, das 7h às 19h; e aos sábados, das 7h às 13h;
- **N1 e N2 – Atendimento Extraordinário 24x7x365:** para serviços críticos, unidades com funcionamento ininterrupto (ex: saúde), e atendimento a autoridades administrativas sempre que houver demanda;
- **N3 e Serviços Especializados de Segurança – Atendimento 24x7x365:** com foco na integridade, disponibilidade e estabilidade dos serviços estratégicos, incluindo domínios, backups, antivírus, SIEM, análise de vulnerabilidades e outros.

5.7. Todas as soluções contratadas deverão contar com suporte técnico integral, de forma a assegurar o pleno funcionamento da estrutura de TI da Prefeitura, a resiliência da infraestrutura crítica e a conformidade com as normas legais aplicáveis, especialmente quanto à proteção de dados, continuidade dos serviços públicos e segurança da informação.

**Processo de Atendimento Técnico**

5.8. Todo o processo de atendimento será executado por meio da Central de Serviços de TI da contratada, que atuará como ponto único de contato (SPoC – Single Point of Contact) para os usuários da Administração Pública. Essa Central será responsável por garantir o funcionamento contínuo do parque tecnológico da Prefeitura, bem como a manutenção dos serviços de tecnologia implantados. O atendimento será estruturado em múltiplos níveis, com escalonamento técnico conforme a natureza e a complexidade das demandas.

**CLÁUSULA SEXTA – Do Prazo de Vigência**

6.1. O prazo de execução do contrato a ser celebrado com a Licitante vencedora é até xx de xxxxx de 20xx, na forma do artigo 105 da Lei n° 14.133, de 2021, a contar de sua assinatura e posterior publicação.

6.1.1. Havendo interesse da Municipalidade, o contrato decorrente desta Licitação poderá ter o seu prazo prorrogado, por meio de aditivo contratual, sempre se observando o prazo estabelecido no art. 106 da Lei 14.133/21 e a existência de saldo contratual.

6.2. As alterações contratuais atenderão ao interesse público, obedecidas as normas gerais previstas na Lei Federal 14.133/21, incorporando as alterações posteriores.

**CLÁUSULA SETIMA – Da Dotação Orçamentária**

7.1. Os recursos necessários ao pagamento das despesas inerentes a este contrato correrão por conta das dotações orçamentárias e elementos de despesa abaixo discriminados:

**UNIDADE: 02.07.01 – SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO E FINANÇAS - SEAF**
**2009 – MANUTENÇÃO DAS AÇÕES DA SEC. MUNICIPAL DE ADMINISTRAÇÃO**
**3390.40 – SERVICOS DE TEC. DA INFO. E COMUNICACAO - PJ**
**FONTES:**
**15000000 – RECURSOS NÃO VINCULADOS DE IMPOSTOS,**
**15010000 – OUTROS RECURSOS NÃO VINCULADOS.**

**CLÁUSULA OITAVA – Da Fiscalização**

8.1. A execução do Contrato será acompanhada por servidor previamente designado pela Administração, nos termos do Art. 117 da Lei nº 14.133/21, que verificará o cumprimento das especificações técnicas, dando ênfase aos aspectos de qualidade e presteza no atendimento, podendo rejeitá-los no todo ou em parte, quando estes não obedecerem ou não atenderem ao desejado ou especificado.

8.2. A fiscalização por parte da CONTRATANTE não desobriga a CONTRATADA de sua responsabilidade quanto a perfeita prestação dos serviços contratados.

8.3. As ordens de serviço e toda a correspondência referente ao contrato, exceto as de rotina, serão feitas por ofício. Na hipótese de a CONTRATADA se negar a assinar o recebimento do ofício no competente livro de carga, o mesmo será enviado pelo correio, registrado, considerando-se feita a comunicação para todos os efeitos.

**CLÁUSULA NONA – Das Penalidades**

9.1. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o contratado que:

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.

9.1. Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

i. **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);

ii. **Impedimento de licitar e contratar**, quando praticadas as condutas descritas nas alíneas "b", "c" e "d" do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);

iii. **Declaração de inidoneidade para licitar e contratar**, quando praticadas as condutas descritas nas alíneas "e", "f", "g" e "h" do subitem acima deste Contrato, 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).

9.2. 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)

9.2.1. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).

9.2.2. 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)

9.2.3. 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 prestada ou será cobrada judicialmente (art. 156, §8º, da Lei nº 14.133, de 2021).

9.2.4. 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.

9.3. 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.

9.4. Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133, de 2021):
a) a natureza e a gravidade da infração cometida;
b) as peculiaridades do caso concreto;
c) as circunstâncias agravantes ou atenuantes;
d) os danos que dela provierem para o Contratante;
e) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

9.5. 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).

*9.6.* A personalidade jurídica do Contratado 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).

*9.7.* O Contratante deverá, no prazo máximo de 15 (quinze) 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), instituídos no âmbito do Poder Executivo Federal. (Art. 161, da Lei nº 14.133, de 2021).

*9.8.* 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.

**CLÁUSULA DÉCIMA – Da Extinção**

10.1. O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

10.2. Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

10.3. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a extinção se não restringir sua capacidade de concluir o contrato.

10.4. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

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

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

10.5.2. Relação dos pagamentos já efetuados e ainda devidos;

10.5.3. Indenizações e multas.

10.6. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório (art. 131, *caput,* da Lei n.º 14.133, de 2021).

10.7. O contrato poderá ser extinto caso se constate que o contratado mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que tenha desempenhado função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau (art. 14, inciso IV, da Lei n.º 14.133, de 2021).

**CLÁUSULA DÉCIMA PRIMEIRA - Da Alteração**

11.1 - Este contrato poderá ser alterado mediante assentimento das partes através de Termos Aditivos, objetivando promover os acréscimos ou supressões que se fizerem necessários ou em decorrência de fatores supervenientes que possam torná-lo inexequível.

11.2. A contratada é obrigada a aceitar nas mesmas condições contratuais os acréscimos ou supressões que se fizerem no objeto do presente contrato, até 25% (vinte e cinco por cento) de seu valor inicial atualizado;

11.3. Eventual reequilíbrio econômico-financeiro, para restabelecer relação que as partes pactuaram inicialmente sobre os encargos do contratado e a retribuição da Administração, poderá ser solicitado pela contratada, observando o previsto no art. 130, da Lei nº 14.133/21.

**CLÁUSULA DÉCIMA SEGUNDA - Do Foro**

12.1. Fica eleito o Foro da Comarca de MORRO DO CHAPÉU, BA para dirimir as questões decorrentes deste Contrato, renunciando as partes, expressamente, a qualquer outro, por mais privilegiado que seja.

E, por estarem justas e combinadas, as partes firmam, em 03 (três) vias de igual teor e forma, o presente Contrato.

MORRO DO CHAPÉU, BA, ..... de .....de 2025.

| | |
|---|---|
| **CONTRATANTE:**<br>**MUNICIPIO DE MORRO DO CHAPÉU, ESTADO DA BAHIA.** | **CONTRATADA:**<br>**xxxxxxxxxxxxxxxxxxxxxx** |
| Juliana P. Araújo Leal<br>Prefeita | xxxxxxxxxxxxxxxxxxx<br>Representante legal |

| | |
|---|---|
| **Testemunhas:** | |
| Nome:_____ | Nome:_____ |
| CPF/RG: | CPF/RG: |

**ANEXO VI**
**MODELO DE PROCURAÇÃO**

CONCORRÊNCIA ELETRÔNICO Nº ____/2025
PROCESSO ADMINISTRATIVO Nº ____/2025

**OBJETO: CONTRATAÇÃO DE EMPRESA PARA PRESTAÇÃO DE SERVIÇO ESPECIALIZADO EM TECNOLOGIA DA INFORMAÇÃO E SEGURANÇA DA INFORMAÇÃO, INCLUINDO SUPORTE TÉCNICO EM MÚLTIPLOS NÍVEIS (N1, N2 E N3), IMPLANTAÇÃO E OPERAÇÃO DE SOLUÇÕES DE SEGURANÇA (BACKUP, ANTIVÍRUS, SIEM, RMM, ITSM, ENTRE OUTRAS), APOIO À RESPOSTA A INCIDENTES, E ESTRUTURAÇÃO DE POLÍTICAS E NORMAS DE SEGURANÇA, VISANDO GARANTIR A CONTINUIDADE DOS SERVIÇOS PÚBLICOS, A ESTABILIDADE DA INFRAESTRUTURA DE TI DO MUNICÍPIO DE MORRO DO CHAPÉU/BA**

Pelo presente instrumento particular de procuração e pela melhor forma de direito a empresa (Nome da Empresa....., ), com sede à Rua.....(endereço completo), devidamente inscrita no CNPJ sob o nº ....., representada, neste ato por seu sócio gerente, Sr....., brasileiro, casado, empresário, residente e domiciliado nesta cidade, nomeia e constitui seu representante, o Sr....., brasileiro, (estado civil), ....(profissão...), portador da cédula de identidade nº ..... e do CPF nº ....., a quem são conferidos poderes para representar a empresa outorgante no **CONCORRÊNCIA ELETRÔNICA Nº _____/2025**, instaurado pela Prefeitura Municipal de MORRO DO CHAPÉU, em especial para firmar declarações e atas, apresentar ou desistir da apresentação de lances verbais, negociar os valores propostos, interpor ou desistir da interposição de recursos e praticar todos os demais atos pertinentes ao certame acima indicado.

Local e data,

**(Assinatura do representante legal)**
Nome e identidade do representante legal

**ANEXO VII**
**MODELO DE DECLARAÇÃO DE MICRO EMPRESA OU EMPRESA DE PEQUENO PORTE**

CONCORRÊNCIA ELETRÔNICA Nº ____/2025
PROCESSO ADMINISTRATIVO Nº ____/2025

**OBJETO: CONTRATAÇÃO DE EMPRESA PARA PRESTAÇÃO DE SERVIÇO ESPECIALIZADO EM TECNOLOGIA DA INFORMAÇÃO E SEGURANÇA DA INFORMAÇÃO, INCLUINDO SUPORTE TÉCNICO EM MÚLTIPLOS NÍVEIS (N1, N2 E N3), IMPLANTAÇÃO E OPERAÇÃO DE SOLUÇÕES DE SEGURANÇA (BACKUP, ANTIVÍRUS, SIEM, RMM, ITSM, ENTRE OUTRAS), APOIO À RESPOSTA A INCIDENTES, E ESTRUTURAÇÃO DE POLÍTICAS E NORMAS DE SEGURANÇA, VISANDO GARANTIR A CONTINUIDADE DOS SERVIÇOS PÚBLICOS, A ESTABILIDADE DA INFRAESTRUTURA DE TI DO MUNICÍPIO DE MORRO DO CHAPÉU/BA**

_____ (nome da empresa), estabelecida na _____ (rua; nº e cidade), neste ato representada por seu representante legal _____ (nome do representante), _____ (nacionalidade), _____ (estado civil), RG nº _____ e CPF nº _____, residente e domiciliado na _____ (rua; nº e cidade), declara, sob as penas das Leis Civis e Penais, que a empresa acima citada classifica-se como Microempresa - ME ou Empresa de Pequeno Porte - EPP, perante a _____ (Receita Federal e/ou Secretaria da Fazenda do Estado).

Local e data,

**(Assinatura do representante legal)**
Nome e identidade do representante legal

**ANEXO VIII**
**MODELO DE DECLARAÇÃO DE INIDONEIDADE**

CONCORRÊNCIA ELETRÔNICA Nº ____/2025

PROCESSO ADMINISTRATIVO Nº ____/2025

**OBJETO: CONTRATAÇÃO DE EMPRESA PARA PRESTAÇÃO DE SERVIÇO ESPECIALIZADO EM TECNOLOGIA DA INFORMAÇÃO E SEGURANÇA DA INFORMAÇÃO, INCLUINDO SUPORTE TÉCNICO EM MÚLTIPLOS NÍVEIS (N1, N2 E N3), IMPLANTAÇÃO E OPERAÇÃO DE SOLUÇÕES DE SEGURANÇA (BACKUP, ANTIVÍRUS, SIEM, RMM, ITSM, ENTRE OUTRAS), APOIO À RESPOSTA A INCIDENTES, E ESTRUTURAÇÃO DE POLÍTICAS E NORMAS DE SEGURANÇA, VISANDO GARANTIR A CONTINUIDADE DOS SERVIÇOS PÚBLICOS, A ESTABILIDADE DA INFRAESTRUTURA DE TI DO MUNICÍPIO DE MORRO DO CHAPÉU/BA**

_____ (nome da empresa), estabelecida na _____ (rua; nº e cidade), neste ato representada por seu representante legal _____ (nome do representante), _____ (nacionalidade), _____ (estado civil), RG nº _____ e CPF nº _____, Declara, sob as penas da Lei, que na qualidade de proponente do procedimento licitatório, sob a modalidade Concorrência Eletrônica nº _____ instaurada pela **Prefeitura Municipal de Morro do Chapéu - Bahia**, que não fomos declarados inidôneos para licitar ou contratar com o Poder Público, em qualquer de suas esferas.

Por ser expressão de verdade, firmamos a presente.

Local e data,

**(Assinatura do representante legal)**
Nome e identidade do representante legal

**ANEXO IX**
**MODELO DE DECLARAÇÃO DE FATOS IMPEDITIVOS**

CONCORRÊNCIA ELETRÔNICA Nº ____/2025
PROCESSO ADMINISTRATIVO Nº ____/2025

**OBJETO: CONTRATAÇÃO DE EMPRESA PARA PRESTAÇÃO DE SERVIÇO ESPECIALIZADO EM TECNOLOGIA DA INFORMAÇÃO E SEGURANÇA DA INFORMAÇÃO, INCLUINDO SUPORTE TÉCNICO EM MÚLTIPLOS NÍVEIS (N1, N2 E N3), IMPLANTAÇÃO E OPERAÇÃO DE SOLUÇÕES DE SEGURANÇA (BACKUP, ANTIVÍRUS, SIEM, RMM, ITSM, ENTRE OUTRAS), APOIO À RESPOSTA A INCIDENTES, E ESTRUTURAÇÃO DE POLÍTICAS E NORMAS DE SEGURANÇA, VISANDO GARANTIR A CONTINUIDADE DOS SERVIÇOS PÚBLICOS, A ESTABILIDADE DA INFRAESTRUTURA DE TI DO MUNICÍPIO DE MORRO DO CHAPÉU/BA**

_____ (nome da empresa), estabelecida na _____ (rua; nº e cidade), neste ato representada por seu representante legal _____ (nome do representante), _____ (nacionalidade), _____ (estado civil), RG nº _____ e CPF nº _____, Declara, sob as penas da Lei, que na qualidade de proponente do procedimento licitatório, sob a modalidade Concorrência Eletrônica nº _____ instaurada pela **Prefeitura Municipal de Morro do Chapéu - Bahia**, que até a presente data inexistem fatos impeditivos para sua habilitação no presente processo e que está ciente da obrigatoriedade de declarar ocorrências posteriores.

Por ser expressão de verdade, firmamos a presente.

Local e data,

**(Assinatura do representante legal)**
Nome e identidade do representante legal

**ANEXO X**
**MODELO DE DECLARAÇÃO DE AUTENTICIDADE DOS DOCUMENTOS**

CONCORRÊNCIA ELETRÔNICA Nº ____/2025
PROCESSO ADMINISTRATIVO Nº ____/2025

OBJETO: **CONTRATAÇÃO DE EMPRESA PARA PRESTAÇÃO DE SERVIÇO ESPECIALIZADO EM TECNOLOGIA DA INFORMAÇÃO E SEGURANÇA DA INFORMAÇÃO, INCLUINDO SUPORTE TÉCNICO EM MÚLTIPLOS NÍVEIS (N1, N2 E N3), IMPLANTAÇÃO E OPERAÇÃO DE SOLUÇÕES DE SEGURANÇA (BACKUP, ANTIVÍRUS, SIEM, RMM, ITSM, ENTRE OUTRAS), APOIO À RESPOSTA A INCIDENTES, E ESTRUTURAÇÃO DE POLÍTICAS E NORMAS DE SEGURANÇA, VISANDO GARANTIR A CONTINUIDADE DOS SERVIÇOS PÚBLICOS, A ESTABILIDADE DA INFRAESTRUTURA DE TI DO MUNICÍPIO DE MORRO DO CHAPÉU/BA**

A Empresa _____, devidamente inscrita no CNPJ sob o n.º. _____, por intermédio de seu representante legal abaixo assinado, Sr. (a). _____, portador(a) do Documento de Identidade n.º. _____, expedido por _____, e inscrito no Cadastro de Pessoa Física do Ministério da Fazenda (CPF/MF) sob o n.º. _____, DECLARA, sob as sanções administrativas cabíveis, inclusive as criminais, e sob as penas da lei, que toda documentação anexada ao Sistema são autênticas, igualmente sendo expressão da verdade a informação por mim prestada, estou ciente que esta declaração estará sujeita as penalidades da Lei, conforme dispõe o art. 299 do Código Penal Brasileiro, que prevê o crime de falsidade ideológica.

Local e data,

**(Assinatura do representante legal)**
Nome e identidade do representante legal